МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)

Экономический факультет

Кафедра мировой экономики и менеджмента

Допустить к защите
Заведующий кафедрой,
д-р экон. наук, проф.
_____ И.В. Шевченко
(подпись)
_____2022 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ КАК ФАКТОР ЭКОНОМИЧЕСКОЙ УСТОЙЧИВОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Работу выполнил _____М.Г. Асаева
(подпись)
Специальность 38.05.01 Экономическая безопасность
(код, наименование)
Специализация Экономико-правовое обеспечение экономической безопасности

Научный руководитель
д-р экон. наук, проф.____С. Н. Третьякова
(подпись)
Нормоконтролер
канд. экон. наук, доц._____ Т.С. Малахова
(подпись)

Краснодар
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Устойчивое развитие страны является крайне важны аспектом в его деятельности. Это связано с тем, что в современных условиях значительно повышается значимость развития всех составляющих национальной безопасности, так как повышается уровень конкуренции на мировом рынке.

Влияние информационной безопасности на стабильное развитие устойчивости страны является важным аспектом.

На данный момент существует большое количество угроз информационной безопасности, ослабевающих функционирование экономики страны. Так, киберугрозы являются одним из видов рассматриваемых угроз.

Именно киберугрозы в последние годы отличаются тем, что наносят огромный вред для страны. Также, киберугрозы практически не наказуемы, так как зачастую не отслеживаются. Начиная с 2020 года объем киберпреступлений вырос езе и за счет того, что с переходом работы предприятий на удаленный формат увеличилась доступность совершения киберпреступлений.

Среди основных способов, с помощью которых совершаются киберпреступления, можно выделить:

– кардинг;

– фишинг;

– крекинг;

– хакинг;

– ньюкинг.

Вопрос кибербезопасности, как фактора устойчивого развития страны является достаточно актуальным не только ввиду сложности его содержания, но и ввиду того, что в последние годы увеличивается влияние киберпреступности на развитие стран. Начиная с 2020 года, когда большое количество предприятий перешло на удаленный режим работы, повысилась доступность информации, на которую совершаются кибератаки.

Проблемам исследования кибербезопасности, как состоянию устойчивого развития страны посвящены труды отечественных и зарубежных ученых. Среди них можно отметить: Н. А. Веселова, Э.А. Арустамова, С.Н. Лебедева, О.В. Морозова и других.

Проблема кибербезопасности в России особо актуальна на данном этапе, поэтому требуется исследование ее современного состояния и тенденций развития, и на этой основе выработка направлений противодействия угрозам кибербезопасности.

Цель дипломной работы – исследование влияния кибербезопасности на устойчивое развитие страны и разработка эффективных методов, инструментов, мероприятий по противодействию угрозам кибербезопасности.

Для реализации цели был разработан и решен ряд задач, среди которых можно выделить:

– рассмотрение понятия и сущности экономической устойчивости;

– рассмотрение факторов, влияющих на экономическую устойчивость РФ;

– рассмотрение кибербезопасности, как фактора экономической устойчивости РФ;

– проведение анализа экономической устойчивости РФ;

– анализ состояния кибербезопасности РФ;

– разработка мер по повышению уровня кибербезопасности;

– рассмотрение угроз устойчивого развития РФ, а также разработка по их нейтрализации.

Объектом исследования является кибербезопасность Российской Федерации. Предмет исследования – экономические отношения, связанные с влиянием кибербезопасности на устойчивое развитие страны /

В исследовании применяются методы системного и комплексного подходов, логического, структурного и факторного анализа, экономико-статистические и финансово-экономические методы, а также общенаучные методы научного познания: формально-логические способы обработки

информации, методы сравнения, абстрагирования, изучение и обобщение российской и мировой практики по исследуемой теме, анализ нормативно-правовой базы, теоретический анализ и синтез.

Информационную основу исследования составили классические и современные труды отечественных и зарубежных ученых, публикации в изданиях, посвященных проблеме кибербезопасности. В работе использованы данные Росстата по РФ и ее субъектам, статистические данные, проводимые в научных публикациях и официальных отчетах, а также факты, опубликованные в научной литературе и печати, законодательные и нормативные документы Российской Федерации.

Теоретическая значимость дипломной работы заключается в анализе взаимосвязи устойчивого развития РФ и кибербезопасности.

Структура дипломной работы определена целью и задачами исследования и состоит из содержания, введения, трех глав, заключения и списка использованных источников.

Первая глава посвящена исследованию теоретической сущности экономической устойчивости, рассмотрению подходов к определению понятия устойчивости, основных факторов, влияющих на нее.

Вторая глава носит практико-аналитический характер и содержит анализ состояния экономической устойчивости и кибербезопасности в РФ.

Третья глава содержит предложения и мероприятия по нейтрализации угроз устойчивости РФ, а также по нейтрализации угроз кибербезопасности

В заключение изложены основные выводы и результаты проведенного исследования, обеспечивающие достижение цели работы и решение поставленных задач.

Практическая значимость работы состоит в выработке предложений по совершенствованию инструментов, мероприятий, направленных на противодействие угрозам кибербезопасности РФ, которые могут быть использованы органами власти.

1 Теоретические аспекты исследования экономической устойчивости

1.1 Понятие и сущность экономической устойчивости

В соответствии с Указом Президента РФ от 13 мая 2017 года № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» экономическая безопасность – «состояние защищённости национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство её экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации» [40].

Основными суждениями, сопряженными с финансовой защищенностью, считаются:

– финансовая суверенность России – объективно имеющаяся автономность страны в проведении внутренней, а также внешней финансовой политики с учётом интернациональных обязательств;

– опасность финансовой защищенности – комплекс обстоятельств, а также условий, формирующих прямую либо непрямую вероятность нанесения вреда государственным интересам Российской Федерации в финансовой среде;

– вызовы экономической безопасности – комплекс условий, способных при конкретных обстоятельствах послужить причиной к появлению опасности финансовой защищенности;

– угроза в сфере экономической безопасности – вероятность нанесения вреда государственным интересам Российской Федерации в финансовой области во взаимосвязи вместе с реализацией угроз финансовой безопасности;

– гарантия экономической безопасности – осуществление органами общегосударственной власти, органами местного самоуправления а также Центрального банка Российской Федерации в содействии вместе с

институтами гражданского общества комплекса общественно-политических, координационных, социально-экономических, информативных, правовых а также других мер, нацеленных в противодействие вызовам а также угрозам финансовой защищенности а также защиту государственных интересов Российской Федерации в финансовой области.

Всемирное производство на нынешней стадии становления характеризуется усилением роли глобализации. Любое государство, как элемент всемирной системы экономики, заинтересовано в единстве, а также эффективной интеграции во всемирное сообщество. Все без исключения положительные факторы ускоренного обмена факторами производства бесспорны, однако имеется и негативная область – повышение связи государства с экспортной торговлей. Экономическая обстановка в условиях глобализации у государств разная. То, в какой степени государство находится под воздействием всемирного сообщества находится в зависимости с ее социально-экономическим формированием. Российская Федерация отнюдь не редкий случай, а напротив броский образец того, как процедура интеграции формирует финансовые трудности в стране.

Вопрос финансовой защищенности в обстоятельствах интернационализации экономики становится главным нюансом исследования финансовой политики Российской Федерации. Решение финансовых вопросов может быть только линией формирования и правильного функционирования правового механизма, дозволяющего осуществлять направленные, а также последовательные решения в сфере финансовых взаимоотношений, соответствующие условиям финансовой защищенности.

Основная роль концепции финансовой защищенности Российской федерации – способность регулировать возможными противоречиями интересов страны, сообщества, личности. Вместе с целью успешного управления следует классифицировать компоненты этой концепции, исследовать их, что даст возможность дать верную оценку, а также

осуществить анализ состояния экономики в микро– а также макроуровне, сформировать мероприятия по предотвращению опасностей [5].

Чтобы определить систему направлений обеспечения экономической безопасности России, её нужно разделить на части. Основными элементами экономической безопасности являются [10]:

1. Энергетическая безопасность. Она состоит в устойчивости поставок энергоносителей с целью удовлетворения потребностей экономики, а также оборонного комплекса. Энергетическая составная часть финансовой безопасности страны содержит в себе недопущение, обнаружение, а также активное уничтожение происшествий, какие имеют все шансы причинить вред формированию топливно-энергетического комплекса (ТЭК). Отечественная макроэкономика имеет топливно-сырьевую направленность. В настоящий период топливная индустрия никак не готова повысить размеры собственного продукта. Необходима новейшая, точная политика ТЭК, в какой основной ценностью считается предоставление экономической независимости государства. Энергетическая система государства в нынешних обстоятельствах рынка, конкурентноспособных взаимоотношений имеет необходимость в модернизировании, а также реформировании с учётом применения Российского, а также иностранного опыта. Кроме того, к количеству трудностей, оказывающих большое влияние на сокращение энергетической защищенности страны, относится изношенность основных фондов, масштабы приватизации сектора экономики, подъем аварийности в предприятиях ТЭК государства, стоимостное несоответствие в энергоносителях как внутренний, так и всемирный.

2. Продовольственная, а также сырьевая безопасность - снабжение продовольствием и сырьём в размерах, требуемых для успешного функционирования государственного хозяйства. Одна из главных трудностей снабжения продовольственной, а также сырьевой составляющей считается взаимозависимость государственного хозяйства от ввоза продовольственных, а также сырьевых ресурсов.

3. Технико-производственная защищенность содержит в себе предупреждение, а также недопущение отрицательных последствий в случае внешнеэкономических нарушений и внутренних потрясений государства, а также ориентирована на стабильную процедуру расширенного производства, удовлетворение социальной, а также оборонной потребности страны.

4. Автотранспортная составная часть – безопасная деятельность автотранспортного комплекса, охрана интересов личности, сообщества, страны в области автотранспортного комплекса от противозаконных действий.

Предоставление транспортной безопасности объектов автотранспортной инфраструктуры и автотранспортных средств возлагается на субъекты инфраструктуры. Правительственное контролирование, а также госнадзор в сфере обеспечения автотранспортной безопасности исполняется уполномоченным федеральным органом исполнительной власти в соответствии с законодательством Российской Федерации.

5. Управленческая безопасность предполагает собою комплекс умений, а также навыков, требуемых менеджерам для управления. Данные умения, а также мастерства разделяются в 2 категории:

– реализация управленческого цикла, направленного на успешное решение проблем, определение перспективных целей, рациональное планирование своей работы и работы своих подчиненных, чёткая постановка задач для подчиненных, недопущение текучести кадров, соблюдение режима и условий труда.

– коммуникативные функции – это умение общаться с людьми и подчинёнными, налаживание деловых контактов с партнёрами, различными организациями и государственными структурами, умение выслушать собеседника, контролировать свои эмоции, владение письменной и устной речью. В современном мире очень большое влияние на экономическую безопасность, определяется качеством управленческого потенциала и эффективностью управления.

6. Стабильность финансового роста, а также экономическая безопасность страны вероятна только при инвестиционном виде развития национального хозяйства. Отталкиваясь из этого, возникает вопрос инвестиционной безопасности страны. При данном в качестве главных элементов инвестиционной безопасности как правило рассматриваются 2 характеристики: инвестиционный риск, а также инвестиционные возможности. В данной взаимосвязи необходимо отметить, что Российская Федерация имеет огромный инвестиционный потенциал, осуществление которого сейчас еще замедляется существующим инвестиционным риском.

7. Демографическая защищенность тесным образом соединена с иными разновидностями государственной безопасности - финансовой, общественной, общественно-политической, природоохранной, информативной, правовой.

Демографическая защищенность обеспечивается конституционными законодательными мерами защиты, интересов личности, сообщества, а также страны от разных внешних и внутренних опасностей.

8. Экологическая защищенность:

– это события, процессы, воздействия, состояния, которые практически никаким образом не должны являться источником значительных потерь, причиняемым естественной среде, народам, а также целому населению земли;

– совокупность операций, которые гарантируют природоохранное равновесие во всемирном территориальном пространстве;

– совокупность качеств окружающей среды, при которых, с учётом допустимых нагрузок для биосферы, а также, принимая во внимание социальные, а также экономические факторы, гарантируется полноценная жизнедеятельность общества, учитываются и исключаются негативные исходы антропогенного воздействия для следующих поколений.

Экологическая защищенность считается одной из элементов не только лишь государственной, но и международной защищенности. Именно она устанавливает права человека на безопасную для здоровья находящуюся вокруг среду, а кроме того, гарантирует условия использования естественных ресурсов вместе с поддержкой регулировки техногенной деятельности. Природная защищенность определяет географические, а также природоохранные концепции абсолютно всех иерархических рангов.

9. Информационная защищенность – данное состояние безопасности информации, а также сохранение информационной инфраструктуры от непреднамеренных либо намеренных влияний природного, либо синтетического характера, которые имеют все шансы причинить недопустимый вред субъектам информационных взаимоотношений.

10. Научно-техническая безопасность предполагает собою положение безопасности значимых интересов сообщества, страны, личности от внешних а также внутренних опасностей, сопряженных с реализацией существующих либо новейших технологий в производственной деятельности, в том числе ресурсы и меры, гарантирующие степень развития технологий с целью предоставления суверенитета, социально-экономического развития страны а также его государственной защищенности.

Предоставление научно-технической защищенности подразумевает:

– в обстоятельствах интернационального распределения труда, научно-техническую независимость государства;

– целостность просветительной, промышленной, общегосударственной научно-технической политической деятельности;

– определение опасных технологий федерального уровня, а также реализацию приоритетных направлений формирования техники и науки;

– перестройку промышленности;

– модернизацию государственной научно-технической базы;

– руководство научно-техническим развитием, а также его информационное снабжение.

11. Экономическая защищенность Российской федерации – умение без помощи других реализовывать экономическую политику в согласовании с государственными интересами, создавать экономические потоки в таких размерах, какие нужны с целью исполнения национальных задач.

Условием предоставления экономической защищенности считается ослабление воздействия экономических упадков в социально-политическую, а также финансовую системы, предупреждение вывоза капитала за рубеж, устранение инцендентов при распределении государственных бюджетных денег, привлечение денег иностранных инвесторов.

Проанализированная система финансовой защищенности – это целая концепция, при помощи которой исполняется развитие социальных взаимоотношений в разных областях производства, потребления, распределения, нацеленных на развитие вещественных благ.

Едиными свойствами системы экономической защищенности считаются:

– целенаправленность;

– двойственность;

– регулируемость;

– повышение, т. е. умение саморазвиваться, быть автономной;

– инерционность;

– устойчивость;

– адаптивность.

С учётом нынешнего состояния Российской федерации позволительно акцентировать несколько «специальных» свойств:

– последовательность исторического формирования;

– устойчивость по отношению к воздействию из вне;

– защита природоохранной системы;

– разделение предметов безопасности;

– высоконаучность, применение, а также внедрение финансовых методов и исследований согласно обеспечению защищенности;

– передовое урегулирование и его разработка, применение разных альтернатив и информационное развитие.

Все вышеизложенное формирует основу для наиболее тщательного усовершенствования, а также оценивания, а затем и решения разных трудностей.

Процедура возведения системы финансовой защищенности содержит в себе 7 конструкций по главным критериям и суждениям.

В рамках построения и рассмотрения системы общегосударственной финансовой защищенности следует обнаруживать условия, создавать мероприятия защищенности, осуществлять экспертизы нормативных действий, муниципальных заключений согласно проблемам, затрагивающим финансовую защищенность Российской Федерации.

1.2 Факторы влияющие на экономическую устойчивость РФ

Концепция финансовой безопасности содержит в себе 7 конструкций, соответствующих главным ее категориям и суждениям [10]:

- теория национальной защищенности;
- государственные интересы Российской федерации в области экономики;
- угрозы в области экономики;
- индикаторы финансовой безопасности;
- пороговые показатели финансовой безопасности;
- организация экономической защищенности;

– правовое обеспечение финансовой защищенности.

Структуру финансовой защищенности допускается отобразить через уровни (организационная структура) а также виды (многофункциональная структура).

Заведено различать 5 уровней финансовой защищенности:

– международная (всеобщая, а также региональная);

– государственная;

– областная (внутри государства);

– организации (предприятия, компании);

– личности.

Уровень 1. Международная финансовая защищенность предполагает собой конкретное положение экономики, при котором совершается выгодное сотрудничество государств в решении как государственных, так и вселенских трудностей хозяйствования, независимость выбора, содействие в международном разделении труда. Из числа государств сформированы специализированные общества, с поддержкой которых гарантируется интернациональная финансовая защищенность, к примеру, Всемирная торговая организация либо Международно-валютный фонд. Партнерские договоры касательно независимого движения денежных средств, товаров, а также услуг, также представляют немаловажную роль.

Можно анализировать интернациональную экономическую защищенность как стойкое положение интернациональной системы, противостоящей внешним, а также внутренним угрозам, обеспечивающее при этом любой стране:

– свободные тенденции экономического развития;

– охрану от внешних опасностей, закрепленных международным правом;

– устойчивость к глобальным экономическим кризисам.

Системой, вызванной гарантировать интернациональную защищенность, считается Организация Объединённых Наций (ООН).

Уровень 2. Государственная безопасность – это финансовая система, характеризующаяся присутствием наращенного производства, устойчивостью валютной системы, рациональностью структуры внешней торговли, поддержанием на установленном уровне научного потенциала, формированием финансовых, а также правовых условий, которые ликвидируют криминализацию общества, обеспечением требуемого уровня жизни населения.

Несомненно, то что финансовая защищенность страны обусловливается, в первую очередь, состоянием производственных мощностей, а также социально-экономических взаимоотношений, масштабами применения достижений научно-технического прогресса в хозяйстве государства, текстурой внешнеэкономических взаимосвязей. В данной взаимосвязи возможно заявлять, то, что вещественную базу финансовой защищенности страны составляют сформированные производительные силы, умеющие гарантировать наращенное воспроизводство, а также цивилизованную жизнедеятельность людей.

Финансовая защищенность страны непосредственно сопряжена вместе с суждениями «развитие», а также «устойчивость» экономики. Формирование государственного хозяйства – одна из частей экономической безопасности. В случае если экономика не развивается, то у страны стремительно уменьшаются способности сопротивляемости отрицательным внешним, а также внутренним влияниям. Стабильность государственного хозяйства государства как общей системы значит надежность, а также безопасность ее компонентов, финансовых, а также координационных взаимосвязей между ними, умение переносить внутренние, а также внешние перегрузки. Несомненно, то, что к главным условиям финансовой защищенности государства, кроме того, принадлежат: ее географическое положение; резервы естественных ресурсов; производственный, а также аграрный потенциал; уровень социально-демографического формирования а также, в конечном итоге, качество государственного управления.

Уровень 3. Региональная финансовая безопасность.

Финансовая защищенность региона – совокупность мер, нацеленных на стойкое, непрерывное формирование, а также усовершенствование экономики региона, непременно предусматривающей механизм противодействия внешним а также внутренним угрозам.

Во внутренней структуре финансовой защищенности региона возможно выделить 3 основных блока.

1. Финансовая самостоятельность, что носит условный вид по причине экономико-политической зависимости региона от федерального центра и взаимосвязанности экономик субъектов Федерации. В данных обстоятельствах финансовая независимость значит возможность контролирования региональной власти региональных ресурсов (в рамках предоставленных федеральным центром возможностей); результат такого уровня изготовления, производительности а также качества продукции, который гарантирует ее конкурентоспособность а также дает возможность на равных принимать участие в межрегиональной а также интернациональной торговле, кооперационных отношениях а также обмене научно-техническими достижениями.

2. Устойчивость а также стабильность региональной экономики, допускающая охрану имущества в абсолютно всех ее конфигурациях; формирование достоверных условий а также гарантий с целью предпринимательской деятельности; подавление условий, способных ослабить обстановку (соперничество с преступными структурами в экономике, недопущение серьёзных разрывов в распределении прибыли, угрожающих спровоцировать общественные потрясения и т. д.).

3. Способность к саморазвитию, а также прогрессу – формирование подходящего атмосферного климата с целью инвестиций и инноваций, непрерывное усовершенствование изготовления, повышения профессионального, образовательного а также цивилизованного уровня развития сотрудников и т. д.

Обычно формирование (либо деградация) системы рассматривается в рамках довольно мягких и сравнительно устойчивых финансовых действий, описываемых связями, близкими к линейным. Но в следствии осуществлении внешних либо внутренних опасностей в системе никак не исключается появление упадка, т. е. условия переходного характера. Создание программы финансовой защищенности должно основываться на точном понимании нынешних опасностей, крайне разнообразных и обладающих различным уровень остроты. В качестве более основательных из них допускается отметить соответствующие: прогрессирующий упадок производства; распад научно-технического потенциала; деиндустриализация экономики; угроза потери продовольственной автономии; увеличение отсутствия работы, а также снижение рабочей мотивации; повышение наружного, а также внутреннего долга; криминализация экономики; повышение материальной дифференциации жителей и увеличение степени бедности; увеличение недостатка бюджета.

В комплексе мер, создающих концепцию финансовой защищенности региона, главную роль играет нейтрализация возникающих угроз. С позиций экономической безопасности немаловажно производить оценку, а также давать прогноз воздействия абсолютно всех прогнозируемых опасностей, кроме того, экономических и неэкономических влияний на их развитие, а основное – обнаруживать вероятность внезапного катастрофического регресса и опасного порога. В то же время вместе с прогнозно-аналитической появляется и противоположная цель, заключающаяся в исследовании, а также осуществлении системы мер, нацеленных на недопущение наступления упадка и на преодолевание опасного порога.

Уровень 4. Финансовая защищенность компании – положение субъекта хозяйствования, при котором совершается накапливание, а также интенсивное вложение денежных средств, стабильное увеличение основных показателей активности, усовершенствованное свойство управления, в том числе и

рисками, исполняются нововведения в сфере технологий и информационной основы.

Из числа вероятных опасностей финансовой защищенности компании возможно отметить 2 главных типа опасностей: внутренние (действия/бездействие работников, какие имеют все шансы дестабилизировать службу компании, потеря данных, трудности с партнерами и т. д.) а также наружные (преступная деятельность соперников а также индивидуальных лиц, несостоятельные партнеры, разнообразные преступления со стороны «власть имущих» должностных лиц).

При точной оценке возможностей появления угроз допускается использовать результативные методы профилактики, а также борьбы с этими трудностями, выстроив единую систему финансовой безопасности в компании. Из числа многофункциональных элементов финансовой защищенности возможно отметить экономическую, умственную, а также профессиональную, политико-правовую, природоохранную и силовую.

Для организации эффективной финансовой защищенности фирмы нужна специальная служба, работа которой ориентирована на исследование и исполнение предупредительных мероприятий по охране бизнеса, получение, а также сохранение данных о партнёрах и работниках компании, охрану информационной защищенности, исполнение защиты территории и собственности компании и другие сопутствующие задачи.

Уровень 5. Финансовая защищенность личности предполагает собою конкретное состояние жизнедеятельности, при котором существует как финансовая, так и законная охрана актуальных интересов при соблюдении конституционных прав и обязанностей. Финансовая защищенность личности непосредственно находится в зависимости от совокупного состояния экономики.

Индивид (личность), находясь непосредственно предметом, а также субъектом, системой безопасности, присутствует в абсолютно всех иных системах безопасности, представляя базисную системообразующую

значимость. Отсюда предоставление личной безопасности становится обстоятельством предоставления защищенности абсолютно всех иных ее форм, а также степеней, однако, в свою очередь, состояние личности обусловливается состоянием сообщества, страны, природы. Человек находится в фокусе абсолютно всех угроз, таким образом равно как от любых деструктивных социально-политических, природоохранных, народных и промышленных происшествий испытывает страдания непосредственно индивид.

Объектами экономической безопасности личности выступают граждане и общество, субъектами – потенциальные рабочие места, сфера социального обеспечения, материальное производство [3].

Предметом государственной деятельности в области экономической безопасности личности являются:

– анализ и синтез факторов, негативно влияющих на систему экономической безопасности человека;

– осуществление такой государственной экономической политики и институциональных сдвигов, которые элиминировали бы несовершенство социально – экономической политики.

Современному мировому сообществу характерны признаки многополярности. При этом процессы, происходящим в мировой экономике, сопровождаются нарастанием геополитической нестабильности, обострением глобальной конкуренции, перераспределением ресурсов новыми центрами экономического роста и политического влияния. Происходят существенные изменения в области международного права, военно-политической и экономической областях.

С целью оценки современной безопасности российского государства следует знать и понимать факторы, которые устанавливают степень экономической безопасности России. К таким факторам относятся:

– геополитическое и экономико-географическое положение России, и связанное с этим расположение производительных сил на территории государства, доступ к российским и иностранным ресурсам;

– экономическая и военно-политическая мощь России и её конкурентоспособные позиции в международной экономической концепции, согласно стратегически значимым видам экономической деятельности;

– ориентация институциональной системы страны на поддержание отраслей экономики, от которых зависит степень экономической безопасности;

– приоритеты экономической политики России в отношении общественно-экономической и экологической сферы, обеспечивающие результат международных стандартов качества жизни населения государства;

– параметры отраслевой и региональной структур валового внутреннего продукта, учитывающие стратегическую важность сфер национальной экономики и регионов государства с целью предоставления экономической безопасности;

– условия, определяющие принципы формирования национальной экономики в составе Всемирной торговой организации, и зависящие от этих условий структуры экспорта и импорта материальных благ первого и высшего порядков, а кроме того, нематериальных активов, причисленных к группе стратегической важности;

– наличие резервов стратегически важных материальных благ первого и высшего порядков в размерах, необходимых для обеспечения экономической безопасности в условиях непредвиденных обстоятельств. Аналогичные условия могут возникнуть вследствие обострения межгосударственных взаимоотношений, возникновения военных конфликтов и террористических действий, обострения конкурентной борьбы как внутри страны, так и за её пределами, истощение значимых ресурсов, появление стихийных бедствий и экологических катастроф в государстве и за границей.

1.3 Кибербезопасность как ключевой фактор обеспечения экономической устойчивости в современных условиях

В соответствии с Доктриной информационной безопасности РФ 2016 г. она рассматривается как состояние защищенности государства, общества, личности от внутренних и внешних информационных угроз.

При этом обеспечиваются: реализация прав и свобод индивидов, повышение и поддержание достойного уровня и качества жизни граждан, территориальная целостность, суверенитет, оборона и безопасность, устойчивое социально-экономическое развитие страны.

Систему обеспечения информационной безопасности РФ исследователи С. Е. Коротченко, М.Е. Листопад условно подразделяют на три блока. Во-первых, это правовая база; во-вторых, информационно-технический блок (программное и аппаратное обеспечение); в-третьих, экономический блок (разработка и совершенствование программ, средств, методов обеспечения информационной безопасности). Представляется, что эта структура должна быть дополнена и политическим блоком, таким как разработка стратегических ориентиров обеспечения этой сферы, взаимодействие с членами мирового сообщества по снижению негативного влияния ИКТ на мировое информационное пространство [5].

Важной задачей реализации российской национальной инновационной системы является ее интеграция в мировую экономику, в регионы, в которых имеются стратегические интересы для нашей страны.

С. Е. Коротченко, М.Е. Листопад справедливо выделяют следующие сферы российской экономике, наиболее подверженные воздействию информационных угроз: национальная система статистики; кредитно-финансовая система; системы автоматизации учета органов исполнительной власти; российские предприятия, учреждения, организации, в том числе реализующие финансовые, биржевые, таможенные сделки.

По оценкам аналитического центра «TAdviser», по итогам 2020 года объем российского рынка информационной безопасности составил 109 млрд руб. и вырос на 8 %. Лидером отечественных компаний в области обеспечения информационной безопасности продолжает оставаться «Лаборатория Касперского». В пятерку компаний также входят «Acronis», «Софтлайн», «Информзащита», «Оптима». Данные РБК свидетельствуют, что засекреченная часть российского бюджета в 2022 году останется на отметке в 17,61 % от общих расходов государственной казны. Доля закрытых расходов по разделу «Национальная безопасность и правоохранительная деятельность» увеличится до 38,27 % - максимума с 2007 года, но это будет компенсировано сокращением секретных частей «гражданских» разделов – «Национальная экономика» и «Общегосударственные вопросы» [14].

Секретные расходы по разделу «Национальная оборона» в 2022 году останутся на уровне чуть ниже 66 %, как и в 2021-м (это единственный раздел бюджета, в котором секретных расходов больше, чем несекретных). Закрытые ассигнования увеличились по подразделу «Другие вопросы» национальной обороны: если в 2021 году их доля ожидается на уровне 59% (по показателям сводной бюджетной росписи), то в 2022 году запланирован 71 %. В федеральном бюджете есть подразделы, засекреченные на 100 % или почти на 100 %. Это ядерно-оружейный комплекс (раздел «Национальная оборона»), где никогда не было открытых расходов; подразделы «Органы пограничной службы» (100 %) и «Органы безопасности» (99,8%), к последним относятся ФСБ, ФСО, Федеральная служба по техническому и экспортному контролю (ФСТЭК) [14].

Необходимо выделить предпринимаемые в последнее время множественные усилия большого количества автономных аналитических фирм оценки информационной безопасности как отдельной финансовой категории. При этом главной задачей выдвигается установление основных характеристик, а также систематическое исследование взвешенной оценки информационной защищенности. Из года в год замечается увеличение

финансирования в рамках предоставления информационной защищенности, то что обуславливается увеличением вреда от утраты данных.

Таким образом, на сегодняшний день более острой задачей в сфере предоставления защищенности в информационной области считается сохранение большой информации касательно индивидуальных сведений граждан государств, какие они предоставляют в глобальной сети Интернет.

Опасности кибербезопасности Российской Федерации:

– увеличение иностранными государствами способностей информационно-технического влияния на информационную инфраструктуру в военных целях.

– увеличение масштабов применения специальными службами отдельных стран средств оказания информационно-психологического влияния, сосредоточенного на дестабилизацию внутриполитической, а также общественной ситуации в разных регионах общества приводящего к подрыву суверенитета, а также патологии территориального единства других стран

– применение террористическими, а также экстремистскими учреждениями элементов информационного влияния на индивидуальное, массовое, а также социальное понимание в целях формирования межэтнической общественной напряженности, разжигания народной, а также религиозной злобы или вражды, пропаганды экстремистской идеологии, а кроме того привлечения к террористической деятельности новых приверженцев.

– увеличение компьютерной преступности, в первую очередь в кредитно-финансовой области, увеличение количества правонарушений, сопряженных с нарушением прав, а также свобод лица и гражданина, в том числе в доли, касающейся неприкосновенности личной жизни, индивидуальной и семейной тайны, при обработке личных сведений вместе с применением информационных технологических процессов.

Персональные данные пользователей выступают своего рода параметрами, по которым можно оценивать состояние и динамику развития

общественных систем, находить уязвимые места и оказывать на них давление. Отсюда вытекает, что информация носит глобальный характер. А персональные данные можно использовать в различных целях, в том числе и с целью накопления и последующего использования информации для проведения пропаганды.

В различных международных соглашениях выделяется триада, источники международных информационных угроз: террористические группы, киберпреступники, государства. Следует подчеркнуть, что в рамках ООН неоднократно рассматривались вопросы борьбы с киберпреступностью. Резолюция ГА ООН (4.12.2000) раскрывает основные направления борьбы с киберпреступлениями: обязанность стран обеспечивать на уровне национального законодательства борьбу с этими правонарушениями; кооперация с правоохранительными органами при расследовании использования ИКТ в преступных целях; судебное преследование с координацией на мировой арене всеми государствами. Принятие в 2001 г. Советом Европы Конвенции по киберпреступности стало воплощением этих направлений. Однако поскольку Конвенция была разработана ограниченным числом представителей из западных стран, она имеет особенность, связанную с реализуемым подходом обеспечения кибербезопаности [27].

В ст. 32 (в) Конвенции присутствует положение, предусматривающее возможность проводить следственные мероприятия в сфере информационной инфраструктуры страны без наличия на это ее согласия. Данное положение сделалось преградой в ратификации Конвенции отдельными государствами. Таким образом, к примеру, Российская федерация не поставила подпись на данную конвенцию, не были согласованы приемлемые для Российской Федерации требования трансграничного допуска к компьютерным системам. Но Российская федерация рекомендовала собственный план кибербезопасности, поясняющий то, то что на нынешней стадии «регулирование» не включает в надлежащем объёме взаимоотношения в сфере киберпространства как элемента информационного пространства.

Следует подчеркнуть, что формирование и развитие мирового информационного пространства привело к наращиванию геополитического влияния путём использования ИКТ с целью информационного воздействия на массовое сознание, общественный и государственный порядок в разных странах, например, для смены в них политического режима.

Сегодня США предпринимают значительные усилия для преобразования информационного пространства «под себя», в среду, создающую возможности свободной реализации преимуществ ИКТ для обеспечения своих национальных интересов. Другими словами, США стремятся сохранить контроль над управлением Интернетом, рискуя лишиться свободного доступа в информационное пространство других стран, потерять политическое и экономическое влияние.

На сегодняшний день опасности, которые объединены с применением ИКТ в военно-политических, а также военно-стратегических целях отталкиваются из мирового информационного пространства. В минувшие года они стали сильным дестабилизирующим условием, которое устанавливает нацеленность интернациональных взаимоотношений.

Основными факторами, оказывающими воздействие на совершение киберпреступлений экономического характера, являются [51]:

– экономический кризис,

– повышение цен на товары первой необходимости,

– повышение уровня безработицы.

Основными источниками преступлений, совершаемых в киберпространстве, являются:

– незаконная предпринимательская деятельность,

– незаконная банковская деятельность,

– организация, проведение азартных игр.

Интернет, помимо площадки незаконной деятельности, являет собой место для легализации денег, полученных преступным путем. Всемирная сеть и образованное ею киберпространство создали единственную среду и

уникальные условия для осуществления преступной деятельности (легализация денежных средств, полученных преступным путём, получение быстрого и стабильного дохода).

Легализация денежных средств в киберпространстве создаёт трудности в правоприменительной практике, и это, в свою очередь, приводит к необходимости совершенствования законодательства.

В совокупность способов легализации денежных средств, полученных в результате совершения киберпреступления входят: использование социальных сетей, помимо данных средств злоумышленник может открывать собственные сайты разной направленности, а также использовать уже существующие интернет-банки, криптовалюту биткоин.

Таким образом, для легализации денег используются привычные операции, которые может совершать любой человек.

Одним из распространённых способов легализации денежных средств является продажа несуществующего имущества через сайты-объявления.

Преступник создаёт несколько аккаунтов на сайте, регистрируясь под разными именами с разных адресов, и выставляет на сайте различные товары. Далее в качестве покупателя использует денежные средства, полученные преступным путём. Метод проиллюстрирован на рисунке 1.

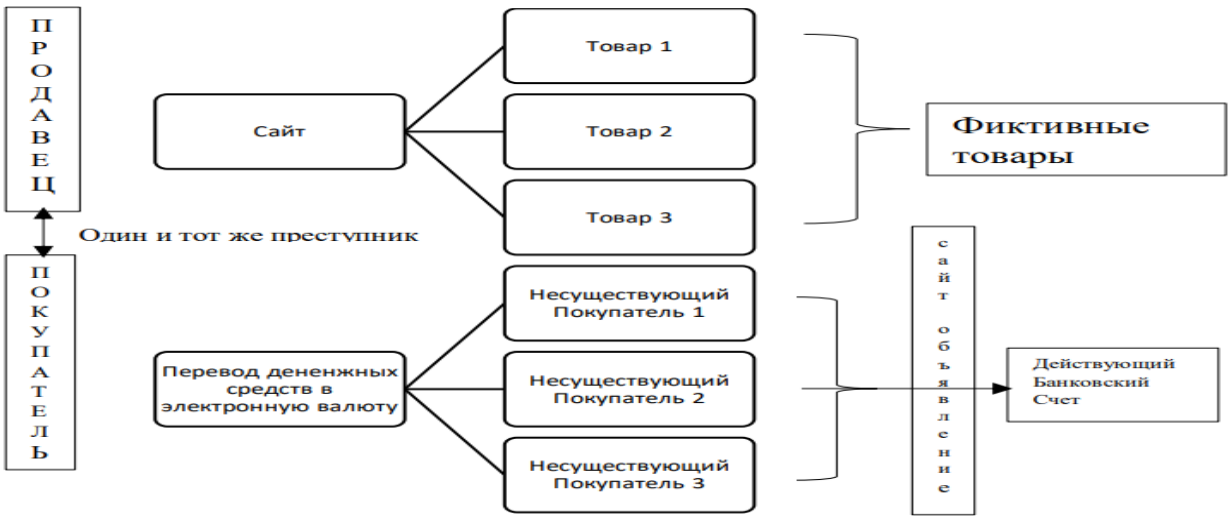

Рисунок 1 – Схема продажи несуществующего имущества (составлено автором)

Во-первых, правонарушитель переводит деньги в электронную валюту на заранее созданные ложные аккаунты электронных денежных систем. Во-вторых, переводит деньги с этих аккаунтов на электронные кошельки якобы различных покупателей. В-третьих, злоумышленник от имени каждого «ложного покупателя» покупает несуществующие товары, которые он же и выставил на продажу в качестве продавца. В результате осуществления этой схемы полученные деньги переводятся на действительный банковский счет. В качестве подтверждения легальности полученного дохода может быть предоставлена выписка из истории покупок сайта или иные документы, свидетельствующие о правомерном характере дохода.

Вместе с возникновением новейших технологий прослеживается возникновение новейших, наиболее непростых видов преступности. Это указывает о том, что правонарушители довольно быстро применяют итоги научно-технического прогресса в собственных целях. Эта направленность предполагает значительную опасность абсолютно всем социальным взаимоотношениям, складывающимся в киберпространстве, так как на этой стадии формирования киберпространство и социум уже неразрывны. Основными факторами, а также критериями жизни финансовой киберпреступности считаются неизвестность пользователей киберпространства, а также неизвестность информативных сетей, промышленное несовершенство, а кроме того небольшой уровень информационной защищенности людей. Правоохранительным органам становится известна только небольшая доля совершаемых финансовых киберпреступлений.

2 Опенка состояния экономической устойчивости в РФ

2.1 Оценка и анализ действующего состояния экономической устойчивости РФ

В стратегии экономической безопасности Российской Федерации до 2030 года указаны 40 показателей состояния экономической безопасности. Некоторые из этих показателей показали положительную динамику.

Рост ВВП определил рост такого показателя как индекс физического объёма ВВП (таблица 1).

Таблица 1 – Показатели ВВП в динамике за 2017–2021гг. [42]

Показатель	2017	2018	2019	2020	2021
ВВП (в текущих ценах, млрд. руб.)	91843	103862	109608	107390	131015
Индекс физического объема ВВП (в % к предыдущему году)	101,8	102,8	102,2	97,3	104,7
ВВП на душу населения (по ППС), тыс. руб.	625,5	707,4	746,8	733,2	898,2
Индексы физического объема валового внутреннего продукта на душу населения (в процентах к предыдущему году)	101,7	102,8	102,2	97,5	105,2
Мировой ВВП, трлн долл. США	80,14	84,74	87,27	85,24	96,29
ВВП РФ, трлн руб.	91 843,2	103 861,7	109 608,3	107 315,3	131 015,0
Доля в мировом ВВП, %	1,15	1,23	1,26	1,26	1,36

Фактически индекс физического объёма ВВП увеличился за последние пять лет на 42,4%, его рост за последний год может говорить как о постепенном выходе российской экономике из кризиса, так и о её стагнации.

Положительная динамика и у валового внутреннего продукта на душу населения (по паритету покупательной способности) (таблица 1) – это макроэкономический показатель, который позволяет более точно отразить состояние отечественной экономики, так как он рассчитывается путем преобразования ВВП в международные доллары на основе паритета покупательной способности (ППС) разделённый на численность населения

страны.

То есть покупательная способность – это отношение денежных единиц одной страны, которые нужны для приобретения такого же количества продуктов, на которое можно приобрести на одну денежную единицу другой страны.

Для расчёта обычно используется доллар США, как базовая и расчётная валюта.

Динамика ВВП на душу на селения (по ППС) внушает оптимизм, и может свидетельствовать о росте экономики РФ.

Незначительный рост и у доли российского валового внутреннего продукта в мировом валовом внутреннем продукте (таблица 1).

Этот показатель не имеет ярко выраженной негативной динамики, однако, снижения энергоёмкости ВВП происходит крайне медленно. И задача поставленная Президентом РФ в 2008 году снизить этот показатель к 2020 году на 40% от уровня 2007 года, может быть не выполнена.

Низкие темпы снижения энергоёмкости ВВП подтверждает и министр энергетики России А.В. Новак: «Однако в целом за период с 2008 г общее снижение получается достаточно скромным – 13%, это ниже запланированных цифр».

Кризис мировой экономики в целом и российской экономики в частности, а также санкционное давление на Российскую Федерацию привело к тому, что за последние 5 лет доля российского ВВП в мировом ВВП сократилась на 0,21%.

За анализируемый период доля ВВП РФ в мировом ВВП не превышает 1,5%.

Стабилизация российской экономики определила положительную динамику доли инвестиций в основной капитал в валовом внутреннем продукте (таблица 2).

Таблица 2 – Инвестиционно-производственные показатели основного капитала [42]

Показатель	2017	2018	2019	2020	2021
Инвестиции в основной капитал, млрд. руб.	16027,3	17782,0	19329,0	20302,9	22945,4
% к предыдущему году	104,8	105,4	102,1	99,5	107,7
доля инвестиций в основной капитал в ВВП, %	21,4	20,0	20,6	21,8	21,9

Доля инвестиций в основной капитал в валовом внутреннем продукте в России в течении длительного времени находится на уровне 20%, это средний показатель среди стран мира, но необходимо стремиться к показателям стран – лидерам стран экономического роста.

Значительная положительная динамика у одного из важнейших социально-экономических показателей экономической безопасности России – это уровень инфляции (таблица 3).

Таблица 3 – Уровень инфляционно-внешнедолговых значений [35]

Показатель	2017	2018	2019	2020	2021
Уровень инфляции, %	102,5	104,3	103,0	104,9	108,4
Внешний долг РФ, млн. долл	51 211,8	49 827,3	49 156,5	54 848,3	56 702,9
в т. ч. по государственным гарантиям Российской Федерации в иностранной валюте:	17 596,6	13 252,8	11 567,4	10 357,2	11 730,5

С целью сдерживания инфляционных ожиданий Банк России снизить ключевую ставку до 14,0% (по данным на 14 мая 2022 года), что свидетельствует о постепенном выходе российской экономики из кризиса. Всего же за анализируемый период ключевая ставка Банка России колебалась от 10 до 20%. Увеличение внешнего долга Российской Федерации на 10,7% (таблица 3) за анализируемый период нельзя считать негативной динамикой, так как его увеличение из-за положительной курсовой переоценки, которая связана с ослаблением американского доллара к рублю. В тоже время государственный внешний долг не превысил, установленный в бюджете на 2022 год предел в 60 млрд. долларов.

Рост таких показателей как доля инновационных товаров, работ, услуг в общем объеме отгруженных товаров, работ, услуг (таблица 4) и доля высокотехнологичной и наукоемкой продукции в валовом внутреннем продукте (таблица 4) свидетельствует об улучшении в сфере науки и инноваций.

Таблица 4 – Доля инновационных товаров в общем объеме отгруженных товаров [35]

Показатель	2017	2018	2019	2020	2021
Объем инновационных товаров, млрд. руб.	57 611,1	68 982,6	92 253,9	91 296	-
Доля инновационных товаров в общем объеме, %	7,2	6,5	5,3	5,7	-
Доля высокотехнологичной и наукоемкой продукции в ВВП, %	21,1	21,8	21,3	22,0	22,1
Инвестиции всего, млрд. руб.	13450,2	13902,6	13897,2	14639,8	12025,6
В машины и т.п., млрд. руб.	5212,8	5052,0	4375,1	4480,7	4066,8
Доля инвестиций в машины, %	38,8	36,3	31,5	30,6	33,8

Увеличение доли инвестиций в машины, оборудование и транспортные средства в общем объеме инвестиций в основной капитал (таблица 4) вызвано снижением общего объема инвестиций в основные средства.

Не может не вселять оптимизм положительная динамика снижения дефицита федерального бюджета, в том числе нефтегазовый дефицит федерального бюджета (таблица 5), также следует учитывать то, что дефицит бюджета на 2021 год планировался на уровне 2008,09 млрд. рублей.

Таблица 5 – Дефицит федерального бюджета и золотовалютных резервов РФ [35]

Показатель	2017	2018	2019	2020	2021
Дефицит федерального бюджета, млрд. руб.	323,0	334,7	1961,0	2956,4	1336,37
В т.ч. нефтегазовый дефицит, млрд. руб.	6857,0	7768,5	7823,7	7800,4	5840,2
Золотовалютные резервы, $млн.	515590	418880	364708	385288	431636
Объем импорта, $млн.	341269	307875	193021	191588	205300
Отношение, %	1,51	1,36	1,89	2,01	2,10

Рост золотовалютных резервов РФ обеспечил положительную динамику такому показателю как отношение золотовалютных резервов Российской Федерации к объему импорта товаров и услуг (таблица 6).

Таблица 6 – Индексы экспортно-импортной деятельности [42]

Показатель	2017	2018	2019	2020	2021
Объем экспорта РФ, $млн.	521835	496806	341419	281850	321000
Индекс физического объема экспорта, %	98,94	95,2	68,72	82,55	113,89
Объем импорта, $млн.	341269	307875	193021	191588	205300
Индекс физического объема импорта, %	101,63	90,22	62,7	99,26	107,16
Сальдо торгового баланса, $млн.	+180566	+188931	+148513	+90262	+116108
Коэффициент покрытия импорта экспортом, %	152,91	161,36	176,88	147,11	156,36
Импорт всего, $млн.	315298	287063	182718	182267	205000
Импорт машин и т.п., $млн.	152773	136580	81868	86059	104960
Доля машин и т.п. в общем объеме импорта, %	48,5	47,6	44,8	47,2	51,2
Доля импорта в объеме товарных ресурсов продовольственных товаров, %	36	34	28	23	22
Экспорт машин и т.д., $млн.	28841	26495	25440	24432	28069
Доля машин и т.д. в общем объеме несырьевого экспорта, %	5,5	5,3	7,4	8,6	7,9
Доля организаций, осуществляющих технологические инновации, %	8,9	8,8	8,3	7,3	8
Индекс производства по виду экономической деятельности «Добыча полезных ископаемых»,%	101,1	101,4	100,3	102,5	102,0

Положительную динамику, не смотря на санкционное давление на Россию, имеют такие внешнеэкономические показатели экономической безопасности как индекс физического объема экспорта, индекс физического объема импорта и сальдо торгового баланса. Увеличение доли машин, оборудования и транспортных средств в общем объеме импорта говорит о модернизации промышленности РФ, а снижение доли импорта в объеме товарных ресурсов продовольственных товаров свидетельствует об импортозамещении на рынке продовольствия.

В 2021 году наблюдалось снижение доли машин, оборудования и транспортных средств в общем объеме не сырьевого экспорта.

Причинами негативной динамики этих показателя являются как общее снижение инвестиционной активности, так и недостаточное развитие отечественного рынка машин оборудования и транспортных средств, что в период санкционного давления сказывается на этом показателе.

Негативной можно считать динамику такого показателя как доля организаций, осуществляющих технологические инновации.

По данным Высшей школы экономики и Росстата, сегодня в России технологическими инновациями занимается не более 8 % предприятий, тогда как данный показатель в Восточной Европе находится на уровне 25-30 %, а в Западной Европе составляет более 40-50 %.

Незначительное снижение индекса производства по виду экономической деятельности «Добыча полезных ископаемых» не может свидетельствовать о негативной динамике этого показателя.

Такой показатель, как доля прироста запасов полезных ископаемых (по стратегическим видам полезных ископаемых) в общем объеме погашенных в недрах запасов не может быть проанализирован, так как расчёт данного показателя и его пороговые значения определяются в соответствии с Указом Президента Российской Федерации от 31.12.2019 № 684 «Об оценке и государственном мониторинге состояния национальной безопасности Российской Федерации», который отсутствует в открытом доступе.

Индекс денежной массы (денежные агрегаты М2) – это показатель изменения наличных денег, чеков, вкладов до востребования и срочных вкладов (таблица 7).

Таблица 7 – Динамика денежной массы (денежные агрегаты М2) [42]

Показатель	2017	2018	2019	2020	2021
Наличные деньги(М0), млрд.руб.	6430,1	6985,6	7171,5	7239,1	7714,8
Денежная масса (М2), млрд. руб.	27164,6	31155,6	31615,7	35179,7	38417,9
Удельный вес М0 в М2, %	23,7	22,4	22,7	20,6	20,1
Индекс денежной массы, %	112,2	114,7	101,5	111,3	109,2

Увеличение денежной массы при снижении инфляции может свидетельствовать как о росте доверия населения к финансовым рынкам государства и к национальной валюте, так и то, что рост денежной массы сопровождает рост ВВП. И то и другое свидетельствует о развитии экономики и увеличению инвестиционного спроса на деньги.

Подводя итог, стоит отметить, что положительная динамика прослеживается только у половины показателей экономической безопасности Российской Федерации указанных в «Стратегии экономической безопасности». Стоит отметить такой показатель как уровень инфляции, который в 2021 году составил 8,4 %, и оказывает непосредственное негативное влияние на социально-экономическую сферу. Стабильную положительную динамику имеют показатели, относящиеся ко внешнеэкономической деятельности и оборот розничной торговли, которые сигнализируют об уменьшении влияния санкционного давления на российскую экономику.

2.2 Анализ состояния кибербезопасности РФ

Вопросы кибербезопасности в нашей стране стоят особенно остро, в частности, потому, что нет ее досконально прописанной правовой основы. Практически, систематизированного подхода к внутри российской кибербезопасности в настоящее время нет. Например, не прописаны подробно и не подкреплены конкретными законами вопросы своевременной и адекватной реакции на преступные по своей сути действия в компьютерных сетях, применение Интернета в преступных целях. Хотя эти преступления как правило представляют собой только прелюдию к совершению реальной кражи или мошенничества.

Так, для Российской Федерации вопрос кибербезопасности является особо актуальным. Для того чтобы отразить реальное состояние кибербезопасности страны следует провести аналитические исследования.

Для начала следует выделить ряд критериев, по которым мы будем оценивать состояние кибербезопасности. Отразим эти показатели на рисунке 2.

Рисунок 2 – Показатели, характеризующие кибербезопасность в России (составлено автором)

Для начала следует проанализировать такой показатель, как объекты кибератак.

Объекты кибератак представляют собой категории организаций, которые подвергались воздействию киберпреступлений.

Отразим объекты на рисунке 3.

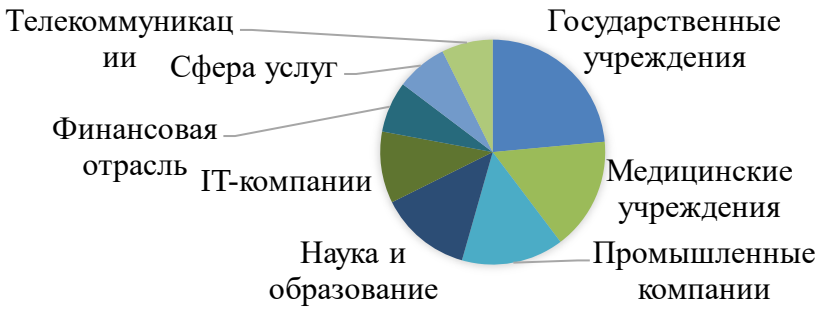

Рисунок 3 – Объекты, подвергаемые киберугрозам по состоянию на 2021г., % [31]

Таким образом, мы видим, что основную часть объектов киберугроз составляют государственные учреждения. Далее идут медицинские организации и учреждения науки и образования. Влияние кибератак на государственные учреждения наблюдаются чаще всего. Данный факт можно связать с тем, что исполнителями являются кибернаемники иностранных государств.

На государственные структуры чаще всего направлены такие атаки, как:

– фишинг;

– эксплуатация уязвимости веб-приложений, находящихся в доступе в сети интернет;

– взлом инфраструктуры подрядчиков.

Далее проанализируем количество киберпресуплений. Отразим этот показатель в динамике за 2019–2021гг.

Таблица 8 – Количество киберпреступлений в динамике за 2019–2021 гг. [29]

Показатель	2019	2020	2021
Количество киберпреступлений, тыс.	287 778	510 748	518 000

Оценка количества преступлений была проведена на основе возбужденных уголовных дел, связанных с информационными технологиями. Как видно из данных таблицы 8, за рассматриваемый период количество киберпреступлений увеличилось в 1,8 раза, что является крайне негативной динамикой и говорит о том, что снижает уровень информационной безопасности в стране.

На наш взгляд, такое увеличение киберпреступлений связано с тем, что участились случаи телефонного мошенничества.

Далее проанализируем нормативно-правовую базу киберпреступности. Она представлена документами разного уровня, регулирующими киберпреступность и кибертерроризм.

Представим уровни документации на рисунке 4.

Рисунок 4 – Нормативно-правовые акты, регулирующие киберпреступность (составлено автором по материалам [26])

Данные категории нормативно-правовых актов представлены следующими документами:

– Гражданский кодекс РФ;

– Уголовный кодекс РФ;

– Кодекс РФ об административных правонарушениях;

– Закон РФ от 27.12.1991 г. № 2124–1 «О средствах массовой информации»;

– Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

– Перечень сведений конфиденциального характера. Утвержден Указом Президента РФ от 6 марта 1997 г. № 188;

– Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при

использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– Указ Президента РФ от 5 декабря 2016 г. № 646 «Доктрина информационной безопасности Российской Федерации»;

– Распоряжение Правительства Российской Федерации от 22 октября 1999 г. № 1701 -р «О мерах по усилению борьбы с преступлениями в сфере высоких технологий»;

– Постановление Правительства РФ от 23 января 2006 г. № 32 «Правила оказания услуг связи по передаче данных»;

– Положение о создании, развитии и эксплуатации аналитической информационной системы обеспечения открытости деятельности федеральных органов исполнительной власти, размещенной в информационно-телекоммуникационной сети «Интернет» (www.programs.gov.ru). Утверждено постановлением Правительства РФ от 23 июля 2015 г. № 748;

– Приказ ФСБ России, Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. № 416/489 «Требования о защите информации, содержащейся в информационных системах общего пользования»;

– Конвенция о компьютерных преступлениях и Дополнительный протокол к Конвенции о компьютерных преступлениях, касающийся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы, 2001 г.;

– Соглашение о сотрудничестве в области обеспечения международной информационной безопасности, 2010 г. и т. д.

Таким образом, мы видим, что перечень нормативно-правовых актов, регламентирующих защиту от киберпреступлений достаточно широк, что говорит о высоком уровне регламентации защиты от киберпреступлений.

Далее рассмотрим данные, которые наиболее часто подвергаются воздействию кибератак.

Отразим их на рисунке 5.

Рисунок 5 – Информация, которая чаще всего подвергается воздействию кибератак в России на 2021г. (составлено автором по материалам [31])

Таким образом, мы видим, что чаще всего злоумышленников интересует информация, связанная с персональными данными, а также учетные данные и данные, связанные с коммерческой тайной.

Также, немаловажным является сравнение показателей киберпреступности в России и в мире.

Так, в таблице 9 отразим темпы роста кибератак в разных странах по состоянию на 2021 год.

Таблица 9 – Темпы прироста кибератак в разных странах по состоянию на 2021г. [51]

Показатель	Темпы прироста, %
Россия	54
Африка	15
Азиатско-Тихоокеанский регион	20
Латинская Америка	37
Европа	65
Северная Америка	57

Так, как видно из данных таблицы 9, в России не самые высокие темпы прироста количества кибератак, тем не менее, этот показатель достаточно высок. Показатель выше, чем в России наблюдается в Северной Америке и в

Европе. Основной причиной такого прироста можно назвать пандемию коронавируса и переход работы на удаленный формат.

На данный момент наблюдается рост киберпреступлений в части криптовалюты. Так как появился новый мотив – кража криптоденег.

Также, рост киберпреступности связан и с тяжелыми внешнеэкономическими отношениями России и других стран. Государственные органы России становятся главной мишенью для иностранных наемников.

Таким образом, мы видим, что состояние кибербезопасности России находится не на таком высоком уровне. Количество киберпреступлений растет, темпы роста атак также выросли. Несмотря на достаточно широкую нормативно-правовую базу регулирования киберпреступности в России, ее влияния оказывается недостаточно. Большинство киберпреступлений совершается в отношении государственных органов. Объектом чаще всего являются персональные данные. Если говорить о сравнении показателей России и мира, то мы видим, что показатели роста киберпреступлений за последний год в России находятся на высоком уровне. Выше этих показателей только значения Европы и Северной Америки.

Влияние кибербезопасности на устойчивость страны прямо отражается через ее основные показатели, например через уровень преступности в части кибербезопасности, также, кибератаки на государственные органы влияют на эффективность их работы, что также снижает финансовую устойчивость. Также, кибератаки на физические лица могут косвенно снижать уровень жизни населения и финансовую устойчивость как следствие.

3 Направления повышения экономической устойчивости РФ

3.1 Основные направления рисков и угроз устойчивого развития страны, а также предложения по их нейтрализации

Устойчивое развитие страны зависит от степени влияния основных рисков и угроз.

Угрозы устойчивого развития страны представлены большим спектром и зависят от составляющих национальной безопасности.

Так, на рисунке 6 отразим основные направления угроз развития страны.

Рисунок 6 – Основные направления угроз устойчивого развития угроз страны (составлено автором по материалам [10])

Так, начнем с технологических угроз. В целом технологическая безопасность представляет собой состояние развития научно-технического потенциала страны, следовательно, технологические угрозы будут неразрывно

связаны с нарушением развития данного сектора. Так, в качестве основных технологических угроз можно выделить:

– нарушение прав страны на промышленную и интеллектуальную собственность;

– утечка высоких технологий, передовых научных технологий;

– отсутствие квалифицированных кадров;

– значительное отставание в части инноваций от зарубежных стран и т. д.

Далее рассмотрим технико-производственные угрозы. В целом технико-производственная безопасность представляет собой возможность экономики страны компенсировать негативное воздействие от внешнеполитических потрясений, то есть осуществлять расширенное воспроизводство, находить альтернативу импортных товаров, а также создавать новые воспроизводства в сжатые сроки.

Среди основных технико-производственных угроз можно выделить:

– монополизация производственной сферы;

– дефицит оборотных средств;

– износ основных фондов;

– высокая зависимость производства от импорта комплектующих;

– осуществление производства без учета меняющегося спроса.

Далее рассмотрим минерально-сырьевые составляющие угроз для устойчивого развития страны. Данный вид безопасности предусматривает обеспеченность страны важнейшими видами сырья и минералов, которые позволят создать устойчивую систему функционирования национальной экономики страны.

Угрозы материально-сырьевой сфера обуславливаются, чаще всего, естественными условиями. Так, основными проблемами материально-сырьевой безопасности могут быть:

– недостаточный уровень обеспеченности государства сырьевыми ресурсами;

– ограниченные сроки исчерпания полезных ископаемых и т. д.

Далее рассмотрим энергетические угрозы устойчивому развитию Российской Федерации. Данный вид угроз влияет на энергетическую безопасность, которая характеризуется достаточный уровень обеспеченности страны энергоносителями. В РФ данная проблема не является актуальной, так как наша страна является одним из мировых лидеров по поставкам энергоносителей, тем не менее, актуальным является адаптация цен к новым мировым.

Так, среди основных угроз энергетической безопасности можно увидеть:

– изношенность основных фондов;

– отличия во внутренних ценах на энергоносители и в мировых ценах;

– недостаточность открытия новых месторождений;

– недостаточная конкурентоспособность отдельных топливных ресурсов и т. д.

Валютно-кредитные угрозы подрывают финансовую безопасность страны, происходят нарушения в устойчивом функционировании финансово-валютной системы.

В качестве основных угроз выделим:

– недостаточность инвестиций в экономику страны;

– ускорение темпов роса цен;

– введение финансовых санкций и т. д.

Далее идет продовольственная составляющая угроз устойчивого развития страны. Данный вид угроз влияет на продовольственную безопасность, которая характеризуется наличием достаточного количества продовольствия, необходимого для эффективного функционирования национального хозяйства.

Среди основных продовольственных угроз можно увидеть:

– низкий уровень доходов населения;

– рост уровня инфляции

– низкие темпы технической оснащенности агропромышленного комплекса;

– изменение курса национальной валюты;

– зависимость АПК от импорта семян и т. д.

Далее рассмотрим информационные угрозы. Данный вид угроз является наиболее актуальным в рамках рассматриваемой работы. Так, в качестве основных угроз информационной безопасности можно выделить:

– неправомерный доступ к конфиденциальной информации;

– преднамеренное изменение данных, имеющих статус конфиденциальности;

– ограничение возможности получения доступа к информации информационных систем.

В современных условиях огромное влияние оказывает уровень кибербезопасности в стране.

В связи с этим устранение угроз кибербезопасности будет являться важнейшим направлением политики государства. К основным киберугрозам относят фишинг, то есть неправомерное получение конфиденциальной информации, баз данных. Помимо фишинга угрозой являются и атаки со стороны программ-вымогателей. Такие программы буквально похищают базы данных, в том числе государственных органов с целью получения выкупа. Еще одной киберугрозой, требующей нейтрализации является криптоджекинг, то есть захват компьютера с целью майнинга криптовалюты. Все виды киберугроз оказывают огромное влияние на развитие устойчивости страны, в связи с чем они требуют незамедлительного устранения.

Демографические угрозы влияют на стабильность численности населения страны. Основными демографическими угрозами являются:

– снижение уровня рождаемости и повышение уровня смертности;

– низкий уровень жизни населения;

– эпидемиологические проблемы, влияющие на здоровье населения;

– низкий уровень экологии страны и т. д.

Далее рассмотрим социальные угрозы. Среди основных социальных угроз можно выделить:

– глубокая дифференциация доходов общества;

– увеличение числа бедного населения;

– рост уровня безработицы в стране;

– кризис образовательной системы, а также системы здравоохранения;

– увеличение количества потребления алкоголя, наркотиков и т. д.

Далее рассмотрим экологические угрозы устойчивого развития Российской Федерации, которые могут стать причиной нанесённого ущерба национальной безопасности страны.

Основными экологическими угрозами являются:

– изменение климата из-за выброса вредных химикатов;

– нарушение озонового слоя земли;

– загрязнение морской среды и т. д.

Далее рассмотрим информационные угрозы. Данный вид угроз является наиболее актуальным в рамках рассматриваемой работы. Так, в качестве основных угроз информационной безопасности можно выделить:

– неправомерный доступ к конфиденциальной информации;

– преднамеренное изменение данных, имеющих статус конфиденциальности;

– ограничение возможности получения доступа к информации информационных систем.

В современных условиях огромное влияние оказывает уровень кибербезопасности в стране.

В связи с этим устранение угроз кибербезопасности будет являться важнейшим направлением политики государства. К основным киберугрозам относят фишинг, то есть неправомерное получение конфиденциальной информации, баз данных. Помимо фишинга угрозой являются и атаки со стороны программ-вымогателей. Такие программы буквально похищают базы данных, в том числе государственных органов с целью получения выкупа. Еще

одной киберугрозой, требующей нейтрализации является криптоджекинг, то есть захват компьютера с целью майнинга криптовалюты. Все виды киберугроз оказывают огромное влияние на развитие устойчивости страны, в связи с чем они требуют незамедлительного устранения.

Указанные выше угрозы требуют разработки мер по их нейтрализации.

Мы предлагаем следующие мероприятия:

– обеспечение ужесточения мер контроля за соблюдением нормативно-правовых актов в части кибербезопасности. Данная мера может быть реализована с помощью создания новых нормативно-правовых актов, ужесточающих контроль;

– создание новых мер поддержки инновационных отраслей экономики. Среди таких мер поддержки мы можем предложить создание малых предприятий, которые смогут быть объектами делегирования деятельности более крупных киберкомпаний. Это позволит развивать МСП в сфере киберинноваций, а также продвигать эти инновации за счет финансирования и непосредственного управления со стороны крупных компаний;

– увеличение объемов льготного кредитования для компаний, занимающихся киюерюезопасностью. Важным моментом должен стать тот факт, что гарантом выполнения обязательств перед банками должно стать государство. Это позволит развивать кибербезопасность, тем самым повышая экономическую устойчивость страны;

– ограничение либо запрещение доступа иностранных инвестиций в киберкомпании, признаваемые особо важными для экономического и социокультурного развития государства. Это связано с тем, что наблюдается недостаточность инвестиций в Российской Федерации, а имеющиеся инвестиции в больших объемах поступают из-за границы. Ограничение объемов инвестиций со стороны иностранных инвесторов сможет привести к тому, что все инвестиции будут поступать из внутренних источников, будет расти потенциал России и развиваться кибербезопасность страны.

Как мы видим, данные меры нейтрализации угроз касаются различных составляющих системы устойчивого развития страны, в частности нас интересуют меры по нейтрализации киберугроз.

3.2 Основные мероприятия для повышения кибербезопасности

Проблема высокого уровня киберпреступности в России и в мире является актуальной, так как с каждым годом растет количество способов совершаемых преступлений.

Для того чтобы сократить количество фактов преступлений в сфере кибербезопасности следует разработать ряд мер, которые позволят снизить уровень киберпреступности, повысить информационную безопасность.

На данный момент уже существуют меры, которые предпринимаются в отношении кибербезопасности. Тем не менее, как мы выяснили, данные меры не являются достаточно эффективными, так как количество киберпреступлений растет.

Рассматривая данный вопрос, мы пришли к выводу, что кибербезопасность нуждается в разработке и введении новых по повышению ее уровня.

Для повышения уровня кибербезопасности в стране следует предпринять ряд мер, которые бы осуществлялись с разных сторон. Так, например, основными рекомендациями могут стать улучшения в организационном направлении, в нормативно-правовом, а также в экономическом.

Для начала отразим основные направления предлагаемых нами рекомендаций на рисунке 7.

Рисунок 7 – Основные направления рекомендаций по повышению кибербезопасности страны (составлено автором)

Раскроем данные рекомендации более детально.

Первым направлением будет экономическое. В рамках данного направления мы предлагаем снизить процентную ставку налога на добавленную стоимость с 20% до 10 % для предприятий, занимающихся инновациями в области кибербезопасности.

В настоящее ставка налога на добавленную стоимость для предприятий, занимающихся кибербезопасностью составляет 20%, как и для всех других предприятий. Для того чтобы осуществить поддержку деятельности таких

компаний, а также повлиять на увеличение компаний в отрасли следует снизить ставку до 10 %.

Для реализации данного проекта следует создать программу по поддержке предприятий киберзащиты, которая предусматривала бы процедуру снижения налогов. Данная мера должна осуществляться при условии, что компания занимается именно инновациями в части кибербезопасности, а именно разработкой ПО.

То есть, доля стимуляции деятельности киберкомпаний нужно понизить налоговую ставку на налог на добавленную стоимость путем издания соответствующего документа.

На начальном этапе данная мера приведет к тому, что снизятся налоговые поступления в бюджет от налога на добавленную стоимость, взимаемого с продажи программного обеспечения. Тем не менее, экономичсекую эффективность можно будет наблюдать спустя 3–5 лет. За этот период появится большее количество компаний, так как условия для осуществления деятельности в части кибербезопасности будут являться максимально выгодными. На данный момент для IT предприятий уже существуют льготы в части пониженного налога на прибыль, а также сниженных страховых взносов.

Применение нашего предложения в совокупности с существующими мерами приведет к расширению числа киберкомпаний, как следствие и к созданию новых инновационных продуктов, в частности нового программного обеспечения. Экономический эффект от данной меры будет заключаться еще и в том, что объем ВВП страны вырастет от роста денежных средств, вращающихся в экономики. Социальный эффект выразится в создании новых рабочих мест, повышении уровня жизни населения.

Разработка новых кибертехнологий, их внедрение в деятельность экономических агентов ведет к стабильности производственных секторов и экономической безопасности страны, а также к росту кибербезопасности. В

качестве одной из мер такой поддержки предложим создание государственной гарантии для венчурных фондов по инвестиционной поддержке IT компаний.

На данный момент венчурные фонды, денежные средства которых направлены на инвестирование средств внутри страны, занимают очень маленький процент, а если и есть, то направлены на развитие игр, интернет-платформ или интернет-проектов.

Увеличение объема внутренних инвестиций в компании, занимающиеся киберразработками приведет к росту привлекательности таких компаний, а также к повышению уровня кибербезопасности страны за счет разработки новых средств защиты.

В качестве поддержки таких венчурных фондов можно предложить страховую государственную гарантию возмещения денежных средств в случае, если деятельность стартапа будет нерентабельной. Такую гарантию может предоставлять Фонд развития инновация за счет средств фонда.

Данная поддержка должна составить 10% от вложенных инвестиций. В случае, если компания все-таки получит прибыль от успешной реализации стартапа киберкомпании, оно должно выплатить за предоставленные государством гарантии 10% от суммы прибыли.

Для того, чтобы определить целесообразность предлагаемых мероприятий необходимо сопоставить затраты на организацию таких программ.

Так, рассмотрим затраты, связанные с внедрением проекта. Основная статья затрат в этом проекте заключается в сумме государственных гарантий, которые будут предоставляться венчурным фондам, которые осуществят финансовое обеспечение стартапов в сфере киберзащиты.

В целом венчурные фонды вкладывают деньги в проекты на ранних стадиях развития, которые обещают быстро расти.

Так, в таблице 9 отразим основные затраты на создание страховых государственных гарантий для венчурных фондов.

Таблица 9 – Расчет затрат и прибыли при реализации проекта страховой государственной гарантии инвестиций венчурных фондов в IT технологии (составлено автором)

Показатель	Значение
Государственная гарантия	10%
Средняя сумма, необходимая для создания венчурного фонда млн руб.	900
В т. ч. аренда офисного помещения, выплата заработной платы сотрудникам, другие расходы, млн руб. (в расчете за 5 лет)	300
В т. ч. сумма инвестиций, млн руб.	600
Сумма государственной гарантии, млн руб.	60
Сумма прибыли при успешной реализации стартапа, млн руб.	240
Сумма, которую получит государство в случае успешной реализации стартапа, млн руб.	24

Таким образом, первоначальные расходы составят 60 млн руб. На начальном этапе затраты государства будут нужны именно для предоставления страховой гарантии.

Доходность венчурных фондов от инвестиций составляет 20–40 % согласно исследованиям Maxfield Capital.

Следовательно, при успешном запуске такого стартапа владельцы фонда получат прибыль в размере 240 млн (до вычета налогов), а государство получит взнос в размере 24 млн руб., при условии, что вложено около 600 млн руб.

При учете, что успешными становятся 7 из 10 стартапов, то государство получит около 168 млн руб., а потеряет 180 млн руб.

Но нельзя не учитывать повышение уровня кибербезопасности страны, а также повышение уровня ВВП за счет прибыли, которую получат эти компании, тем самым повышая уровень устойчивости.

Данная мера для повышения уровня кибербезопасности приведет к развитию средств киберзащиты, программного обеспечения, а также позволит увеличить уровень устойчивого развития страны.

Далее, мы предложим нормативно-правовую меру по повышению уровня кибербезопасности.

В качестве нашего предложения выступает ужесточение действующего законодательства в части киберпреступлений.

Данное предложение связано с тем, что несмотря на существующие меры, количество преступлений растет, что говорит об их недостаточности.

Так, в таблице 10 отразим предлагаемые нами мероприятия, а также сравнение с существующими мерами наказания киберпреступности.

Таблица 10 – Предлагаемое ужесточение мер наказания за киберпреступления (составлено автором)

Вид преступления	Существующее наказание	Предлагаемое наказание
Создание, распространения, использование компьютерной информации (для неправомерного воздействия на информационную структуру)	Принудительные работы на срок до 5 лет с ограничением свободы, либо лишением свободы на срок от 2 до 5 лет со штрафом от 500 тыс. рублей до 1 млн.	Принудительные работы на срок до 10 лет, с ограничением свободы на срок от 5 до 10 лет со штрафом от 500 тыс. рублей до 1,5 млн руб.
Совершение действий, направленных на неправомерный доступ к охраняемой компьютерной информации с использованием вредоносных компьютерных программ и заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации,	Лишение свободы на срок до 6 лет	Лишение свободы на срок до 10 лет
Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, в случае причинения вреда критической информационной инфраструктуре Российской Федерации	Принудительные работы на срок до 5 лет с лишением права занимать определенные должности на срок до 3 лет, либо лишение свободы на срок до 6 лет	Принудительные работы на срок до 7 лет с лишением права занимать определенные должности на срок до 3 лет, либо лишение свободы до 8 лет

Такие меры по повышению уровня кибербезопасности приведут к тому, что снизится количество преступлений.

Так, согласно данным исследования RTM Group, количество преступных атак увеличилось на 35 %. В связи с этим, на наш взгляд, данная мера поможет замедлить эти темпы примерно на 10 % в ближайший год, и на 15–20 в последующие.

Это связано с тем, что в первый год данные изменения только начнут применяться, тогда как через несколько лет они закрепятся в нормативно-правовом пространстве, будет больше фактов их применения, что приведет к сокращению киберпреступности.

Для наглядности эффективности данного предложения отразим уровень преступности, которого можно достичь благодаря ужесточению наказания.

Отразим это в таблице 11.

Таблица 11 – Эффективность ужесточения наказания за киберпреступления (составлено автором)

Имеющиеся показатели киберпреступности по состоянию на 2021 год (количество преступлений), ед.	518 000
Планируемые показатели киберпреступности после применения предлагаемой меры (в краткосрочной перспективе, 10%) (количество преступлений), ед.	466 200
Планируемые показатели киберпреступности после применения предлагаемой меры (в долгосрочной перспективе, 25%) (количество преступлений), ед.	388 500

Так, ужесточение наказания за киберпреступления может привести к значительному снижению количества преступлений.

Следующим предложением будет мера организационного характера, которая представляет собой ограничение незащищенного доступа в сеть Интернет со стороны стратегически важных для Российской Федерации отраслей экономики.

Реализация данной меры должна осуществляться через использование специальных программ, которые будут ограничивать незащищенный доступ.

На рисунке 8 отразим основные инструменты для реализации данного предложения.

Рисунок 8 – Инструменты ограничения доступа к сети Интернет (составлено автором по материалам [13])

Применение данных инструментов в некоторых отраслях поможет сократить количество кибератак, совершаемых в преступных целях.

Основной упор должен быть сделан на критическую информационную инфраструктуру.

Эти отрасли наиболее часто подвергаются воздействию кибератак. На данный момент некоторые госучреждения уже пользуются ограничением доступа к интернету, но на наш взгляд, для большей безопасности страны и конфиденциальной информации следует распространить это воздействие на все госорганы.

Применение прокси-сервера подойдет преимущественно для государственных органов. Данное программное обеспечение является наиболее простым, для его применения нужно будет лишь два компьютера.

Аппаратная система с применением отдельного сервера контроля представляет собой ограничение доступа через использование компьютера, коммутатора и ПО. Данный инструмент достаточно затратен, но эффективен.

Интернет-шлюз выполняет функцию всё того же программного обеспечения и устанавливает надзор за локальной сетью. Кроме ПО, готовый шлюз может представлять собой и аппаратный комплекс, снабжённый высокопроизводительными устройствами.

Реализация данного мероприятия может быть осуществлена и с помощью создания конкурса на создание общей системы, например для промышленного комплекса России, которая будет содержать все необходимые для деятельности компании сервисы, но не будет позволять сотрудникам пользоваться социальными сетями или другими интерфейсами сети Интернет.

Ограничение доступа к сети Интернет в данных сферах приведет к значительному сокращению успешных кибератак, а также к повышению уровня безопасности информации, которая влияет на устойчивость страны.

Таким образом, предложенные нами мероприятия приведут к значительным экономическим и социальным эффектам, которые повысят уровень кибербезопасности и устойчивость страны.

Таким образом, основными предлагаемыми нами мерами повышения уровня кибербезопасности будет:

– снижение ставки налога на добавленную стоимость с 20 % до 10% для киберкомпаний;

– создание страховых государственных гарантий для венчурных фондов, инвестирующих в киберразработки;

– ужесточение статей уголовного кодекса в части киберпреступлений;

– ограничение незащищенного доступа в интернет в наиболее стратегически важных отраслях, а также в отраслях, где замечено наибольшее количество кибератак.

ЗАКЛЮЧЕНИЕ

Состояние устойчивости экономики Российской Федерации достигается только путем соблюдения основных постулатов экономической безопасности страны. Рассматривая кибербезопасность, как фактор, влияющий на состояние экономической безопасности России, мы пришли к выводу, что данная сфера имеет множество проблем, которые требуют незамедлительного решения, так как от нейтрализации данных проблем зависит развитие экономики страны.

Так, в первой главе мы рассмотрели теоретические аспекты исследования экономической устойчивости.

По итогам данной главы можно сделать следующие выводы:

– в соответствии с Указом Президента РФ от 13 мая 2017 года № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» экономическая безопасность – «состояние защищённости национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство её экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации».

– главная функция системы экономической безопасности России – умение управлять возможными противоречиями интересов государства, общества, личности. С целью эффективного управления необходимо систематизировать элементы данной системы, изучить их, что позволит дать правильную оценку и провести анализ состоянии экономики на микро– и макроуровне, выработать меры по предупреждению угроз.

– направлениями обеспечения экономической безопасности является энергетическая безопасность, продовольственная безопасность, технико-производственная безопасность, транспортная безопасность и т. д.

– среди факторов, влияющих на экономическую безопасность, можно выделить геополитическое и экономико-географическое положение России, экономическую и военно-политическую мощь России, приоритеты

экономической политики России, параметры отраслевой и региональной структур ВВП, наличие резервов стратегически важных материальных благ.

– в соответствии с Доктриной информационной безопасности РФ 2016 г. кибербезопасность рассматривается как состояние защищенности государства, общества, личности от внутренних и внешних информационных угроз.

– сегодня наиболее острой проблемой в области обеспечения безопасности в информационной сфере является хранение большой информации о личных данных граждан государств, которые они предоставляют в глобальной сети Интернет.

– к угрозам кибербезопасности Российской Федерации можно отнести расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, использование террористическими и экстремистскими организация механизмов информационного воздействия на индивидуальное, групповое и общественное сознание, рост компьютерной преступности и т.д.

– основными факторами, оказывающими воздействие на совершение киберпреступлений экономического характера, являются: экономически кризис, повышение цен на товары первой необходимости, снижение уровня жизни, повышение уровня безработицы.

Во второй главе нами был проанализирован уровень финансовой устойчивости РФ.

По итогам данной главы можно сделать следующие выводы:

– положительная динамика прослеживается только у половины показателей экономической безопасности Российской Федерации, указанных в «Стратегии экономической безопасности». Стоит отметить такой показатель как уровень инфляции, который в 2021 году составил 8,4 %, и оказывает непосредственное негативное влияние на социально-экономическую сферу. Стабильную положительную динамику имеют показатели, относящиеся ко внешнеэкономической деятельности и оборот розничной торговли, которые

сигнализируют об уменьшении влияния санкционного давления на российскую экономику.

– состояние кибербезопасности России находится не на таком высоком уровне. Количество киберпреступлений растет, темпы роста атак также выросли. Несмотря на достаточно широкую нормативно-правовую базу регулирования киберпреступности в России, ее влияния оказывается недостаточно. Большинство киберпреступлений совершается в отношении государственных органов. Объектом чаще всего являются персональные данные. Если говорить о сравнении показателей России и мира, то мы видим, что показатели роста киберпреступлений за последний год в России находятся на высоком уровне. Выше этих показателей только значения Европы и Северной Америки.

– влияние кибербезопасности на устойчивость страны прямо отражается через ее основные показатели, например через уровень преступности в части кибербезопасности, также, кибератаки на государственные органы влияют на эффективность их работы, что также снижает финансовую устойчивость. Также, кибератаки на физические лица могут косвенно снижать уровень жизни населения и финансовую устойчивость как следствие.

В третьей главе нами были разработаны направления повышения экономической устойчивости РФ через повышение уровня кибербезопасности.

Мы предлагаем следующие мероприятия по повышению устойчивости страны:

– обеспечение ужесточения мер контроля за соблюдением нормативно-правовых актов в части кибербезопасности. Данная мера может быть реализована с помощью создания новых нормативно-правовых актов, ужесточающих контроль;

– создание новых мер поддержки инновационных отраслей экономики. Среди таких мер поддержки мы можем предложить создание малых предприятий, которые смогут быть объектами делегирования деятельности

более крупных киберкомпаний. Это позволит развивать МСП в сфере киберинноваций, а также продвигать эти инновации за счет финансирования и непосредственного управления со стороны крупных компаний;

– увеличение объемов льготного кредитования для компаний, занимающихся киюерюезопасностью. Важным моментом должен стать тот факт, что гарантом выполнения обязательств перед банками должно стать государство. Это позволит развивать кибербезопасность, тем самым повышая экономическую устойчивость страны;

– ограничение либо запрещение доступа иностранных инвестиций в киберкомпании, признаваемые особо важными для экономического и социокультурного развития государства. Это связано с тем, что наблюдается недостаточность инвестиций в Российской Федерации, а имеющиеся инвестиции в больших объемах поступают из-за границы. Ограничение объемов инвестиций со стороны иностранных инвесторов сможет привести к тому, что все инвестиции будут поступать из внутренних источников, будет расти потенциал России и развиваться кибербезопасность страны.

Основными предлагаемыми нами мерами повышения уровня кибербезопасности будет:

– снижение ставки налога на добавленную стоимость с 20 % до 10% для киберкомпаний;

– создание гарантий для венчурных фондов, инвестирующих в киберразработки;

– ужесточение статей уголовного кодекса в части киберпреступлений;

– ограничение доступа в интернет в наиболее стратегически важных отраслях, а также в отраслях, где замечено наибольшее количество кибератак.

Таким образом, данные мероприятия позволят повысить уровень устойчивости нашей страны.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Актуальные киберугрозы: итоги 2021 года // Электронный ресурс. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения: 20.05.2022).

2. Актуальные киберугрозы: итоги 2020 года // Электронный ресурс. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения: 20.05.2022).

3. Абанина, Е.Н., Агапов, Д.А. Российское правотворчество в целях перехода к устойчивому развитию / Е.Н. Абанина, Д.А. Агапов // Право. Законодательство. Личность. 2019. № 2. С. 134-141

4. Бадалян, Л.Х. Экономический ущерб от выбросов загрязняющих веществ и возмещение нанесенного автотранспортом вреда / Л.Х. Бадалян, В.Н. Курдюков // Экономический вестник Ростовского государственного университета. 2019. — Т. 6. — № 3. — Ч. 2. — С. 134 — 137.

5. Авчаров, И.В. Борьба с киберпреступностью / И.В. Авчаров. // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. - М., 2019. - С. 191-194.

6. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.

7. Букин, Д.А. Underground киберпространства/ Д. Букин // Рынок ценных бумаг. 2013. - №8. - С. 104 - 108.

8. Бураева, Л.А. Информационный терроризм как угроза национальной безопасности Российской Федерации // Пробелы в российском законодательстве. 2016. №6. URL: https://cyberleninka.ru/article/n/informatsionnyy-terrorizm-kak-ugroza-natsionalnoy-bezopasnosti-rossiyskoy-federatsii (дата обращения: 05.06.2022).

9. Баух, Д.А. Продовольственная безопасность и импортозамещения как часть экономической безопасности / Д.А. Баух // Сборники конференций НИЦ

Социосфера. — 2020. — № 25. — С. 171–174. Богомолов, В.А. Введение в специальность «Экономическая безопасность»: Учебное пособие / В. А. Богомолов. — М.: ЮНИТИ-ДАНА, 2018. — 279 с.

10. Василенко, О. А. Основные цели и задачи государственной политики России в сфере экономической безопасности // Вопросы науки и образования. 2018. №16 (28). URL: https://cyberleninka.ru/article/n/osnovnye-tseli-i-zadachi-gosudarstvennoy-politiki-rossii-v-sfere-ekonomicheskoy-bezopasnosti (дата обращения: 01.06.2022).

11. Вершило, Н.Д. Правовые основы устойчивого развития/ Н.Д. Вершило //Вестник Саратовской государственной академии права. 2020. № 4. С. 56–57.

12. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.

13. Валько, Д.В. Киберпреступность в России и мире: сопоставительная оценка // Управление в современных системах. 2016. №3 (10). URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka (дата обращения: 05.06.2022).

14. В 2021 году число кибератак на организации во всем мире выросло на 40% — исследование // Электронный ресурс. URL: https://rb.ru/news/cybercrime-2021/?ysclid=l40cfftq52 (дата обращения: 20.05.2022).

15. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

16. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

17. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.

18. Единый реестр субъектов малого и среднего предпринимательства. [Электронный ресурс]. URL: https://ofd.nalog.ru/statistics.html? (дата обращения: 24.02.2022).

19. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 с.

20. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. Москва: Риор, 2017. 480 с.

21. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.

22. Забелина, А.О., Утигалиева, П.А. О мерах по нейтрализации глобальных угроз экономической безопасности // ИБР. 2018. №3 (32). URL: https://cyberleninka.ru/article/n/o-merah-po-neytralizatsii-globalnyh-ugroz-ekonomicheskoy-bezopasnosti (дата обращения: 01.06.2022).

23. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

24. Информационная безопасность. Защита информации. URL: http://all-ib.ru/ (дата обращения: 13.05.2022).

25. Итоги 2021 года и прогнозы на 2022-й в области кибербезопасности по версии Positive Technologies // Электронный ресурс. URL: https://cisoclub.ru/itogi-2021-goda-i-prognozy-na-2022-j-v-oblasti-kiberbezopasnosti-po-versii-positive-technologies/ (дата обращения 20.05.2022).

26. Консультант. [Электронный ресурс]. // URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=148429 (дата обращения: 24.02.2022).

27. Мамаева Людмила Николаевна, Шульдякова Виктория Владимировна, Удалов Дмитрий Валериевич Влияние глобальных угроз на

национальную экономическую безопасность // Вестник Саратовского государственного социально-экономического университета. 2018. №5 (74). URL: https://cyberleninka.ru/article/n/vliyanie-globalnyh-ugroz-na-natsionalnuyu-ekonomicheskuyu-bezopasnost (дата обращения: 05.06.2022).

28. МинФин России Официальный сайт. [Электронный ресурс]. // URL:https://minfin.gov.ru/ru/statistics/fedbud/execute/?id_65=80041yezhegodnaya_informatsiya_ob_ispolnenii_federalnogo_byudzheta annye_s_1_yanvarya_2006_g. (дата обращения: 24.05.2022).

29. Министерство Внутренних Дел Российской Федерации. [Электронный ресурс]. // URL: https://мвд.рф/?ysclid=l38l7mscfo (дата обращения: 24.05.2022).

30. Остроух, Е.Н. Разработка методов и алгоритмов проверки работы предприятия с точки зрения информационной безопасности его функционирования / Е.Н. Остроух, Ю.О. Чернышев, С.А. Мухтаров; под ред. Е.Н Остроух // Инженерный вестник Дона. – 2016. Т. 41. – № 2 – (41). С. 31.

31. Отчет Итоги контроля уязвимостей Российских компаний за 2021 год // Электронный ресурс. URL: https://rt-solar.ru/upload/iblock/7a9/kc1dio23g2v2x657ne6xo0nu2zjlvqie/Itogi-kontrolya-uyazvimostey-rossiyskikh-kompaniy-za-2021-god.pdf (дата обращения 01.06.2022).

32. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.

33. Постановление Правительства Российской Федерации от 8 мая 1996 г. № 559 «О разработке проекта государственной стратегии устойчивого развития Российской Федерации» //Собр. законодательства Рос. Федерации. 1996. № 20. Ст. 2351.

34. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 с.

35. Росфинмониторинг // URL: https://www.vestifinance.ru/articles/115216 (дата обращения 16.03.2022).

36. Ражабов, А. Х. О теоретических основах устойчивого развития / А.Х. Ражабов // Молодой ученый. — 2018. — №13. — С. 495-498.

37. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.

38. Скоморохина, Е.В. Стратегия (концепция) устойчивого развития: перспективы реализации в мире и России / Е.В. Скоморохина // Вестник Воронежского государственного университета. Серия: Право. 2018. № 4 (23). С. 13-18.

39. Урсул, А.Д. Концептуальные проблемы устойчивого развития / А.Д. Усул // Бюллетень РАН. Использование и охрана природных ресурсов в России. — 2019. — № 1. — С. 30-38.

40. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

41. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (последняя редакция).

42. Федеральная служба государственной статистики. [Электронный ресурс]. // URL: https://rosstat.gov.ru/ (дата обращения: 20.03.2022).

43. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» // Российская газета, № 295 (с изм. и доп.).

44. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. Москва: Форум, 2017. 448 с.

45. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336с.

46. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. - Москва: Форум, Инфра-М, 2017. - 416 с.

47. Шайденко, Н.А. Устойчивое развитие как глобальная проблема современного общества / Н.А. Шайденко // Успехи современной науки. 2017. Т. 1. № 2. С. 68-71.

48. Шумилов, Ю.В., Шумилова, М.Ю. О концепции устойчивого развития в неустойчивом мире / Ю.В. Шумилов, М.Ю. Шумилова // Евразийское Научное Объединение. 2017. Т. 2. № 2 (24). С. 159-162.

49. Шаньгин, В. Ф. Информационная безопасность и защита информации / Шаньгин Владимир Федорович. Москва: ДМК Пресс, 2017. 249 с.26.

50. 12 простых советов по кибербезопасности, которые помогут лучше защитить ваши данные // Электронный ресурс. URL:https://www.securitylab.ru/blog/personal/bezmaly/350620.php? (дата обращения 05.06.2022).