МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет экономический**

**Кафедра мировой экономики и менеджмента**

Допустить к защите

Заведующий кафедрой

д-р экон. наук, проф.

\_\_\_\_\_\_\_\_\_\_\_И.В. Шевченко

(подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2023 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

**(Дипломная РАБОТА)**

**ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕГИОНА**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.П. Карибов

(подпись)

Специальность 38.05.01 Экономическая безопасность

(код, наименование)

Специализация Экономико-правовое обеспечение экономической

безопасности

Научный руководитель

док. экон. наук, доц.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_К.В. Косенкова

(подпись)

Нормоконтролер

преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Н.В. Хубутия

(подпись)

Краснодар

2023

**СОДЕРЖАНИЕ**

Введение 3

1. Теоретические основы обеспечения информационной составляющей экономической безопасности 6
   1. Проблемы и сущность обеспечения информационно-функциональной составляющей экономической безопасности 6
   2. Отечественный и зарубежный опыт использования современных средств защиты информации 14
   3. Правовые основы обеспечения информационно-функциональной составляющей экономической безопасности 25
2. Оценка основных показателей информационной безопасности Краснодарского края 30
   1. Анализ индикаторов информационной составляющей экономической безопасности 30
   2. Выявление угроз информационной составляющей экономической безопасности 42
3. Разработка мероприятий по обеспечению информационной функциональной составляющей экономической безопасности 48
   1. Основные направления снижения угроз экономической   
      безопасности 48
   2. Разработка мероприятий по совершенствованию защиты информационной составляющей экономической безопасности 52

Заключение 69

Список использованных источников 72

# ВВЕДЕНИЕ

Актуальность данной работы обусловлена быстро изменяющейся обстановкой в мире. В настоящее время информационная безопасность становится одной из важнейших задач в построении комплексной системы безопасности. С развитием информационных технологий и все большей цифровизации различных сфер деятельности, возникают новые угрозы и вызовы в области безопасности данных и информационных систем. Киберпреступления, хакерские атаки, утечки конфиденциальной   
информации — все это становится реальностью, с которой необходимо активно бороться.

Целью выпускной квалификационной работы является определение эффективных механизмов информационного обеспечения экономической безопасности Краснодарского края.

Задачи выпускной квалификационной работы:

1. изучить текущее состояние информационной безопасности в обеспечении экономической безопасности Краснодарского края. Проанализировать проблемы, с которыми регион сталкивается в этой сфере;
2. определить основные угрозы и риски, связанные с информационной безопасностью в экономике Краснодарского края. Проанализировать возможные последствия и негативные воздействия на региональное развитие;
3. исследовать существующие механизмы информационного обеспечения экономической безопасности на примере Краснодарского края. Анализ и оценка эффективности применяемых инструментов и методов;
4. разработать рекомендации по совершенствованию информационного обеспечения экономической безопасности Краснодарского края. Определение приоритетных направлений и мероприятий для обеспечения защиты информации и минимизации рисков;
5. провести практический анализа и предложить рекомендации на примере конкретных ситуаций в экономике.

Объектом исследования является информационная безопасность в обеспечении экономической безопасности Краснодарского края.

Предметом исследования являются механизмы и методы информационного обеспечения, направленные на защиту экономических интересов Краснодарского края и обеспечение его устойчивого развития.

Теоретической и методологической основой исследования послужили труды зарубежных и отечественных ученых, публицистов, а также энциклопедическая и справочная литература, законодательные и нормативные акты Российской Федерации.

При написании работы использовались следующие методы: теоретические методы (анализ источников литературы   
и нормативно‑правовой документации, их сравнение и обобщение); эмпирические методы (анализ документов и фактических материалов); методы обработки данных (качественный и количественный анализ).

Теоретическая значимость работы заключается в совершенствовании обеспечения информационной безопасности региона на примере Краснодарского края. Полученные сведения могут быть использованы для дальнейшего изучения вопроса.

Практическая значимость состоит в том, что результаты проведенного исследования могут быть использованы для совершенствования информационной системы безопасности в Краснодарском крае.

В качестве информационной базы использованы официальные статистические материалы.

Структура работы: введение, три главы, заключение, список литературы. В первой главе были рассмотрены теоретические аспекты обеспечения экономической безопасности региона. Во второй главе проведена оценка основных показателей информационной безопасности Краснодарского края, в третьей главе разработаны мероприятия по совершенствованию защиты информационной составляющей экономической безопасности.

# Теоретические основы обеспечения информационной составляющей экономической безопасности

# Проблемы и сущность обеспечения информационно-функциональной составляющей экономической безопасности

Информация, как обязательная часть экономических отношений, в настоящее время является важнейшим фактором, во многом определяющим технологическое развитие, а также увеличение ресурсов любой экономической системы. Определить долю участия информационного ресурса в производственном процессе представляется чрезвычайно сложным, однако в условиях развития научно-технического прогресса и ограниченности большинства видов материальных ресурсов информационный ресурс занимает исключительное место в функционировании экономики на всех уровнях. Доля затрат на информационные ресурсы продолжает расти, а развитие информационных технологий приводит к появлению принципиально новых структур, для которых основным фактором производства является не труд, не капитал, а информация [14].

Обеспечение экономической безопасности определяет использование передовых информационных технологий в различных сферах хозяйствования, которые развиваются особенно быстрыми темпами в рыночных условиях. Системы управления, основанные на новейших информационных технологиях, также развиваются значительными темпами.

В связи с расширением информационных технологий в России, как и во всем мире, возникли не только возможности для быстрого прогресса   
и эффективного использования информационных сетей в предпринимательской деятельности, но и новые угрозы. Процессы внедрения и развития информационно-коммуникационных технологий происходят намного оперативнее, чем законодатели и правоохранительные органы могут реагировать на данный рост.

Проблема преступности в глобальных информационных сетях имеет два компонента [14]:

1. возникают новые преступления, такие как нарушение целостности, доступности и конфиденциальности электронных данных, которые направлены против новых интересов, возникших в результате развития информационных технологий;
2. глобальные информационные сети применяются для осуществления действий, которые уже признаны криминализованными в законодательстве большинства стран, таких как кража собственности, нарушение конфиденциальности личной жизни и другие.

Была проведена достаточная исследовательская работа по роли информации в обеспечении функционирования экономических систем и методам ее использования отдельными предпринимателями, предприятиями и региональными структурами управления. Однако, информация в качестве составной части эффективного организационно-экономического механизма обеспечения экономической безопасности региона пока не получила достаточного уровня глубокого исследования. Развитие региональных информационных институтов является актуальной задачей в современном контексте регионального управления.

В процессе такого управления необходимо осуществлять следующие действия [14]:

* создание и развитие региональных информационных институтов для эффективного сбора, обработки и анализа информации о состоянии   
  и потенциале региона;
* обеспечение доступности и своевременной передачи информации между различными уровнями регионального управления, а также между государственными органами и предпринимательским сектором;
* разработку и внедрение современных информационных технологий и систем для улучшения эффективности управления региональными ресурсами и развития экономики;
* обеспечение защиты информации и кибербезопасности региональных информационных систем;
* привлечение и обучение квалифицированных специалистов в области информационных технологий и систем для работы с региональными информационными институтами;
* установление партнерских связей и сотрудничество с другими региональными и международными информационными институтами для обмена опытом и передачи передовых практик;
* постоянное совершенствование и развитие региональных информационных институтов в соответствии с изменяющимися потребностями и вызовами современности.

На микроуровне экономическая информация может быть получена из различных источников, включая:

* средства периодической печати, которые представляют собой надежный источник информации по широкому спектру тем. Однако их недостатком является низкое соотношение между полезной и неполезной информацией, за исключением специализированных изданий;
* телевидение и радио, которые часто предоставляют информацию с рекламным характером;
* информационные базы данных (БД), где экономическая информация представлена в формализованном и систематизированном виде;
* телекоммуникационные сети, включая как общедоступные, так   
  и специализированные сети, которые также могут служить источником экономической информации.

Основная цель информационной безопасности заключается в создании условий, гарантирующих качественную и эффективную защиту конфиденциальной информации от нежелательного или преднамеренного вмешательства, которое может привести к потере, удалению, изменению, подмене или другим негативным воздействиям на информацию.

Для обеспечения эффективной эксплуатации системы информационной безопасности необходимо выполнить следующие шаги [14]:

1. идентифицировать специфические требования по защите информации для конкретного объекта защиты;
2. учесть требования национального и международного законодательства, касающиеся информационной безопасности;
3. применить установленные практики, стандарты и методологии, используемые для построения систем обеспечения информационной безопасности;
4. назначить ответственные подразделения, которые будут отвечать   
   за реализацию и поддержку системы обеспечения информационной безопасности;
5. распределить области ответственности между подразделениями в отношении выполнения требований системы обеспечения информационной безопасности;
6. на основе управления рисками информационной безопасности разработать общие положения, технические и организационные требования, которые составят политику информационной безопасности;
7. реализовать требования политики информационной безопасности путем внедрения соответствующих программно-технических методов   
   и средств защиты информации;
8. установить и реализовать систему управления информационной безопасностью;
9. используя систему управления информационной безопасностью, которая позволяет регулярно контролировать эффективность всех мероприятий, направленных на защиту информации, регулярно контролировать эффективность системы и, при необходимости, производить пересмотр и корректировку.

Задачи систем информационной безопасности включают в себя:

1. обеспечение безопасного хранения информации на носителях, чтобы предотвратить несанкционированный доступ или потерю данных;
2. защита данных, передаваемых по каналам связи, с помощью шифрования, контроля целостности и других мер безопасности;
3. создание резервных копий информации и восстановление после аварийных ситуаций, чтобы минимизировать потери данных и обеспечить их восстановление;
4. обеспечение доступности информации, чтобы пользователи могли получить требуемую информацию в приемлемые сроки, а также предотвращение несанкционированного отказа в доступе к информации;
5. обеспечение целостности информации, предотвращая несанкционированное изменение или разрушение данных, например, с помощью контроля целостности, цифровых подписей и аудита информационных систем;
6. обеспечение конфиденциальности информации, предотвращая несанкционированный доступ или раскрытие информации, например, с помощью шифрования, управления доступом и защиты персональных данных.

Нарушение информационных параметров, таких как конфиденциальность, целостность, доступность, надежность и другие, может иметь серьезные последствия, включая сбои в системах управления технологическими процессами и других критических системах.

Организация и функционирование системы безопасности субъекта информации должны осуществляться на основе следующих принципов [5]:

1. комплексность;

Данный принцип включает в себя обеспечение защищенности персонала, материальных и финансовых ресурсов, а также информации от всех возможных угроз. Это достигается с помощью применения всех доступных законных средств и методов защиты.

1. надежность;

Данный принцип предполагает, что различные зоны безопасности должны быть одинаково надежными с точки зрения вероятности реализации угрозы. Это означает, что все компоненты и механизмы системы безопасности должны быть проектированы и реализованы с высоким уровнем надежности, чтобы минимизировать возможность взлома, нарушений или несанкционированного доступа;

1. своевременность;

Этот принцип подразумевает, что система безопасности должна обладать способностью упреждать угрозы на основе анализа   
и прогнозирования. Это включает в себя постоянное мониторинг и оценку потенциальных угроз безопасности, а также разработку и реализацию эффективных мер противодействия им;

1. непрерывность;

Данный принцип предполагает отсутствие перерывов в действиях системы безопасности, вызванных проведением ремонтных работ, заменой компонентов, профилактическими мероприятиями и другими подобными процедурами.

1. разумная достаточность;

Этот принцип предполагает установление приемлемого уровня безопасности, при котором вероятность возникновения угроз   
и потенциальный ущерб сочетаются с максимально допустимыми затратами на разработку и эксплуатацию системы безопасности.

1. централизация управления;

Этот принцип предполагает, что система безопасности должна функционировать на основе единых организационных, функциональных   
и методологических принципов. Централизация управления обеспечивает единообразие подходов к обеспечению безопасности, координацию действий и централизованное принятие решений в отношении безопасности организации или субъекта.

1. компетентность.

Этот принцип предусматривает, что система безопасности должна создаваться и управляться компетентными специалистами, обладающими достаточной профессиональной подготовкой. Компетентные специалисты способны корректно оценивать обстановку, анализировать риски и принимать адекватные решения, особенно в условиях повышенного риска

При разглашении сведений, составляющих государственную тайну, нарушении достоверности финансовой документации, несанкционированном доступе к персональным данным работников, а также при разглашении сведений, содержащих состояние материальных и финансовых потоков, договорной деятельности, данных бухгалтерского и управленческого учета, могут возникнуть следующие последствия [14]:

* ухудшение или разрыв деловых отношений с партнерами;
* отказ от решений, ставших неэффективными из-за раскрытия информации;
* новые потери, связанные с разработками;
* снижение цен или объемов реализации;
* потеря репутации и прочее.

Таким образом, нынешняя сеть безопасности данных ставит своей задачей обеспечение защиты приватной информации от незаконного доступа, предотвращение намеренных или случайных изменений (контроль неприкосновенности) и обеспечение необходимого уровня доступности.

Выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам объекта, является одним из важнейших видов деятельности по обеспечению информационной безопасности.

Угрозы условно можно разделить на четыре следующие группы [4]:

1. программное обеспечение или ПО, вирусы,   
   программно-аппаратные устройства для скрытого контроля, уничтожение   
   и изменение данных в информационных системах;
2. технические;

Перехват информации в передающих линиях связи, радиоэлектронное подавление сигнала в линиях связи и системах управления.

1. физические;

Уничтожение средств обработки и носителей информации.

1. режимные.

Нарушение принципов обмена информацией, незаконный сбор   
и использование данных, несанкционированный доступ к информационным ресурсам, незаконное копирование данных в информационных системах, кража носителей информации, а также аппаратных или программных парольных ключей, распространение дезинформации, скрытие или искажение информации, кража информации из баз данных.

При разработке эффективной системы обеспечения информационной безопасности, анализ угроз и рисков играет решающую роль.

Наиболее распространенными угрозами информационной безопасности являются распространение вирусов, хакерские атаки, спам и фишинг. Кроме того, необходимо учитывать внутренние угрозы, которые исходят от сотрудников, такие как небрежное отношение к безопасности, кража информационных ресурсов, мошенничество и несанкционированное использование информационных ресурсов и т.д. [14].

Кроме того, современная статистическая информация имеет следующие недостатки:

* некоторые показатели не являются информативными или не отражают полную картину;
* присутствует множественное дублирование данных, что приводит к избыточности и неэффективности;
* аналогичные данные из разных источников не сопоставимы, что затрудняет сравнение и анализ;
* терминология, используемая в экономической информации, не унифицирована.

Развитие региональной статистики, в первую очередь, требует методологических усовершенствований. Несмотря на прогресс в области региональной статистики, использование информационных ресурсов для отслеживания изменений в масштабах производства и потребления, анализа финансово-экономической деятельности предприятий и социальной ситуации в регионе остается сложной задачей.

Таким образом, в настоящее время крайне сложно получить полное   
и всестороннее представление о реальных факторах, механизмах   
и взаимосвязях, которые определяют современное социально-экономическое развитие региона и его уровень экономической безопасности.

Для организации информационной инфраструктуры и эффективного информационного обслуживания на региональном уровне необходимо повысить эффективность региональной информационной системы. Важно обеспечить оперативное и регулярное предоставление пользователям качественной деловой и коммерческой информации.

В современных условиях информационная безопасность является неотъемлемой частью экономической безопасности региона. Обеспечение надежной экономической безопасности является необходимым условием перехода к модели устойчивого развития не только отдельного предприятия, но и всей национальной экономики.

# Отечественный и зарубежный опыт использования современных средств защиты информации

Одним из инструментов регулирования обеспечения информационной безопасности, как на государственном уровне, так и на уровне предприятий   
и граждан является нормотворческая деятельность.

В настоящее время существует программа, направленная на совершенствование существующей модели информационной безопасности.

Её положения были одобрены в 1998 году на парламентских слушаниях в Государственной Думе РФ и на заседании Комитета Государственной Думы по безопасности. В результате этих мероприятий было принято не менее 20 новых законодательных актов. Межведомственный комитет Совета безопасности Российской Федерации по информационной безопасности заявил, что уровень современной информационной безопасности не соответствует международным стандартам, и утвердил следующие направления развития законодательства [8]:

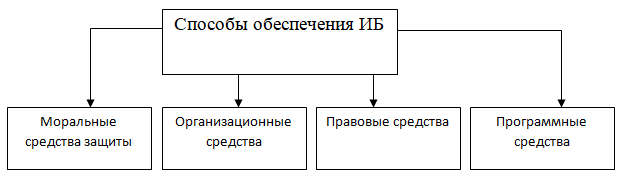
1. необходимо внести изменения в действующее законодательство с целью урегулирования разногласий с соответствующими нормами Конституции Российской Федерации и международными договорами. В работе по обеспечению информационной безопасности Российской Федерации содержится информация в статье 5 Закона «О международных договорах» 1995 года. В данной статье указывается, что в случае, если международным договором Российской Федерации установлены отличные от закона правила, то применяются правила международного договора. Однако, в новом тексте поправок к Конституции, принятых с 1 июля 2020 года, отмечается, что решения, принятые межгосударственными органами на основе толкования положений международных договоров Российской Федерации, противоречащему Конституции Российской Федерации, не могут быть исполнены на территории Российской Федерации;
2. предлагается разработать Государственную программу, которая будет способствовать формированию общественных компьютерных сетей. Эта программа будет включать определение правового статуса   
   интернет-провайдеров и правовое регулирование их деятельности. Она также будет регулировать передачу информации в сети Интернет о работе государственных и местных органов власти. Кроме того, программа будет уделять внимание защите российского языка в Интернете.;
3. предлагается разработать нормативно-правовую базу для создания системы страхования информационных рисков. Эта система будет направлена на обеспечение гарантированного страхового покрытия пользователей, которые оставляют информационные предложения, а также лиц, предоставляющих эти предложения. В рамках этой системы будет осуществляться объяснение правового статуса зарубежного инвестора в сфере вложений и связей с целью обеспечения государственной защищенности Российской Федерации;
4. предлагается провести законодательное разграничение уровней правового регулирования проблем информационной безопасности. Это включает федеральный уровень, уровень субъектов Федерации и уровень местного самоуправления;
5. предлагается законодательно закрепить приоритет развития национальных сетей связи и отечественного производства спутников для космической связи;
6. предлагается внести правовое регулирование развития негосударственной составляющей в формировании информационного общества и обеспечении информационной безопасности России;
7. создание правовой основы функционирования системы региональных центров защиты информации в Российской Федерации.

Действительно, в последние годы информационные процессы имеют значительное влияние на правовое регулирование в сфере информации, информационных технологий и защиты информации. Федеральный закон "Об информации, информационных технологиях и о защите информации" является основным нормативным актом, который устанавливает правовое положение источников информации и регламентирует основные вопросы, связанные с использованием информационных технологий и защитой информации [8].

Преодоление отставания от передовых стран требует организации   
и стимулирования производства. В данном контексте следующие вопросы заслуживают особого внимания [14]:

1. разработка программного кода и формирование продуктов в соответствии с глобальными нормами, особенно для открытых информационных бизнес-систем;
2. установление норм и правил для регулирования взаимодействия в области информационной деятельности и предоставления информационных услуг, организация и обеспечение ответственности различных посредников в коммуникационных системах;
3. формирование рынка информационных продуктов.

Если говорить о гарантировании и контроле информационной безопасности организаций и государства важно учитывать особенности конкретных бизнес-процессов. В практике обеспечения информационной безопасности компаний используются следующие методы:

Рисунок 1 – Основные способы для реализации информационной безопасности [17]

1. моральные средства защиты;

Они представляют собой нормы поведения и правила работы с информационными активами, которые возникают в результате распространения и применения электронных технологий в различных сферах деятельности государства и общества в целом.

1. организационные средства;

Для регулирования работы системы обработки информации, действий сотрудников и процесса их взаимодействия с системой применяются моральные средства защиты, направленные на предотвращение информационных атак или снижение потерь в случае их возникновения.

1. правовые средства;

Основываются на действующих в Российской Федерации законах, решениях и нормативных актах. Они устанавливают нормы и правила для обработки персональных данных, обеспечивают гарантии прав и обязанностей участников работы с источниками информации при их обработке   
и использовании, а также предусматривают ответственность за нарушения этих правил.

1. программные средства;

Для обеспечения безопасности сети используются специализированные программы, которые предназначены для защиты источников информации от несанкционированных действий. В настоящее время разработано множество антивирусных программ, брандмауэров и других средств защиты, которые помогают предотвращать вторжения и обнаруживать потенциальные угрозы в компьютерных системах и сетях.

1. аппаратные средства;

Эти компоненты представляют собой электронные устройства, которые могут быть интегрированы в автоматизированные системы или функционировать как самостоятельные устройства, взаимодействующие с основными блоками системы.

1. физические средства;

Представляют собой различные механические и электронно-механические устройства, которые создают физические преграды с целью предотвращения неправомерного доступа к элементам автоматизированной системы и обеспечения защиты информации. Физические средства охраны служат для защиты от различных угроз, таких как стихийные бедствия, пандемии, военные действия и другие опасности. Они могут включать в себя заборы, ворота, двери с электронными замками, видеонаблюдение, системы контроля доступа и прочие меры, направленные на обеспечение безопасности физического пространства и инфраструктуры.

1. технические способы;

Это разнообразные электронные и специализированные устройства, которые объединены в один автоматизированный комплекс организации   
и выполняют различные функции, связанные с обработкой и хранением персональных данных. К таким устройствам относятся системы персонализации, авторизации, аутентификации, ограничения доступа к активам пользователей и шифрования информации.

1. криптографические методы.

Этот подход основан на использовании шифрования и предоставляет механизмы для защиты конфиденциальной информации при помощи программно-аппаратных средств. Криптографические методы обеспечивают высокую степень защиты и эффективности в индивидуальной защите данных. Они позволяют преобразовывать информацию таким образом, чтобы она стала непонятной или нечитаемой для неавторизованных лиц.

Принимая во внимание существующие методы обеспечения безопасности информации, компании-разработчики из России активно работают над совершенствованием и разработкой новых систем защиты информации.

Согласно исследованию, проведенному компанией CNews Security, следующие организации являются ведущими участниками рынка информационной безопасности в России в 2022 году [1]:

1. Лаборатория Касперского,
2. Softline,
3. Цитадель,
4. Ростелеком-Солар,
5. Bi.Zone.

Данные о выручке компаний представлены в таблице 1.

Таблица 1 – Данные о выручке отечественных компаний за 2021 г. [1]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № 2020 | № 2021 | Название компании | Выручка в 2020 г., млрд рублей с НДС | Выручка в 2021 г., млрд рублей с НДС | Рост выручки 2020/2021 гг., в % |
| 1 | 1 | Лаборатория Касперского | 50,63 | 55,82 | 10,2 |
| 3 | 2 | Softline | 20,32 | 22,31 | 9,8 |
| 2 | 3 | Цитадель | 20,47 | 18,93 | -7,4 |
| 6 | 4 | Ростелеком-Солар | 8,35 | 12,27 | 46,9 |
| 5 | 5 | Bi.Zone | 8,97 | 10,44 | 16,5 |

Из таблицы видно, что компания Kaspersky остается лидером по выручке на рынке информационной безопасности в России. Также можно отметить, что выручка остальных компаний также растет в последние годы, что указывает на рост рынка информационной безопасности в России.

Эксперты выделили пять основных тенденций, которые будут определять развитие российского рынка информационной безопасности в ближайшем будущем.

По мнению экспертов компании, ключевые изменения в отрасли будут вызваны переходом на гибридную программу, сочетающую удаленную   
и офисную работу, ограниченными бюджетами бизнеса и повышением активности киберпреступников в условиях изменений в IT-сфере:

1. в контексте гибридного формата работы подходы к информационной безопасности требуют переосмысления. Границы информации становятся более размытыми, так как они должны охватывать все объекты, на которых работают сотрудники. Переход к дистанционной работе приводит к изменению организационных схем, а также к распределению рабочих мест по географическому принципу, поскольку компании все чаще привлекают сотрудников из разных регионов. Для специалистов отдела информационной безопасности возникает необходимость защищать не только инфраструктуру, находящуюся непосредственно в зданиях, но   
   и информационные системы, используемые сотрудниками в домашних условиях. Важно ясно определить, какие данные хранятся на персональных устройствах сотрудников и каковы связанные с этим риски;
2. увеличение доли информационной безопасности в IT-бюджетах российских предприятий;

В связи с экономической сложностью ситуации российские предприятия сталкиваются с увеличением доли информационной безопасности в своих IT-бюджетах. Это имеет двойственные последствия. С одной стороны, растет активность киберпреступников, которые ищут возможности для атак на компании. С другой стороны, ограниченный рост корпоративных IT-бюджетов ограничивает возможности компаний для финансирования всех аспектов информационных технологий;

1. использование поведенческого анализа для защиты данных;

Эксперты в области информационной безопасности пришли к выводу, что не существует универсального подхода для защиты общества и компаний от всех возможных угроз. Надежная система безопасности имеет модульную структуру и включает в себя комплекс решений. Средства защиты периметра, межсетевых экранов, безопасности веб-приложений и предотвращения утечек данных становятся неотъемлемой частью безопасности для крупных предприятий и различных государственных и муниципальных образований.

1. развитие инструментов автоматизации;

Увеличение активности киберпреступников и ограниченность ресурсов стимулируют растущую потребность в технологиях, которые могут автоматизировать операции в отделах информационной безопасности. Такие системы, с одной стороны, снимут сотрудников с необходимости контролировать большое количество уведомлений, а с другой, не пропустят значимые предупреждения, свидетельствующие о потенциальных атаках.

1. специалисты по информационной безопасности должны развивать аналитические навыки.

Требования к профессионалам в области кибербезопасности претерпевают значительные изменения. Помимо технической экспертизы, директоры по информационной безопасности и их подчиненные нуждаются в усилении аналитических навыков.

Главной проблемой сейчас является замещение импортной продукции на отечественную, вследствие чего был проведен опрос. Результаты ниже на рисунке:



Рисунок 2 – Результаты опроса российских компаний в сфере информационной безопасности на вопрос о миграции на отечественную   
продукцию [1]

Из результатов проведенного опроса видно, что большинство опрошенных высказывают поддержку перехода на отечественные решения в области сетевой безопасности.

При рассмотрении зарубежного опыта использования средств для обеспечения информационной безопасности можно отметить, что ведущие страны на Западе успешно осуществляют свою национальную политику в области информационной безопасности.

Самые передовые и надежные системы защиты информации активно применяются в США, Израиле, Германии, Великобритании и Китае. Это связано с тем, что эти страны постоянно подвергаются сильному внешнему информационному влиянию и, следовательно, вынуждены разрабатывать собственные национальные системы защиты. Такие системы обладают активными компонентами, которые позволяют проводить информационные   
и психологические операции, а также кибератаки против стран-противников.

Система информационной безопасности Соединенных Штатов Америки отличается высокой эффективностью. Ее широкая база охватывает все сферы жизни и имеет многомерный характер, при этом подчиняется общей доминирующей стратегии.

Законодательство тщательно регулирует вопросы обеспечения безопасности информации в компьютерных системах государства, противодействия киберпреступности и защиты прав граждан на доступ к информации и конфиденциальность личной жизни [10]:

* закон «О компьютерной безопасности»;
* закон «О совершенствовании информационной безопасности»;
* закон «О компьютерном мошенничестве и злоупотреблениях»;
* закон «О злоупотреблении компьютерами»;
* закон «О свободе информации»;
* закон «Об освещении деятельности правительства»;
* закон «Об охране личных тайн».

В США существует административно-организационная система, которая направлена на координацию действий по обеспечению информационной безопасности и реализацию единой государственной политики. Ответственность за этот процесс лежит на президенте Соединенных Штатов Америки. Подобным образом, другие европейские страны с высоким уровнем жизни также придают большое значение развитию информационной безопасности, основываясь на своих национальных политиках и принципах защиты населения от угроз и рисков, характерных для современного информационного общества [10].

Во Франции сфера информационной безопасности вместе с информационным сектором, является одной из важных областей жизни, наряду с экономикой, политикой и культурой. Это означает, что информационная сфера обладает таким же высоким уровнем защиты, как   
и другие сферы деятельности. В результате этого можно заключить, что концепция современной многовекторной геостратегии, принимаемая французской правящей элитой, включает новый элемент, который непосредственно влияет на оперативное принятие решений государственными и негосударственными организациями, СМИ и национальными специальными службами, вовлеченными в процесс внедрения и реализации   
стратегии. Таким образом, информационное пространство во Франции является одним из приоритетных объектов защиты, обеспечиваемых с помощью соответствующего законодательства, организационных мер, административных решений, властных действий и информационных технологий [10].

Политика информационной безопасности в Китайской Народной Республике отличается от подхода США и Франции и имеет более централизованный характер. Китайская стратегия включает моноцентрические, оборонительные и наступательные доктрины. Основная цель Китая состоит в интеграции в мировое сообщество в области информационной безопасности, при этом демократическая ориентация является фактором модернизации политической системы КНР и ее потенциального лидерства на региональном и международном уровне.

Проект «Великая китайская информационная стена» направлен на фильтрацию информации, проходящей через технические каналы   
и социальные сети внутри страны. Китайская Народная Республика достигла относительного успеха внутри своей стратегии, охватывая широкий спектр информации как внутри страны, так и за ее пределами. Китай имеет собственную уникальную модель стратегии, которая позволяет ему постепенно занимать лидирующие позиции среди крупных игроков в   
области информационной безопасности на мировой арене, даже конкурируя со США [10].

Таким образом, в мире существует разнообразие стран с различными подходами к государственному управлению, которые успешно реализуют национальную политику информационной безопасности с помощью различных стратегий, начиная от разработки систематизированной нормативной базы до использования разнообразных материальных ресурсов. Изучение успешного опыта ведущих стран позволяет получить выводы, которые могут положительно повлиять на решение многих проблем, существующих в настоящее время в сфере безопасности информационного пространства.

# Правовые основы обеспечения информационно‑функциональной составляющей экономической безопасности

В Российской Федерации правовая основа обеспечения экономической безопасности основывается на системе нормативных правовых актов. В части 1 статьи 8 Закона РФ "О безопасности" указывается, что систему безопасности образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, а также граждане, участвующие в обеспечении безопасности в соответствии с законом. Законодательство регулирует отношения в сфере безопасности.

Конституция Российской Федерации, Закон РФ «О безопасности», другие законы и нормативные акты Российской Федерации, а также нормативные акты республик в составе Российской Федерации и органов государственной власти регулируют обеспечение экономической безопасности. Кроме того, международные договоры и соглашения, заключенные или признанные Российской Федерацией, также играют роль в правовой основе.

Вопросы информационной безопасности регулируются специально принятыми федеральными законами. Целью законодательных мер в этой области является создание законодательной базы, которая устанавливает нормы поведения для субъектов и объектов информационных отношений   
и определяет ответственность за нарушение этих норм. Работа по созданию нормативной базы включает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание эффективной системы контроля за их исполнением.

В России законодательная база в области информационной безопасности включает федеральные законы, указы Президента РФ, постановления Правительства РФ, межведомственные руководящие документы и стандарты. Основополагающими документами являются Конституция РФ и Концепция национальной безопасности.

Конституция Российской Федерации гарантирует право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23, часть 2), а также право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (статья 29, часть 4). Конституция также гарантирует свободу массовой информации (статья 29, часть 5), что означает доступность массовой информации для граждан.

Концепция национальной безопасности РФ, введенная указом Президента РФ №24 в январе 2000 г., определяет важнейшие задачи обеспечения информационной безопасности Российской Федерации:

1. обеспечение осуществления гражданами Российской Федерации их конституционных прав и свобод в области информационной деятельности;
2. улучшение и защита национальной информационной инфраструктуры, включая интеграцию России в глобальное информационное пространство;
3. противодействие угрозе эскалации противоречий в сфере информации.

Для гарантирования гражданских прав в области информационных технологий и реализации задач информационной безопасности, описанных в Концепции национальной безопасности РФ, разрабатываются   
и усовершенствуются нормативные акты в области информационных технологий.

Основными законодательными актами Российской Федерации в области информационной безопасности и защиты информации являются:

1. закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне» с изменениями и дополнениями, которые были внесены после его принятия. Данный закон регулирует отношения, связанные с классификацией информации как государственной тайны, ее деклассификацией и защитой в целях обеспечения безопасности Российской Федерации;
2. закон Российской Федерации «Об информации, информатизации и защите информации» от 20 февраля 1995 года № 24-ФЗ является одним из основных базовых законов в области защиты информации. Он регулирует отношения, связанные с формированием, использованием и защитой информационных ресурсов Российской Федерации. Закон устанавливает принципы сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также регулирует создание и использование информационных технологий. Он также определяет права субъектов, участвующих в информационных процессах и информатизации,   
   и обеспечивает их защиту.

В соответствии с законодательством Российской Федерации, информационные ресурсы государства могут быть классифицированы на следующие пять категорий:

1. открытая общедоступная информация;
2. информация с ограниченным доступом;
3. информация, отнесенная к государственной тайне;
4. конфиденциальная информация;
5. персональные данные о гражданах.

Статья 22 Закона «Об информации, информатизации и защите информации» устанавливает права и обязанности субъектов в области защиты информации.

Необходимо отметить, что процесс создания законодательства является сложным. Вопросы защиты государственной тайны имеют более устойчивую законодательную систему, тогда как вопросы, связанные с защитой служебной, коммерческой и частной информации, часто содержат противоречия и несоответствия.

При разработке и применении законодательных и нормативно-правовых документов, а также при организации информационной безопасности, важно правильно ориентироваться во всей существующей законодательной базе в данной сфере.

Особое значение в системе правового регулирования информационных отношений придается ответственности субъектов за нарушения в сфере информационной безопасности. Это означает, что лица, нарушающие правила и требования в области информационной безопасности, должны нести ответственность за свои действия [21].

В Уголовном кодексе Российской Федерации, принятом в 1996 году, вопросам безопасности информации посвящены следующие главы и статьи:

* Глава 15: «Преступления против правосудия, публичного порядка и безопасности государства», включающая:

1. Статья 138: «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений»;
2. Статья 140: «Отказ в предоставлении гражданину информации»;
3. Статья 183: «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну»;
4. Статья 237: «Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей»;
5. Статья 283: «Разглашение государственной тайны»;
6. Статья 284: «Утрата документов, содержащих государственную тайну».

* Глава 28: «Преступления в сфере компьютерной информации», специально посвященная компьютерным преступлениям, включающая:

1. Статья 272: «Неправомерный доступ к компьютерной информации»;
2. Статья 273: «Создание, использование и распространение вредоносных программ для ЭВМ»;
3. Статья 274: «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

Эти статьи определяют уголовную ответственность за нарушения в области безопасности информации, включая различные аспекты, такие как разглашение тайны переписки, получение и распространение коммерческой или банковской тайны, нарушение государственной тайны, компьютерные преступления и другие.

# Оценка основных показателей информационной безопасности Краснодарского края

# Анализ индикаторов информационной составляющей экономической безопасности

Департамент информатизации и связи Краснодарского края играет ключевую роль на местном уровне в осуществлении региональной политики в сфере информатизации и обеспечении безопасности информации.

В рамках возложенных задач им выполняются следующие мероприятия:

* в 2008 году была учреждена региональная мультисервисная сеть органов государственной власти Краснодарского края (далее – РМС ОГВ), чтобы обеспечить взаимодействие между исполнительными органами власти Краснодарского края в единой телекоммуникационной и информационной среде.

На данный момент РМС ОГВ объединяет все государственные органы власти Краснодарского края, местные органы самоуправления районного уровня в муниципальных образованиях Краснодарского края, множество подразделений исполнительной власти Краснодарского края в районах,   
а также краевые учреждения. Расширение РМС ОГВ является постоянным процессом.

РМС ОГВ предоставляет пользователям такие сервисы, как доступ в интернет, почтовая служба, справочная правовая система, хостинг сайтов   
и порталов, портал информационного взаимодействия исполнительных органов государственной власти Краснодарского края, размещение специализированных государственных информационных систем и прочее.

* для обеспечения электронного взаимодействия между различными уровнями и органами исполнительной власти при предоставлении государственных и муниципальных услуг в Краснодарском крае была создана защищенная сеть – Региональная система межведомственного электронного взаимодействия (далее – РСМЭВ).

РСМЭВ включает в себя рабочие места в исполнительных органах государственной власти Краснодарского края и местного самоуправления. Сеть была создана в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных   
и муниципальных услуг» с целью организации электронного взаимодействия между различными ведомствами [22].

РСМЭВ является крупным инфраструктурным решением, созданным для системы межведомственного электронного взаимодействия. Оно обеспечивает доступ МФЦ (Многофункциональный центр предоставления государственных и муниципальных услуг) к органам государственной власти Краснодарского края, а также позволяет муниципальным образованиям использовать региональные сервисы РСМЭВ. Еще одной характеристикой РСМЭВ является возможность организации подсети органов власти, что позволяет реализовывать их внутренние проекты по защите информации.

Система межведомственного электронного взаимодействия   
(далее – СМЭВ) представляет собой информационную систему, которая включает в себя информационные базы данных. В этих базах данных содержатся сведения об используемых органами и организациями программных и технических средствах, которые обеспечивают доступ к электронным сервисам через СМЭВ. Также в системе содержатся сведения об истории передачи электронных сообщений в СМЭВ при предоставлении государственных и муниципальных услуг, а также другая информация, связанная с функционированием СМЭВ.

СМЭВ предназначена для решения следующих задач [9]:

* гарантирование выполнения государственных и муниципальных обязанностей с использованием электронных средств;
* обеспечение предоставления государственных и муниципальных услуг в электронном виде, включая применение универсальной электронной карты и федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг»;
* содействие электронному взаимодействию при предоставлении государственных и муниципальных услуг, а также выполнении государственных и муниципальных обязанностей.

Основными функциями СМЭВ являются:

* гарантирование передачи запросов, документов и информации, необходимых для получения государственных и муниципальных услуг от заявителей через централизованный портал, в информационные системы органов и организаций, которые обязаны предоставлять эти услуги;
* обеспечение обмена электронными сообщениями между органами и организациями, участвующими в системе взаимодействия, при предоставлении государственных и муниципальных услуг и выполнении государственных и муниципальных функций;
* передача на централизованный портал запросов, документов   
  и информации, обработанных в информационных системах органов   
  и организаций, а также предоставление информации о ходе выполнения запросов на предоставление государственных или муниципальных услуг и их результатов.

В рамках работы СМЭВ осуществляются следующие деятельности: консультирование органов государственной власти по вопросам, связанным с функционированием СМЭВ; помощь в подготовке и отправке заявок на получение доступа к электронным сервисам; регистрация информационных систем и их перерегистрация; разрешение проблемных вопросов   
и устранение неполадок в работе СМЭВ.

На данный момент в Краснодарском крае к системе межведомственного электронного взаимодействия подключены 15 органов исполнительной власти Краснодарского края, которые предоставляют 88 государственных услуг в электронной форме [9].

В рамках программы «Цифровая экономика» в Краснодарском крае были утверждены пять проектов на период с 2019 года до конца 2024 года:

1. «Информационная инфраструктура»;
2. «Информационная безопасность»;
3. «Цифровые технологии»;
4. «Кадры для цифровой экономики».

Реализация данных проектов является одним из наиболее популярных и актуальных показателей развития различных общественных институтов, таких как образование, наука, культура, медицина и экономика. Они способствуют благополучию Краснодарского края. Эта тенденция связана прежде всего с положительными количественными и качественными результатами программы развития, которые эффективно влияют на экономику и создают новые возможности для дальнейшего улучшения состояния рынка.

* 1. информационная инфраструктура.

Основная задача данного проекта заключается в разработке и реализации собственной конкурентоспособной информационной инфраструктуры на территории Краснодарского края, основанной на отечественных разработках.

Рисунок 3 – Финансовое обеспечение реализации регионального   
проекта, в млн. руб. (составлено автором по материалам [15])

Как мы можем увидеть из рисунка 3, общая сумма финансирования проекта по сравнению с 2019 году уменьшилась более чем в 3,5 раза, после чего в 2022 году кратно увеличилось почти в 5 раз.

В рамках проекта была разработана и внедрена региональная мультисервисная сеть, предназначенная для связи и обмена информацией между органами государственной власти Краснодарского края. Эта сеть обеспечивает обработку и хранение данных, необходимых для эффективного исполнения функций органов власти.

Важной составляющей проекта является создание, развитие   
и распространение цифровых платформ. Они предназначены для повышения цифровой грамотности населения, участников бизнеса и государственных служащих. Эти платформы предоставляют обучение и помощь в освоении цифровых технологий, чтобы улучшить навыки владения ими, а также усилить безопасность.

Для реализации проекта «Цифровая инфраструктура» в Краснодарском крае была привлечена активная поддержка инвесторов. Администрация края активно проводила поиск потенциальных партнеров для сотрудничества. В результате успешно были заключены соглашения о взаимодействии в области инвестиций, а также найдены инвесторы-операторы связи и современных информационных сервисов. Это позволило добиться развития и расширения цифровой инфраструктуры в регионе.

Можем констатировать некоторые результаты [9]:

* разработана и введена в эксплуатацию Региональная геоинформационная система Краснодарского края, которая представляет собой централизованную базу данных об информационных системах региона.
* создана технологическая площадка для центра обработки данных исполнительных органов государственной власти Краснодарского края, обеспечивающая эффективную обработку и хранение информации.
* была создана и продолжает развиваться надежная инфраструктура, предназначенная для региональной сети исполнительных органов Краснодарского края.
  1. информационная безопасность.

Основной задачей данного проекта является обеспечение устойчивости и безопасности цифровой информационно-телекоммуникационной инфраструктуры Краснодарского края. Для достижения этой цели применяются отечественное программное обеспечение и высокоскоростные технологии передачи, обработки и хранения больших объемов данных для всех организаций и домохозяйств региона. Основное внимание уделяется эффективной защите прав и законных интересов личности, бизнеса и региона от угроз информационной безопасности.

На проект было выделено 147,8 млн рублей. Финансирование по годам иллюстрирует рисунок 4.

Рисунок 4 – Финансовое обеспечение регионального проекта «Информационная безопасность», данные приведены в млн. рублей (составлено автором по материалам [15])

Однако, несмотря на наличие инновационных технологий, нового программного обеспечения, антивирусных программ, систем обнаружения кибератак и центров мониторинга информационной безопасности, тяжелые последствия могут быть неизбежными, если население не повысит свою цифровую грамотность. Это подтверждает тесную взаимосвязь и взаимозависимость всех пяти региональных проектов Краснодарского края в рамках программы «Цифровая экономика».

Согласно данным «Лаборатории Касперского», самым распространенным видом фишинга является попытка обмануть пользователя, предложив ему фальшивое вознаграждение на фишинговой странице. Из-за недостаточной цифровой грамотности среди населения происходят случаи кражи денежных средств со счетов граждан, несмотря на существующие технологии и сервисы по борьбе с кибератаками. Это говорит о том, что защита от киберугроз требует не только развития и совершенствования технических средств, но и обучения пользователей основам кибербезопасности.

В настоящее время все больше усилий направляется на повышение осведомленности населения о методах атак и приемах защиты. Различные организации и учреждения проводят образовательные мероприятия, семинары и курсы, чтобы научить людей распознавать подозрительные сообщения, не доверять подозрительным ссылкам и быть внимательными при обработке личной информации.

Но помимо обучения, необходимо и практическое применение полученных знаний. Пользователи должны следовать базовым правилам безопасности, таким как регулярное обновление программного обеспечения, использование надежных паролей, ограничение доступа к личной информации и осмотрительное поведение в сети.

Только совместные усилия государства, бизнеса и общества могут обеспечить эффективную защиту от киберугроз. Технологические решения должны сочетаться с повышением осведомленности и ответственности каждого человека в цифровом пространстве.

Для реализации проекта были выделены несколько направлений работы:

1. обеспечение информационной безопасности государственных органов Краснодарского края. Задача была выполнена в соответствии с запланированными показателями. В настоящее время введена в эксплуатацию система обеспечения информационной безопасности исполнительной власти и органов местного самоуправления, создан центр мониторинга информационной безопасности, а также внедрены подсистемы антивирусной защиты и обнаружения компьютерных атак.

Таблица 2 – Доля закупаемого и (или) арендуемого отечественного ПО (составлено автором по материалам [19])

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Единица измерения | Базовое значение | Период, год | | |
| 2019 | 2020 | 2021 |
| Процент | 0 | 0 | 70 | 75 |

1. применение отечественного программного обеспечения. Для достижения этой цели были организованы мероприятия, представленные на рисунке 5. После реализации этих мероприятий доля закупаемого или арендуемого отечественного ПО органами исполнительной власти и местного самоуправления в 2021 году составила 70 процентов, в то время как в 2019 году этот показатель был нулевым, как указано в таблице;
2. создание устойчивой и безопасной инфраструктуры, которая обеспечивает высокоскоростную передачу, обработку и хранение больших объемов данных.

Целью данного направления является доступность такой инфраструктуры для всех организаций и домохозяйств Краснодарского края. Это позволит эффективно использовать информационные ресурсы и обеспечить безопасность данных при их передаче и обработке. На таблице 3 указано, как именно менялось время простоя государственных информационных систем на промежутке 2019-2021 гг.

Исходя из приведенных данных можно сделать несколько выводов:

* средний срок простоя государственных информационных систем в результате компьютерных атак значительно снизился в течение нескольких лет;
* количество подготовленных специалистов в области информационной безопасности с использованием в образовательном процессе отечественных комплексов и средств защиты информации значительно выросло;

Изображение выглядит как текст, чек, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 5 – Процесс разработки и внедрения отечественного ПО   
(составлено автором по материалам [15])

* стоимостная доля закупаемого и (или) арендуемого федеральными органами исполнительной власти, органами исполнительной власти субъектов и иными органами государственной власти отечественного программного обеспечениякратно выросла.

Таблица 3 – Средний срок простоя государственных информационных систем в результате компьютерных атак (составлено автором по материалам [19])

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Единица измерения | Базовое значение | Период, год | | |
| 2019 | 2020 | 2021 |
| Час | 65 | 48 | 24 | 18 |

По итогу 2022 года, были выявлены определенные результаты [19]:

* было закуплено оборудование, ПО и прочие услуги по обеспечению безопасности информационных ресурсов, размещенных в РМС ОГВ;
* показатель импортозамещения при проведении закупки органами исполнительного власти отечественного ПО достиг 95%;
* была реализована защита краевой государственной IT‑инфраструктуры от кибератак из сети «Интернет».
  1. цифровые технологии.

Цель проекта состоит в достижении быстрого внедрения отечественных цифровых решений в экономике и социальной сфере. Это достигается путем партнерства между администрацией региона и коммерческими организациями, а также поддержки и стимулирования разработчиков, стартапов и производителей отечественного программного обеспечения.

В рамках этого процесса теоретически могут проводиться конкурсы на предоставление грантов для внедрения отечественных сервисов и платформ. Предположим, что такие конкурсы будут запущены с целью стимулирования развития и реализации инновационных решений в области кибербезопасности и цифровых технологий.

Возможные направления таких конкурсов могут включать:

1. разработка новых методов обнаружения и защиты от кибератак: Конкурсы могут поощрять разработку инновационных технологий, которые обеспечивают эффективную защиту информации и систем от киберугроз;
2. создание безопасных платформ и сервисов: Гранты могут быть предоставлены для разработки и внедрения платформ и сервисов, которые обеспечивают высокий уровень защиты данных и личной информации пользователей;
3. повышение осведомленности и обучение в области кибербезопасности: Конкурсы могут фокусироваться на разработке и реализации образовательных программ, целью которых является повышение цифровой грамотности и осведомленности населения о методах предотвращения кибератак;
4. интеграция новых технологий в сферу кибербезопасности: Гранты могут способствовать разработке и внедрению инновационных технологий, таких как искусственный интеллект, блокчейн или интернет вещей, для обеспечения безопасности в цифровой среде.

Таблица 4 – Направления грантовой поддержки проектов по внедрению отечественных цифровых решений (составлено автором по материалам [15])

|  |  |  |
| --- | --- | --- |
| Наименование | Направление | Бюджет |
| Компаниям разработчикам | Разработка и развитие цифровых технологий | до 300 млн руб. |
| Компаниям на внедрение новых цифровых решений | Первое коммерческое внедрение отечественных цифровых решений | до 20 млн руб. |
| IT-стартапам | Поддержка развития IT-стартапов | до 80 млн руб. |
| Компаниям на цифровую трансформацию | Поддержка компаний‑разработчиков ПО | до 30 млн руб. |

Власти Краснодарского края планируют продолжать поддержку грантовых программ до 2024 года и продолжают получать федеральные гранты на реализацию региональных проектов. Реализацией данных программ и направлений занимаются Российский фонд развития информационных технологий, фонд содействия информациям и Сколково.

В конце 2020 года был принят региональный закон, поддерживающий развитие IT-сферы и показывающий готовность властей Краснодарского края к сотрудничеству с активными российскими IT-компаниями.

Важно привлекать разработчиков не только из самого региона, но и из других регионов России. Это позволит создать новые рабочие места и увеличить долю отечественных IT-компаний.

Таким образом, администрация Краснодарского края активно осуществляет политику в рамках регионального проекта «Цифровые технологии» и региональной программы «Цифровая экономика» совместно с отечественными компаниями и привлечением инвестиций. Это уже приводит к первым положительным результатам и открывает перспективы для дальнейшего развития.

* 1. кадры для цифровой экономики.

Цель проекта заключается в подготовке высококвалифицированных кадров в области цифровых знаний и навыков через профессиональное образование. Реализация программы направлена на обучение информационно-цифровым компетенциям школьников, студентов, сотрудников организаций, органов власти и органов местного самоуправления в Краснодарском крае.

В сфере образования активно проводятся мероприятия, нацеленные на создание новых образовательных программ, с акцентом на цифровую экономику.

Из таблицы 5 можно увидеть количество специалистов, подготовленных в области информационной безопасности с использованием отечественных высокотехнологических комплексов и средств защиты информации. Проведение мероприятий по привлечению молодых специалистов в эту область может способствовать увеличению числа квалифицированных специалистов в регионе.

Таблица 5 – Количество подготовленных специалистов (составлено автором по материалам [19])

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Единица измерения | Базовое значение | Период, год | | |
| 2019 | 2020 | 2021 |
| Тысяча человек | 0,00 | 0,00 | 0,19 | 0,23 |

Суммируя результаты регионального проекта, можно сделать вывод, что благодаря созданию благоприятных условий для жизни, развитию человеческого капитала и росту предпринимательской активности, программа «Цифровая экономика» становится более качественной и эффективной,   
а уровень информационной безопасности региона повышается, проблемы устраняются. Представленные в таблицах и рисунках показатели Краснодарского края непрерывно улучшаются с каждым годом, что свидетельствует о большом потенциале региона, его человеческих ресурсах   
и активном экономическом населении.

# Выявление угроз информационной составляющей экономической безопасности

В ходе анализа различных индикаторов информационной составляющей экономической безопасности мы пришли к выводу, что несмотря на некоторое количество проблем региона, тенденция сказывается довольно-таки положительная. Однако нужно понимать, как именно нам надо выявлять угрозы, чтобы устранять их как можно раньше.

Выявление осуществляется через несколько ключевых шагов:

* 1. анализ информационной инфраструктуры;

Проводится оценка состояния информационной инфраструктуры региона, включая системы связи, электронные базы данных, сетевые системы и другие элементы, которые могут быть подвержены угрозам.

Так, например, в рамках аппаратно-программного комплекса по результатам проведенного анализа существующих на территории муниципальных образований Краснодарского края было определено, что на сегодняшний день на территории Краснодарского края функционирует 3644 камеры видеонаблюдения, охватывающих парки, скверы, места массового скопления граждан, а также наиболее оживленные перекрестки   
улично-дорожной сети.

При определении требуемого количества камер принималось во внимание обеспечение безопасности всей среды обитания населения и гостей Краснодарского края, а именно, приоритетная установка на территории жилых зон населенных пунктов, общественных и административных зданий   
и сооружений, объекты промышленного и сельскохозяйственного производства, транспортной инфраструктуры, связи, радио- и телевещания, технической сооружений и т.д. [8].

* 1. идентификация уязвимостей;

Этот шаг включает анализ и тестирование систем на уязвимости. Цель состоит в том, чтобы определить потенциальные слабые места   
в информационной инфраструктуре, которые могут быть использованы злоумышленниками для несанкционированного доступа, атак и нарушения информационной безопасности. Это может включать поиск уязвимостей в программном обеспечении, недостатки в настройках системы, недостаточную защиту сетей и другие слабые точки.

Идентификация уязвимостей в информационной инфраструктуре Краснодарского края происходит с помощью различных методов   
и инструментов. Приведем общий пример процесса идентификации уязвимостей:

1. сбор информации;

Начинается со сбора информации о системах, сетях и программном обеспечении, используемых в Краснодарском крае. Это может включать инвентаризацию серверов, компьютеров, сетевых устройств, баз данных   
и других элементов информационной инфраструктуры.

1. сканирование;

С помощью специальных инструментов проводится сканирование систем на предмет наличия уязвимостей. Программы-сканеры просматривают сети и системы на наличие известных уязвимостей, используя базы данных с информацией о них. Например, можно использовать инструменты, такие как Nessus, OpenVAS или Qualys.

1. анализ результатов;

После сканирования полученные результаты анализируются для идентификации уязвимостей. Уязвимости могут быть связаны с открытыми портами, устаревшими версиями программного обеспечения, неправильными настройками безопасности или другими проблемами.

1. оценка уровня риска.

Определяется уровень риска для каждой выявленной уязвимости. Учитываются такие факторы, как вероятность эксплуатации уязвимости злоумышленниками, потенциальный ущерб, степень важности системы   
и доступность патчей или решений.

Например, в ходе сканирования может быть выявлено, что в одной из местных государственных организаций используется устаревшая версия управляющей системы для контроля финансовых операций. По базе данных уязвимостей известно, что данная версия имеет некоторые известные уязвимости, позволяющие потенциальным злоумышленникам получить несанкционированный доступ к финансовым данным. Таким образом, эта уязвимость идентифицирована и требует мер по обновлению системы или применению патчей для устранения уязвимости и уменьшения риска эксплуатации.

* 1. оценка уровня риска;

В процессе оценки уровня риска для информационной составляющей экономической безопасности на региональном уровне проводится анализ различных факторов и параметров. Приведем более подробное описание этого шага:

1. вероятность возникновения угроз;

Оценивается вероятность возникновения угроз информационной безопасности. Это включает изучение статистики и трендов в области кибербезопасности, анализ исторических данных об инцидентах и угрозах,   
а также учет существующих уязвимостей в информационной инфраструктуре Краснодарского края.

1. потенциальный ущерб;

Оценивается потенциальный ущерб, который может быть причинен экономической безопасности Краснодарского края в результате нарушения информационной безопасности. Это может включать финансовые потери, потерю конфиденциальности важных данных, нарушение бизнес-процессов, ухудшение репутации и другие негативные последствия.

1. степень подготовленности и защищенности систем;

Оценивается степень подготовленности и защищенности информационной инфраструктуры регионального уровня. Это включает изучение существующих мер безопасности, таких как политики и процедуры, системы управления безопасностью, наличие антивирусных программ, межсетевых экранов и других средств защиты. Оценивается эффективность   
и соответствие существующих мер безопасности уровню угроз и рискам.

1. возможные последствия нарушений.

Оценивается возможные последствия нарушений информационной безопасности для экономической безопасности Краснодарского края. Это включает анализ влияния на ключевые отрасли и секторы экономики, зависимости от информационных систем и технологий, а также социальные   
и политические последствия. Оценка последствий помогает определить, какие угрозы и риски являются наиболее критическими и требуют срочных мер по укреплению информационной безопасности.

В результате оценки уровня риска формируется общее представление о текущем состоянии информационной безопасности региона и определяются приоритеты и стратегия по укреплению безопасности. Это позволяет принимать обоснованные решения по внедрению соответствующих мер   
и механизмов для защиты информационной инфраструктуры Краснодарского края от угроз.

* 1. мониторинг и обнаружение инцидентов.

Для выявления угроз информационной безопасности региональной информационной составляющей необходимо установить системы мониторинга и обнаружения аномальной активности. Эти системы могут включать специализированное программное обеспечение, которое анализирует данные о сетевой активности, регистрирует события и ищет признаки несанкционированного доступа или атак.

Для этого применяются следующие действия:

1. установка систем мониторинга;

Региональные организации могут использовать специализированное программное обеспечение или аппаратные средства для мониторинга информационной инфраструктуры. Эти системы позволяют собирать данные о сетевой активности, журналах событий, регистрировать действия пользователей и другую информацию, связанную с безопасностью. Они работают в режиме реального времени, анализируя данные на предмет необычных или подозрительных паттернов.

1. обнаружение аномальной активности;

Системы мониторинга проводят анализ активности и ищут признаки, которые могут указывать на наличие несанкционированного доступа или атаки. Например, они могут обнаружить необычные запросы к сетевым ресурсам, повышенную активность в определенных частях сети или неправильные попытки аутентификации. Такие аномалии могут указывать на возможные угрозы безопасности.

1. анализ и реагирование на инциденты;

Когда системы мониторинга обнаруживают потенциальные инциденты или аномалии, следует проводить анализ и реагирование на них. Это может включать исследование подробностей инцидента, определение его серьезности и приоритета, а также принятие соответствующих мер для предотвращения дальнейшего распространения или повреждения. Реагирование на инциденты может включать блокирование угрозы, восстановление системы, сбор и анализ доказательств, а также информирование соответствующих структур и органов об инциденте.

1. улучшение системы мониторинга.

Процесс мониторинга и обнаружения инцидентов требует постоянного совершенствования и улучшения. Это может включать обновление систем мониторинга, внедрение новых.

# Разработка мероприятий по обеспечению информационной функциональной составляющей экономической безопасности

# Основные направления снижения угроз экономической безопасности

Целью системы информационной безопасности Краснодарского края является нивелирование негативного воздействия от внешних и внутренних угроз и обеспечение сохранности данных.

Для того, чтобы выявить слабые и сильные стороны, а также угрозы   
и возможности региона, была составлена таблица SWOT-анализа (таблица 6).

Таблица 6 – SWOT-анализ Краснодарского края (составлено автором по материалам [18])

|  |  |
| --- | --- |
| Направление | Характеристика |
| Сильные стороны | * наличие развитой информационной инфраструктуры, включая сети связи и центры обработки данных; * наличие высококвалифицированных специалистов в области информационной безопасности; * сотрудничество с международными организациями и соседними регионами в области информационной безопасности. |
| Слабые стороны | * недостаточная осведомленность и обученность населения в области информационной безопасности; * отсутствие современных отечественных систем мониторинга и защиты информации на муниципальном уровне; * отсутствие обязательных норм и стандартов информационной безопасности для государственных и частных организаций; |
| Возможности | * создание собственного центра компетенции по информационной безопасности; * укрепление партнерств с ведущими кибербезопасными организациями; |
| Угрозы | * рост киберпреступности и угрозы для информационных систем; * возможность кибершпионажа и кибератак со стороны других государств или киберпреступных группировок; * уязвимость киберинфраструктуры к новым видам атак и угрозам;   распространение вредоносного программного обеспечения и киберугроз через социальные сети и электронную почту |

SWOT-анализ информационной безопасности Краснодарского края выявляет важные аспекты, которые необходимо учесть при разработке стратегии и мер для улучшения информационной безопасности в регионе.

Внимание к сильным сторонам позволяет Краснодарскому краю строить на основе развитой информационной инфраструктуры и наличия высококвалифицированных специалистов центра компетенции по информационной безопасности и развития инновационных технологий в различных секторах экономики. Благодаря этим факторам регион может оперативно реагировать на угрозы и эффективно противодействовать кибератакам. Кроме того, Краснодарский край обладает развитыми центрами образования и научно-исследовательскими институтами, что создает благоприятную среду для разработки новых технологических решений в области информационной безопасности.

Однако анализ также выявляет некоторые слабые стороны, которые требуют пристального внимания. Недостаточная осведомленность   
и обученность населения в области информационной безопасности является одной из главных слабостей. Это может привести к ошибкам и неправильным действиям, которые могут создать дополнительные уязвимости для кибератак. Кроме того, на муниципальном уровне отсутствуют современные системы мониторинга и защиты информации, что ослабляет общую информационную безопасность региона. Также отсутствие обязательных норм и стандартов для государственных и частных организаций создает пробелы в области защиты информации и усиливает риски.

Говоря о возможностях, мы не можем не отметить, что предоставляемые Краснодарскому краю возможности являются потенциалом для улучшения информационной безопасности. Наличие развитой информационной инфраструктуры, специалистов в области информационной безопасности   
и инновационных технологий предоставляет широкие возможности для реализации современных методов защиты информации. Однако для того, чтобы реализовать этот потенциал, необходимо уделить особое внимание пунктам SWOT-анализа и активно работать над их выполнением.

Угрозы, такие как рост киберпреступности, уязвимость киберинфраструктуры и кибершпионаж, требуют немедленных мер для защиты информации. Для предотвращения таких угроз необходимо разработать и внедрить соответствующие решения. Важно создать системы мониторинга и обнаружения инцидентов, усилить защиту сетей   
и информационных ресурсов, а также повысить осведомленность   
и обученность персонала в области информационной безопасности. Необходимо также укрепить сотрудничество с правоохранительными органами и международными организациями для борьбы с киберугрозами.

Таким образом, SWOT-анализ информационной безопасности Краснодарского края позволяет выявить сильные и слабые стороны, а также возможности и угрозы. На основе этого анализа можно разработать стратегию и меры для улучшения информационной безопасности в регионе. При этом необходимо активно использовать сильные стороны региона, решать выявленные проблемы и укреплять систему защиты информации для минимизации рисков и обеспечения стабильности информационного пространства Краснодарского края.

Для повышения экономической безопасности Краснодарского края требуется разработать специальный механизм, который обеспечит эту безопасность. Механизм обеспечения информационной безопасности представляет собой систему мер, организационно-экономических и правовых, направленных на предотвращение экономических угроз. Основной целью такого механизма является создание благоприятных условий для жизни и развития личности, обеспечение социальной, экономической и политической стабильности общества, а также противодействие внутренним и внешним угрозам информационной безопасности, а также сохранение единства и государственности России.

Механизм обеспечения информационной безопасности включает в себя следующие компоненты:

* мониторинг факторов для прогнозирования и предотвращения угроз экономической безопасности;
* разработка пороговых значений информационных показателей;
* действия государства по преодолению или предотвращению угроз экономической безопасности.

Механизм обеспечения информационной безопасности Краснодарского края выполняет несколько важных функций, включая защитную, регулирующую, превентивную, инновационную и социальную функции.

Для обеспечения устойчивого развития информационного сектора необходимо предпринять следующие меры:

1. повышение инвестиций в научно-технический прогресс. Региональные органы власти должны увеличить финансирование и поддержку научных исследований, инноваций и разработок в информационной сфере. Это позволит стимулировать создание новых технологий и продуктов, способствующих развитию отрасли;
2. развитие цифровой инфраструктуры. Важно обеспечить широкий доступ к высокоскоростному интернету и современным информационным технологиям во всех регионах. Региональные органы власти должны инвестировать в создание и модернизацию цифровой инфраструктуры, включая строительство оптоволоконных сетей, развертывание беспроводных технологий и создание инновационных центров;
3. поддержка стартапов и инновационных проектов. Региональные власти должны предоставить специальные программы поддержки для молодых предпринимателей и стартапов в информационной сфере;
4. содействие цифровой грамотности. Важно осуществлять программы по повышению уровня цифровой грамотности среди населения, включая обучение основам информационных технологий, безопасности в сети и эффективному использованию цифровых ресурсов. Это позволит создать общество, способное активно участвовать в цифровом развитии и использовании информационных технологий;
5. сотрудничество с международными партнерами. Региональные органы власти должны активно развивать партнерские отношения с зарубежными странами, международными организациями и компаниями в области информационных технологий. Это поможет привлечь инвестиции, обменяться опытом и новыми технологиями, а также расширить международные рынки для местных IT-компаний.

# Разработка мероприятий по совершенствованию защиты информационной составляющей экономической безопасности

Как было продемонстрировано в предыдущей главе, Краснодарский край имеет хорошую тенденцию к развитию и устранению проблем информационной составляющей экономической безопасности. Разберемся, в каком направлении нужно двигаться, чтобы улучшить результат.

Ознакомиться с предложениями можно с помощью таблицы 7.

Таблица 7 – Основные направления снижения угроз в Краснодарском крае (составлено автором по материалам [13])

|  |  |  |  |
| --- | --- | --- | --- |
| Вид угроз | Характеристика угроз | Мероприятия | Ожидаемый эффект |
| Кибератаки | Несанкционированный доступ к информационным ресурсам и сетям, взломы, вирусы и вредоносное ПО | * развитие систем защиты информационных ресурсов и инфраструктуры; * обучение сотрудников основам информационной безопасности; * разработка и применение антивирусных  и антихакерских программ. | Защита информационных ресурсов от несанкционированного доступа, снижение риска инфицирования вирусами и вредоносным ПО |

Продолжение таблицы 7

|  |  |  |  |
| --- | --- | --- | --- |
| Вид угроз | Характеристика угроз | Мероприятия | Ожидаемый эффект |
| Утечка конфиденциальной информации | Неправомерное раскрытие и передача конфиденциальной информации | * разработка политик и процедур обработки информации; * обучение сотрудников правилам использования информационных ресурсов; | Предотвращение утечки конфиденциальной информации и сохранение ее целостности |
| Недостаточная осведомленность сотрудников  и населения | Отсутствие знаний  и навыков по основам информационной безопасности | * проведение обучающих программ и тренингов; * разработка внутренних политик и процедур обращения с информацией. | Повышение осведомленности персонала о рисках  и методах предотвращения угроз информационной безопасности |
| Ограниченные ресурсы  и техническая база | Недостаток финансовых и технических ресурсов для развития систем защиты информации | * развитие инфраструктуры связи и информационных технологий; * повышение финансирования на развитие систем безопасности. | Улучшение технической базы  и возможностей для эффективной защиты информации |

Для сокращения рисков, связанных с обеспечением высокого уровня информационной безопасности Краснодарского края, можно применить следующие меры:

1. реализация экономического проекта, направленного на усиление инвестиций в разработку современного оборудования;
2. поддержка научно-технического потенциала и повышение конкурентоспособности экономики края по сравнению с другими регионами Российской Федерации;
3. повышение устойчивости экономики для минимизации ущерба от внешних и внутренних угроз;
4. фокусировка внимания на осведомленности и обучении населения информационной безопасности. Важно внедрить эту практику в образовательные программы школ и университетов, включив специальный предмет, который поможет детям и студентам понимать важность разбираться в информации в современном мире;
5. участие региональных властей в создании образовательных программ с использованием отечественного оборудования;
6. обучение сотрудников муниципальных органов основам информационной безопасности, чтобы они получили базовые знания о безопасности, осознали риски кибератак и научились применять правила и процедуры безопасного обращения с информацией;
7. проведение обучающих тренингов и курсов для людей, чтобы они могли быстро адаптироваться к компьютерным технологиям и не поддаваться на фишинговые атаки в социальных сетях;
8. внедрение в систему государственных и муниципальных учреждений нового отечественного программного обеспечения для предотвращения взломов и кибератак;
9. разработка политик и процедур обработки информации, которые устанавливают основные принципы, цели и задачи в области безопасности, определяют конкретные шаги и действия для обработки и защиты информации, включая процедуры регистрации и классификации информации, контроль доступа, резервное копирование и т.д.;
10. создание федеральных и региональных нормативных актов и стандартов, которые детализируют требования к обработке информации, методы и средства защиты, процедуры аудита и контроля, а также устанавливают ответственность за нарушение требований и протоколов информационной безопасности;
11. постоянный мониторинг и обновление процедур с учетом изменений обстановки, чтобы система оставалась актуальной, несмотря на внешние и внутренние угрозы, развитие технологической базы и изменения законодательства;
12. разработка и применение антивирусных и антихакерских программ. Важно установить антивирусные программы на компьютеры и серверы для обнаружения и блокировки вредоносных программ, которые могут негативно сказаться на работоспособности;
13. проведение регулярных проверок системы на уязвимости и атаки для своевременного обнаружения и предотвращения несанкционированного доступа.

Кроме того, разработка системы показателей должна основываться на широком вовлечении заинтересованных сторон, включая экспертов, представителей бизнес-сообщества и общественности. Их мнения и предложения помогут учесть разнообразные аспекты информационной безопасности и обеспечить комплексный подход к её модернизации.

Дополнительно, необходимо уделить внимание сбору и анализу данных, связанных с информационной безопасностью. Регулярное обновление и мониторинг этих данных позволит оперативно реагировать на новые угрозы и вызовы в сфере информационной безопасности. Также следует развивать системы раннего предупреждения и обмена информацией о новых уязвимостях и атаках, чтобы обеспечить эффективное реагирование и защиту информационных ресурсов.

Кроме того, важно осуществлять постоянное обучение и повышение квалификации специалистов в области информационной безопасности. Это позволит им быть в курсе последних тенденций и разработок в области кибербезопасности и эффективно противодействовать новым видам угроз.

Таким образом, модернизация системы обеспечения информационной безопасности Краснодарского края требует не только разработки системы показателей, но и широкого сотрудничества заинтересованных сторон, усиления сбора и анализа данных, развития систем предупреждения и обучения специалистов в данной области. Это позволит региону эффективно справляться с современными угрозами информационной безопасности и обеспечить устойчивое развитие в цифровую эпоху.

Кроме того, считаем необходимым упомянуть о потребности в утверждении Постановления Правительства РФ «О мерах по реализации Государственной стратегии экономической безопасности». Данный нормативно-правовой акт станет тем регулятором процессов обеспечения экономической безопасности регионов РФ, на основании которого будут разрабатываться их собственные стратегии и методики оценки данного состояния.

Для обеспечения устойчивости информационной безопасности Краснодарского края также требуется регулярное проведение аудита с целью оценки текущего уровня защищенности систем и выявления уязвимостей. На основе результатов аудита следует разработать и внедрить политики и процедуры информационной безопасности, которые устанавливают правила и требования для защиты информационных ресурсов.

Помимо этого, необходимо принять физические и логические меры защиты. Физические меры включают контроль доступа к серверным комнатам и применение систем видеонаблюдения. Логические меры, такие как брандмауэры и системы обнаружения вторжений, обеспечивают контроль доступа и обнаружение аномальной активности. Важно также разработать план реагирования на кибератаки, определить роли и обязанности персонала для эффективного реагирования на инциденты.

Чтобы обеспечить надежность систем защиты, необходимо регулярно обновлять программное и аппаратное обеспечение, а также проводить тестирование их эффективности. Эти меры помогут улучшить уровень защиты и минимизировать риски нарушения информационной безопасности.

Однако модернизация системы информационной безопасности Краснодарского края также требует развития кадрового потенциала в этой области. Необходимо предоставить специалистам возможности повышения квалификации и обучения в области информационной безопасности. Активное сотрудничество с вузами и исследовательскими центрами поможет привлечь и подготовить новых кадров, обеспечивая наличие высококвалифицированных специалистов для решения задач в сфере информационной безопасности.

Таким образом, модернизация системы информационной безопасности Краснодарского края требует проведения аудита, разработки политик и процедур, принятия физических и логических мер защиты, разработки плана реагирования на кибератаки, обновления программного и аппаратного обеспечения, а также развития кадрового потенциала в данной области. Эти меры содействуют повышению уровня информационной безопасности и обеспечению устойчивого развития региона.

Одной из ключевых задач модернизации системы обеспечения информационной безопасности Краснодарского края является совершенствование механизмов взаимодействия между органами государственной власти, муниципалитетами, частным сектором и населением. Необходимо создать механизмы для оперативного информационного обмена и координации действий в случае возникновения киберугроз.

Для успешной модернизации информационной безопасности региона необходимо также привлечь инвестиции. Это позволит выделить средства на внедрение новых технологий, закупку современного оборудования и развитие необходимой инфраструктуры. Важно провести анализ финансовых ресурсов и разработать планы по оптимизации расходов и повышению эффективности использования средств.

В целом, модернизация системы обеспечения информационной безопасности Краснодарского края требует комплексного подхода и внедрения мер, направленных на улучшение инфраструктуры, повышение квалификации персонала, разработку стратегии и политик, а также установление эффективных механизмов взаимодействия и привлечение инвестиций. Это позволит обеспечить надежную защиту информации и повысить уровень информационной безопасности в регионе.

Модернизация систем обеспечения информационной безопасности Краснодарского края предполагает деятельность в области совершенствования методологических и технологических основ данного процесса. Так, первым этапом становится формирование системы показателей для проведения соответствующего мониторинга. Данные значения станут материалом для фактического сравнения степени успешности действий руководства исследуемого региона с другими регионами РФ. Чтобы данные были более объективными, показатели следует разрабатывать на федеральном уровне, после чего адаптировать их для отдельных территориальных образований.

Эти индикаторы необходимы для обоснования стратегии развития региона, которая разрабатывается руководством региона. В данном исследовании система показателей включает в себя индикаторы, разделённые на следующие виды в зависимости от их принадлежности к определенной сфере человеческой жизни: финансовые, социальные, научно-технические, продовольственные, экологические.

Считаем необходимым упомянуть о Постановлении Правительства РФ «О мерах по реализации Государственной стратегии информационной безопасности». Данный нормативно-правовой акт будет играть регулирующую роль в обеспечении информационной безопасности на территории Российской Федерации. Он будет служить основой для разработки и внедрения мероприятий, направленных на защиту информационных ресурсов, борьбу с киберпреступностью и повышение уровня киберзащиты, определять стратегические направления деятельности в области информационной безопасности, устанавливать требования к информационным системам и процессам их функционирования, а также регулировать вопросы организации мер по предотвращению и противодействию киберугрозам.

Кроме того, следует отметить важность Закона РФ «О персональных данных». Данный законопроект будет регулировать сбор, хранение, обработку и передачу персональных данных граждан России. Он обеспечит защиту конфиденциальности и прав граждан на их личную информацию, а также установит требования и нормы для организаций и государственных учреждений, работающих с персональными данными.

Также стоит учитывать значимость Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации». устанавливает основы правового регулирования в области информации, информационных технологий и защиты информации. Закон определяет понятия информации, информационных систем, информационных ресурсов и информационных технологий. Он устанавливает требования к сбору, хранению, использованию, обработке, передаче и защите информации, включая персональные данные.

Необходимо провести аудит информационной безопасности с целью оценки текущего уровня защищенности систем и выявления уязвимостей. После анализа слабых мест и недостатков, необходимо разработать и внедрить политики и процедуры информационной безопасности. Это позволит установить правила и требования для защиты информационных ресурсов. Кроме того, необходимо развернуть физические и логические меры защиты. Физические меры включают контроль доступа к серверным комнатам и использование видеонаблюдения.

Логические меры, такие как брандмауэры и системы обнаружения вторжений, обеспечивают контроль доступа и обнаружение аномальной активности. Для эффективного реагирования на инциденты следует разработать план реагирования на кибератаки, определить роли и обязанности персонала. Регулярное обновление программного и аппаратного обеспечения, а также проведение тестирования систем защиты являются неотъемлемой частью данного процесса.

Модернизация системы информационной безопасности Краснодарского края также требует развития кадрового потенциала. Необходимо предоставить специалистам возможности повышения квалификации и обучения в области информационной безопасности. Кроме того, активное сотрудничество с вузами и исследовательскими центрами поможет привлечь и подготовить новых кадров в данной сфере.

Одной из ключевых задач модернизации системы обеспечения информационной безопасности Краснодарского края является совершенствование механизмов взаимодействия между органами государственной власти, муниципалитетами, частным сектором и населением. Необходимо создать механизмы для оперативного информационного обмена и координации действий в случае возникновения киберугроз.

Для успешной модернизации информационной безопасности региона необходимо также привлечь инвестиции. Это позволит выделить средства на внедрение новых технологий, закупку современного оборудования и развитие необходимой инфраструктуры. Важно провести анализ финансовых ресурсов и разработать планы по оптимизации расходов и повышению эффективности использования средств.

В целом, модернизация системы обеспечения информационной безопасности Краснодарского края требует комплексного подхода и внедрения мер, направленных на улучшение инфраструктуры, повышение квалификации персонала, разработку стратегии и политик, а также установление эффективных механизмов взаимодействия и привлечение инвестиций. Это позволит обеспечить надежную защиту информации и повысить уровень информационной безопасности в регионе.

Ожидается, что такие мероприятия позволят улучшить общую безопасность информационных ресурсов и сетей, снизить риск несанкционированного доступа и инфицирования вирусами, а также повысить доверие бизнес-сектора и граждан в безопасность информационных систем и сетей в Краснодарском крае.

Такая логика оправдана, однако в настоящее время не реализуется на практике. Соответственно для наделения государственных и региональных структур такими полномочиям следует усовершенствовать законодательную основу их функционирования.

Так, например, Положение о деятельности министерств следует дополнить пунктами о создании специальных подразделений, сотрудники которых будут уполномочены выполнять указанные функции. Закономерно также будет увеличить расходы бюджетных средств.

Вторым документов, который требует совершенствования в рамках проведения мониторинга, становится прогноз социально-экономического развития региона и приложение к нему. Именно его должны формировать указанные выше сотрудники министерств. Такое решение позволит учитывать широкий перечень угроз для информационной безопасности.

Проведение мониторинга систем информационной безопасности на региональном уровне включает следующие этапы:

1. определение целей и задач мониторинга: на этом этапе определяются основные цели мониторинга, такие как обнаружение угроз и атак, оценка эффективности мер безопасности, выявление уязвимостей и анализ активности в сети;
2. выбор инструментов и систем мониторинга: выбираются специализированные инструменты и системы, которые позволяют осуществлять мониторинг информационной безопасности. Это может включать системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS), системы журналирования событий и анализаторы сетевого трафика;
3. настройка систем мониторинга: после выбора инструментов необходимо осуществить их настройку в соответствии с конкретными потребностями и требованиями региональной системы информационной безопасности. На этом этапе определяются критерии и параметры, которые будут использоваться для обнаружения аномалий и потенциальных угроз;
4. сбор и анализ данных: системы мониторинга будут непрерывно собирать данные о сетевой активности, журналах событий и других источниках информации. Затем проводится анализ этих данных с использованием специализированных алгоритмов и методов, чтобы выявить потенциальные угрозы и аномалии в системе.

При сборе материалов для анализа и мониторинга информационной безопасности Краснодарского края, важным источником данных являются информационные ресурсы и статистические отчеты, предоставляемые службами государственной статистики. Эти данные обрабатываются с учетом специфики мониторинга информационной безопасности, чтобы получить полезную информацию о текущем состоянии и уровне защищенности систем.

Для обеспечения удобства доступа, обработки и использования собранных данных, необходимо создать специальную базу данных. Центр обработки данных станет такой базой, которая соберет и систематизирует информацию о системе обеспечения информационной безопасности Краснодарского края.

Центр обработки данных будет играть ключевую роль в хранении, анализе и обработке полученных данных. Он обеспечит эффективное управление информацией, предоставляя возможность создания отчетов, проведения аналитики, а также мониторинга и оценки текущего уровня защищенности систем. Это поможет принимать обоснованные решения и разрабатывать стратегии в области информационной безопасности.

Центр обработки данных также будет заниматься обеспечением безопасности хранимой информации, применяя соответствующие технические и организационные меры. Кроме того, он будет содействовать эффективному взаимодействию и обмену данными с другими организациями, ответственными за информационную безопасность в регионе.

Структурное подразделение создается на базе министерств и является государственной структурой. Он выполняет посреднические функции, аккумулируя и передавая информацию между следующими субъектами: Советом безопасности РФ, Федеральной службы статистики, министерствами.

Также могут привлекаться и другие заинтересованные стороны для обеспечения безопасности, отображенные на рисунке 6.

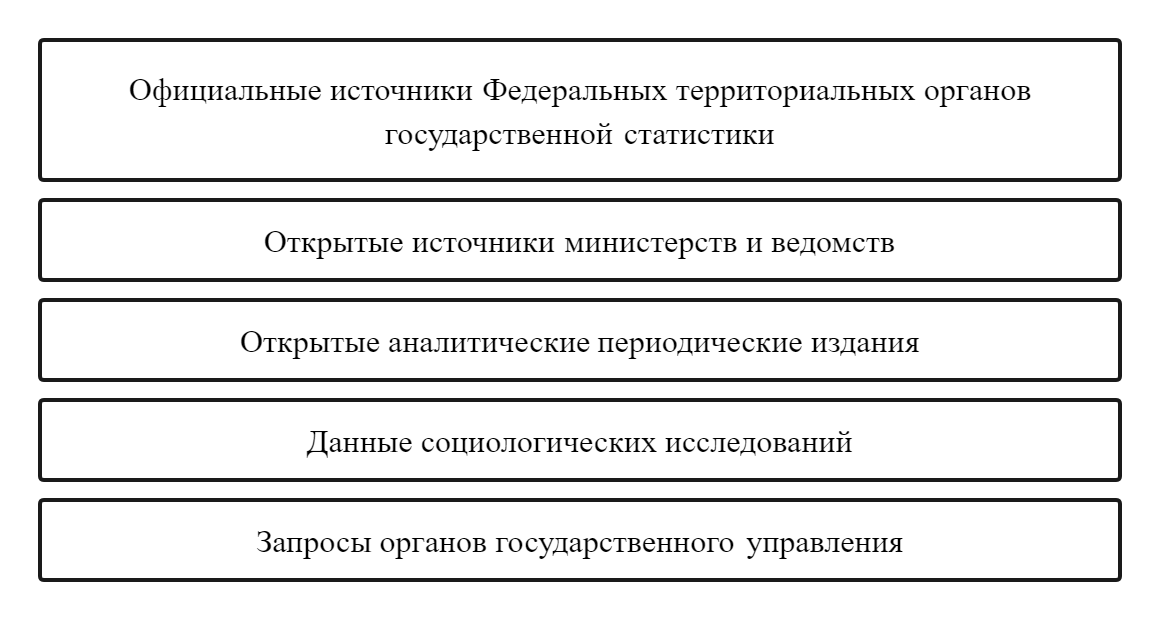


Рисунок 6 – Источники информации для оценки информационной безопасности Краснодарского края (составлено автором по материалам [13])

1. обнаружение и реагирование на угрозы: на основе результатов анализа данных системы мониторинга определяются потенциальные угрозы и аномалии. Важно оперативно реагировать на эти угрозы, принимать меры для их устранения и предотвращения дальнейшего вреда. Это может включать автоматическое обнаружение подозрительной активности, использование систем обнаружения вторжений и механизмов анализа журналов событий;
2. оценка эффективности и отчетность: после проведения мониторинга необходимо оценить эффективность принятых мер и результаты работы системы мониторинга. Регулярная отчетность об уровне безопасности, выявленных уязвимостях и предпринятых действиях позволяет оценить состояние информационной безопасности и определить дополнительные шаги для ее улучшения. Это включает подготовку и представление отчетов о текущем состоянии безопасности, анализ трендов и рекомендации по улучшению защиты информационных ресурсов.

Внедрение указанной системы формирования информационной безопасности позволит обеспечивать своевременное информационное сопровождение и получение данных о вероятных внешних и внутренних угрозах. Это поможет создать осведомленную среду, способствующую принятию эффективных решений и реагированию на угрозы информационной безопасности.

Мы считаем, что для формирования стратегии информационной безопасности Краснодарского края следует придерживаться следующей системы способов в зависимости от частоты поступления информации (см. рисунок 7).

Изображение выглядит как текст, снимок экрана, Шрифт, Параллельный

Автоматически созданное описание

Рисунок 7 – Предлагаемые способы анализа состояния информационной безопасности Краснодарского края [13]

Внедрение указанной системы позволит обеспечивать своевременное информационное сопровождение и получение данных о вероятных угрозах.

При разработке плана развития информационной безопасности региона следует учитывать понимание населением важности соблюдать определенные правила пользования компьютерами и прочими информационными сетями.

Для повышения осведомленности и эффективности в этой области, рекомендуется принять следующие практические меры:

* проведение образовательных программ, лекций, семинаров   
  и тренингов по информационной безопасности для населения и сотрудников государственных и муниципальных служб, включение в эти программы разделов про безопасность в сети Интернет и т.д.;
* создание и внедрение современных материалов и ПО отечественного производства;
* распространение бюллетеней, новостных рассылок или подписок на тему безопасности;
* популяризация использования надежный паролей и их регулярная смена (раз в полгода-год);
* обеспечение каналов обратной связи с населением для сообщения о подозрительной активности или инцидентах, а также предоставление консультаций.

Следовательно, первостепенной задачей государства становится формирование комфортной среды для жизнедеятельности граждан, в том числе путем повышения их образованности в сфере информационной безопасности;

Для этих целей нужно, в первую очередь, уделить внимание дополнительному финансированию образовательной сферы и указать населению на необходимость проведения этих мероприятий.

Проект «Открытое правительство» представляет собой систему механизмов и принципов, направленных на эффективное взаимодействие власти и общества в современной России. Он имеет целью минимизировать издержки работы государственных служб по предоставлению услуг населению и упростить процесс их получения. Основные принципы проекта включают обеспечение качества и сбалансированности принимаемых решений, высокий уровень прозрачности и свободный обмен информацией между государством и обществом, а также активное участие общества в подготовке и реализации решений органов власти.

«Открытое правительство» предоставляет возможность гражданам получать необходимую информацию и услуги от государственных органов более удобным и прозрачным способом. Он способствует развитию электронного правительства, где множество услуг и процедур доступны онлайн, сокращая бумажную работу и ускоряя процессы взаимодействия между государством и гражданами.

В рамках проекта «Открытое правительство» реализуются различные инициативы, такие как создание электронных площадок для обмена информацией и обратной связи с гражданами, публикация открытых данных и отчетов о деятельности государственных органов, проведение общественных слушаний и консультаций при разработке законов и регулирующих документов.

В результате внедрения проекта «Открытое правительство» ожидается улучшение качества предоставляемых государственных услуг, повышение прозрачности деятельности государственных органов, укрепление доверия граждан к власти и увеличение их участия в процессах принятия решений. Это способствует развитию открытого и ответственного государства, которое нацелено на удовлетворение потребностей и интересов граждан. Отдельным моментом в обеспечении информационной безопасности является замена зарубежного оборудования на отечественное.

Для того, чтобы выполнить этот этап, нужно предпринять определенные меры:

* + 1. проанализировать требования и оценить существующую ситуацию, чтобы выявить существующие уязвимости и проблемы, связанные с использованием зарубежного программного обеспечения;
    2. на основе требований выбрать подходящее отечественное программное обеспечение, которое соответствует функциональным   
       и безопасным требованиям учреждения;
    3. разработать и определить последовательности действий, необходимых для успешного внедрения новой системы. Это можно осуществить в порядке конкурса (таблица 8).

Таблица 8 – Этапы проведения конкурса с конкретными действиями (составлено автором по материалам [13])

|  |  |  |
| --- | --- | --- |
| № | Этап | Действия |
| 1 | Постановка задачи и определение требований | Четкое определение задач, которые должны решать отечественное ПО. Это могут быть требования к защите данных, предотвращение кибератак, обнаружение аномалий и соответствующее ей реагирование. Задачи должны быть четко задокументированы и изложены. |
| 2 | Поиск и предварительный отбор ПО | Поиск отечественного ПО, которое может решить поставленные задачи. Важно провести анализ рынка и исследование существующих решений, чтобы выделить наиболее подходящие варианты. |
| 3 | Подготовка документации | На этом этапе готовится необходимая документация, которая описывает требования к ПО, а также процедуры конкурса. |
| 4 | Проведение конкурса | Проводится сам конкурс с участием поставщиком отечественного ПО. Конкурс должен быть проведен в соответствии с законодательством и правилами, установленными для государственных и муниципальных закупок. Поставщики предоставляют свои предложения, соответствующие поставленным требованиям и документации. |

Продолжение таблицы 8

|  |  |  |
| --- | --- | --- |
| № | Этап | Действия |
| 5 | Оценка и выбор победителя | Предложения, полученные от поставщиков, оцениваются на соответствие требованиям и критериям. Оценка может проводиться экспертной комиссией, которая анализирует и сравнивает предложения по различным аспектам, включая функциональность, безопасность, цену, техническую поддержку и т.д.  На основе результатов выбирается победитель конкурса. |
| 6 | Заключение договора и внедрение ПО | После выбора победителя конкурса заключается договор на поставку и внедрение отечественного ПО. Важно учесть условия договора, включая гарантийные обязательства, условия поддержки и обновлений, согласование графика внедрения и т.д. После заключения договора производится внедрение ПО в систему информационной безопасности. |

* + 1. подготовить к внедрению и провести необходимые тесты. Этот этап включает в себя обучение персонала новому оборудованию, информированию их о преимуществах и функциональных возможностях, а также установку и подготовку инфраструктуры, необходимой для работы системы;
    2. заняться мониторингом и обновлением. После успешного внедрения необходимо осуществлять постоянный мониторинг системы   
       и обновление ПО. Регулярные проверки помогут выявить и устранить возможные уязвимости и обеспечить надежность на долгосрочной основе.

Для получения комплексного высокого уровня экономической безопасности следует учитывать все направления работы, указанные нами выше. Только их одновременное укрепление позволит добиться желаемого эффекта.

# ЗАКЛЮЧЕНИЕ

Результаты проведенного исследования подтверждают, что информационная безопасность является важной составляющей экономической безопасности в современном мире. С развитием информационных технологий и автоматизации процессов все больше организаций и предприятий зависят от информационных систем и сетей. Поэтому необходимо уделить особое внимание обеспечению информационной составляющей экономической безопасности и двигаться в направлении ее улучшения.

Анализ проблем и основных аспектов информационно-функциональной составляющей экономической безопасности Краснодарского края, а также изучение отечественного и зарубежного опыта использования современных средств защиты, позволяют выявить проблемные области и применить успешные практики для улучшения системы безопасности региона.

Важно основываться на следующих принципах функционирования системы безопасности Краснодарского края: комплексность, надежность, своевременность, непрерывность, разумная достаточность, централизация управления и компетентность. Для достижения высокого уровня безопасности необходимо соблюдать определенные стандарты, улучшать системы образования в области информационной безопасности и разрабатывать современные отечественные технологии.

Также важно быть внимательными к обстановке в мире, соответствовать мировым стандартам в области безопасности, предотвращать угрозы и использовать возможности для увеличения преимуществ и минимизации недостатков.

Применение этих принципов и подходов позволит повысить уровень информационной безопасности в Краснодарском крае, обеспечить надежную защиту информации и снизить риски, связанные с внешними и внутренними угрозами.

Оценка основных показателей информационной безопасности Краснодарского края позволила определить наличие некоторых уязвимостей и проблем в данной области: недостаточная осведомленность населения в вопросах информационной безопасности, отсутствие современного оборудования и ПО, а также недостаточное применение правовых механизмов. Всё это требует немедленного внимания и принятия соответствующих мер.

На основе проведенного исследования были разработаны рекомендации и мероприятия по обеспечению информационно-функциональной составляющей экономической безопасности Краснодарского края. Эти меры включают в себя усиление финансирования разработки современного оборудования, поддержку научно-технического потенциала региона, повышение осведомленности населения о вопросах информационной безопасности, участие региональных властей в создании образовательных программ, обучение сотрудников муниципальных органов основам информационной безопасности, а также внедрение современного программного обеспечения и разработка политик и процедур обработки информации.

Реализация предложенных мероприятий позволит снизить риски, связанные с обеспечением высокого уровня безопасности Краснодарского края, а также способствовать его экономическому развитию. Они обеспечат улучшение конкурентоспособности региона и повысят степень защиты информации.

Следование за постоянно меняющимися угрозами и технологиями также является неотъемлемой частью обеспечения информационной безопасности. Мы должны постоянно отслеживать и изучать новые виды угроз, анализировать их характеристики и разрабатывать соответствующие меры защиты. Это позволит нам эффективно бороться с угрозами и обеспечивать надежную защиту информационных ресурсов.

Обеспечение устойчивого развития региона и защита его информационных ресурсов требуют постоянного внимания и усилий. Мы должны стремиться к постоянному совершенствованию и инновациям в области информационной безопасности, чтобы быть готовыми к новым вызовам и обеспечить безопасную и стабильную среду для развития края.

В заключение, исследование и развитие информационной безопасности являются критически важными задачами для развития края. Увеличение усилий в этой области поможет нам достичь устойчивого развития и обеспечить надежную защиту информационных ресурсов. Мы должны продолжать исследования, обновлять системы и следить за новыми угрозами и технологиями, чтобы быть на шаг впереди и обеспечить безопасное будущее для нашего региона.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. CNews Security. Интернет-издание о высоких технологиях. Крупнейшие компании России в сфере защиты информации 2022 [Электронный ресурс]. URL:https://www.cnews.ru/reviews/security2022/review  
   \_table/12b4f5538e57db6abd0a5e202c744bc94f1ec876 (дата обращения: 12.05.2023).
2. Авдийский В.И. Теневая экономика и экономическая безопасность государства / В. И. Авдийский. – Москва: НИЦ ИНФРА-М, 2022. – 538 с.
3. Анализ рисков информационной безопасности. [Электронный ресурс]. URL:https://www.buhgalteria.ru/article/analiz-riskov-informatsionnoy-bezopasnosti (дата обращения: 30.05.2023).
4. Анализ существующих на территории Краснодарского края информационных, аналитических и управляющих систем, коммуникационной инфраструктуры, обеспечивающих безопасность территорий, населения и среды обитания. [Электронный ресурс]. – URL: https://23.mchs.gov.ru/deyatelnost/poleznaya-informaciya/bezopasnyy-gorod/i-organizacionnye-i-planiruyushchie-dokumenty/4-analiz-sushchestvuyushchih-na-territorii-krasnodarskogo-kraya-informacionnyh-analiticheskih-i-upravlyayushchih-sistem-kommunikacionnoy-infrastruktury-obespechivayushchih-bezopasnost-territoriy-naseleniya-i-sredy-obitaniya (дата обращения: 30.05.2023).
5. Баранова Е.К. Информационная безопасность и защита. Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: РИОР, Инфра-М, 2023. - 324 c.
6. Гаджиев Н.Г. Экономическая безопасность России на современном этапе социально-экономического развития общества / Н.Г. Гаджиев, О.В. Киселева, О.В. Скрипкина [и др.]. – Москва: НИЦ-ИНФРА-М, 2022. – 233 с.
7. Галатенко В.А. Основы информационной безопасности: учебное пособие / Галатенко В.А. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 c.
8. Генеральная прокуратура Российской Федерации. Документ. Правовое регулирование правоотношений в сети Интернет. [Электронный ресурс]. URL: https://epp.genproc.gov.ru/ru/web/gprf/documents/scientific-materials?item=4894605 (дата обращения: 12.05.2023).
9. Департамент информатизации и связи Краснодарского края [Электронный ресурс]. – URL: https://dis.krasnodar.ru/ (дата обращения: 25.05.2023).
10. Егшатян М.И. Информационная безопасность в современном мире // Евразийский Научный Журнал №12 2021 (декабрь 2021) // 2021 г., [Электронный ресурс] URL: https://journalpro.ru/articles/informatsionnaya-bezopasnost-v-sovremennom-mire/ (дата обращения: 12.05.2023).
11. Итоги реализации национальной программы «Цифровая экономика» за 2022 год. [Электронный ресурс]. – URL: https://kuban24.tv/item/v-krasnodarskom-krae-podveli-itogi-realizatsii-natsionalnoj-programmy-tsifrovaya-ekonomika-za-2022-god (дата обращения: 30.05.2023).
12. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 01.07.2020 N 11-ФКЗ) // [Электронный ресурс]. URL: https://www.consultant.ru/document/cons\_doc\_LAW\_28399/ (дата обращения: 12.05.2023).
13. Криворотов В.В. Экономическая безопасность государства и регионов: учебное пособие для студентов вузов, обучающихся по направлению «Экономика» / В. В. Криворотов, А. В. Калина, Н.Д. Эриашвили. – Москва: ЮНИТИ-ДАНА, 2017. – 351 с.
14. Мельников В.П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2019. – 336 c.
15. Мирошниченко М.А. Траектория реализации национальной программы «Цифровая экономика» в проектах Краснодарского края / К. К. Сивинцева, В. Л. Тагирова // Естественно-гуманитарные исследования № 37 (5) – 2021 г., с. 197-207.
16. Орлова А.В. Экономическая безопасность: региональный аспект: монография / А.В. Орлова, Е.В. Никулина. – Германия: LAP LAMBERT Academic Publishing, 2013. – 120 с.
17. Остапенко Г.А. Информационные операции и атаки в социотехнических системах. Организационно-правовые аспекты противодействия: моногр. / Г.А. Остапенко, Е.А. Мешкова. - Москва: Гостехиздат, 2023. - 208 c.
18. Официальный портал исполнительных органов государственной власти Краснодарского края. [Электронный ресурс]. – URL: https://krasnodar.ru/ (дата обращения: 12.05.2023).
19. Паспорт регионального проекта. Информационная безопасность (Краснодарский край). [Электронный ресурс]. – URL: https://admnvrsk.ru/gorozhanam/natprojects/proekty/RP\_Informacionnaya\_bezopasnost-\_1\_.pdf (дата обращения: 25.05.2023).
20. Российская Федерация. Законы. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 28.04.2023). [Электронный ресурс]. URL: https://www.consultant.ru/document/cons\_doc\_LAW\_10699/ (дата обращения: 25.05.2023)
21. Стратегия социально-экономического развития Краснодарского края до 2030 года. [Электронный ресурс]. – URL: https://www.economy.gov.ru/material/file/e4e8b9ddede078a93f60f5e7a08fce28/krasnodar.pdf (дата обращения: 25.05.2023).
22. Угрозы информационной безопасности. Защита данных с помощью DLP-систем. [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/ (дата обращения: 12.05.2023).
23. Утечки информации ограниченного доступа в мире 2022 г. [Электронный ресурс]. URL:https://www.infowatch.ru/analytics/analitika/utec  
    hki-informatsii-ogranichennogo-dostupa-v-mire-2022-g (дата обращения: 25.05.2023).
24. Федеральные законы Российской Федерации. [Электронный ресурс]. – URL: https://www.consultant.ru/document/ (дата обращения: 12.05.2023).
25. Федеральный проект «Умное правительство». Официальный сайт. [Электронный ресурс]. – URL: https://open.krasnodar.ru/ (дата обращения: 01.06.2023).
26. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – Москва: Форум, 2023. – 416 с.