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**

**КУРСОВАЯ РАБОТА**

**Информационная безопасность государства: современное состояние и перспективы укрепления**

|  |  |  |
| --- | --- | --- |
| Работу выполнил | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись) |  В.В. Павлов |
| Специальность | 38.05.01 Экономическая безопасность |  курс | 3 |
| Специализация | Экономико-правовое обеспечение экономической безопасности |
| Научный руководитель канд. экон. наук, доц. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись, дата) |  С.В. Шевченко |
| Нормоконтролер канд. экон. наук, доц. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись, дата) |  С.В. Шевченко |

Краснодар

2022

Содержание

[Введение 4](#_Toc104247149)

[1 Теоретические аспекты изучения информационной безопасности 6](#_Toc104247150)

[1.1 Понятие и роль защиты информации как элемента национальной безопасности 6](#_Toc104247151)

[1.2 Государственные структуры, обеспечивающие информационную безопасность в РФ 10](#_Toc104247152)

[1.3 Методы и инструменты защиты информационной безопасности 13](#_Toc104247153)

[2 Анализ эффективности системы информационной безопасности в Российской Федерации 16](#_Toc104247154)

[2.1 Анализ современного состояния информационной безопасности 21](#_Toc104247155)

[2.2 Анализ деятельности государственных органов по обеспечению информационной безопасности в РФ 20](#_Toc104247156)

[2.3 Новая платежная система - ответ на западные санкции и защита финансового фонда России 24](#_Toc104247157)

[3 Предложения и пути по совершенствованию системы информационной безопасности РФ 26](#_Toc104247158)

[Заключение 29](#_Toc104247161)

[Список использованных источников 31](#_Toc104247162)

#

**ВВЕДЕНИЕ**

Актуальность темы исследования заключатся в том, что как системообразующий фактор современного и динамично развивающегося общества, информационная сфера оказывает существенное влияние на политическое, экономическое, культурное, идеологическое состояние и элементы безопасности жизни государства, его народов и отдельных лиц, что подчеркивает важность информационной безопасности в системе национальной безопасности. Информационная безопасность – это состояние национального сообщества, в котором гарантируется всесторонняя и безопасная защита личности, общества и государства от всевозможных информационных рисков и угроз, радикально ориентированных политических и социальных сил[1].

Следовательно, информационная безопасность — это сложный процесс постепенного преодоления любого информационного риска. Вызовы и угрозы информационной безопасности определяют конкретное содержание практических шагов и мер, обеспечивающих национальную безопасность.

Вопрос обеспечения безопасности жизненно важно для реализации национальных интересов и развития национальной политики, направленной на сохранение и воспроизводство социальной системы.

Целью исследования является комплексное изучение и определение особенностей обеспечения информационной безопасности в системе национальной безопасности страны. Цепь исследования предполагает решение следующих задач:

1. Рассмотреть основные категории информационной безопасности.
2. Охарактеризовать сущность информационной безопасности как важнейшего компонента национальной безопасности.
3. Исследовать понятие и содержание информационной безопасности России.
4. Проанализировать особенности оценки состояния и организации защиты от информационных угроз в РФ.

Объектом исследования выступает информационная безопасность государства.

Предмет исследования - состояние и методы обеспечения информационной безопасности России в современных условиях.

Теоретическую базу исследования составляют теоретические положения, вытекающие из общей теории безопасности, концепции и доктрины национальной безопасности России, Конституции Российской Федерации, а также из положений, содержащихся в федеральных законах, указах Президента РФ, постановлениях Правительства Российской Федерации и других правовых актах Российского государства, в трудах отечественных и зарубежных ученых, а также фундаментальные и монографические труды отечественных и зарубежных исследователей[2].

Структура работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трех глав, заключения и библиографического списка.

Во введении обоснована актуальность выбора темы, определены предмет, объект, цель и соответствующие ей задачи, охарактеризованы методы исследования и источники информации.

В первой главе рассматриваются теоретические аспекты изучения информационной безопасности.

Во второй главе анализируются сущность и состояние информационной безопасности в Российской Федерации. В третьей главе предлагаются пути решения по совершенствованию системы информационной безопасности РФ. В заключении, на основе рассмотренных вопросов, даны соответствующие выводы.

**1. Теоретические аспекты изучения информационной безопасности**

С древних времен до наших дней вопрос обеспечения безопасности социокультурной жизни рассматривался как высшая цель практического и теоретического значения. Хотя концепция безопасности исторически трансформировалась, развивалась, но первоначальное понимание этого явления остается неизменным: самосохранение и отсутствие риска. Результатом процедуры информатизации является новый элемент национальной безопасности - информационная безопасность.

В последние годы безопасное развитие информационной сферы заработало значительнее в сложных и противоречивых процессах глобализации. В настоящее время многие важнейшие интересы человека, общества и государства в значительной степени определяются количественными и качественными характеристиками окружающей их информационной сферы[3].

**1.1. Понятие и роль защиты информации как элемента национальной безопасности**

Можно с полным основанием сказать, что информационная безопасность является важнейшим элементом национальной безопасности, проникшим во все остальные виды безопасности. Приоритет того или иного вида обеспечения определяется:

* Необходимость функционирования и развития граждан;
* Широкий спектр опасностей и угроз для общества, государства и международного сообщества, которым можно противостоять со специфической системой обеспеченности и сопротивления.

Очевидно, все эти факторы применимы к информационной безопасности. Информационная безопасность — это состояние защищенности национальных интересов Российской Федерации в информационной сфере, которая определяется балансом интересов общества и государства. Информационная сфера включает в себя защиту конституционных прав и свобод человека и гражданина при получении и использовании информации, обеспечение духовного и политического развития России, сохранение и укрепление нравственных ценностей страны, ее патриотических и гуманитарных традиций, культурного и научного потенциала[4].

Во-первых, наличие фундаментальных жизненных ценностей российского общества, рисков посягательства на его интересы воспринимается как национальная безопасность, а кроме того, как цель информационной политики государства. Во-вторых, это информационное обеспечение государственной политики. Оно предоставляет достоверную информацию российской и международной общественности, официальную позицию государства о важнейших политических и общественных событиях в государстве и в международной жизни, обеспечивая доступность граждан для открытых средств массовой информации.

Третья составляющая национальных интересов в информационной сфере является развитие современных технологий, в том числе информационных средств, телекоммуникаций и связи. Оно включает также обеспечение потребностей национального рынка информационных продуктов и выход этого продукта на международный рынок, а также сохранение и эффективное использование национальных информационных ресурсов.

Четвертый компонент - защита информационных ресурсов от несанкционированного доступа и обеспечение безопасности информационных, коммуникационных и телекоммуникационных систем. С этой точки зрения вопросы обеспечения информационной безопасности в России включают:

* активное противодействие адвокатской и психологической деятельности противника, постоянное совершенствование ее форм и средств;
* подготовку специалистов по информационной безопасности в области обороны.

Для уточнения концептуального понимания информационной безопасности необходимо приступить к анализу субъектов информационных отношений, их интересов и потребностей. Иными словами, понятие «информационная безопасность» тесно связано с социально-философскими категориями «национальные интересы» и «цели» [5]. Ландшафт национальных интересов использования информационно-коммуникационных технологий представляет собой совокупность информации, доступности, целостности и конфиденциальности вспомогательной инфраструктуры.

С точки зрения обеспечения информационной безопасности целью является активная защита интересов и требований субъектов информационных отношений. Хотя интересы различны, все они сосредоточены на обеспечении доступности, полноте и конфиденциальности информации. Национальные интересы рассматриваются в 3-х аспектах в рамках информационной сферы. Эти аспекты отражают различные уровни проявления интересов:

1. Уровень индивидуальных интересов в информационной сфере, где анализируются конституционные права человека и гражданина. Эти права обеспечивают доступность информации, использование информации в интересах физического, духовного и интеллектуального развития личности, а также эффективную защиту информации, которая обеспечивает личную безопасность. Личная информационная безопасность человека определяется уровнем защиты его психологического состояния и сознания от возможных опасных воздействий[6].

2. Уровень социальных интересов. Здесь речь идет об укреплении демократии, правовом и социальном государственном устройстве, диалоге и установлении общественного согласия.

3. Уровень состояния. Национальные интересы государства требуют создания благоприятных условий для гармоничного развития информационной инфраструктуры России, обеспечения государственной и общественной безопасности, полной реализации конституционных прав и свобод человека и гражданина. Суверенитет законодательных процедур и нерушимость территориальной целостности РФ находятся в неразрывной диалектической связи. Чем быстрее и успешнее осуществляются права и свободы человека и гражданина, тем эффективнее процесс укрепления информационной безопасности.

Этот прогресс во многом зависит от уровня развития информационных потребностей человека, общества и государства – чем выше уровень информационных потребностей, тем сильнее ориентация на духовное и интеллектуальное развитие человека. Кроме того, жизнедеятельность человека строится в соответствии с целевыми требованиями концепции информационной безопасности. Исходя из учета национальных интересов в сфере информации, стратегических и текущих вопросов внешней и внутренней политики, направленных на сформулированное обеспечение информационной безопасности [7]. Информационная безопасность общества и государства характеризуется практическим потенциалом противодействия, приостановки и нейтрализации информационных воздействий, которые деконструируют, дестабилизируют, ставят под угрозу и нарушают интересы страны. А также характеризуется высоким уровнем защиты информации и, следовательно, относительной стабильностью всех сфер жизнедеятельности общества (экономики, науки, техносферы, управления, военного дела, общественного сознания и др.).

Трансформация и развитие социальных систем стабилизируется тем, что они практически способны воспринимать и поглощать трансформирующиеся внешние и внутренние стимулы, органично включаясь в демократический процесс, предотвращение конфликтов и их использование. С этой точки зрения могут возникать опасные информационные эффекты и, следовательно, объекты информационной безопасности - умы людей, ментальный мир, информационно-технические системы различного масштаба и значения и объекты социальной защиты информации - личность, общество, государство, международное сообщество.

**1.2 Государственные структуры, обеспечивающие информационную безопасность в РФ**

Объектами информационной безопасности можно считать структуры, которые заняты обеспечением безопасности. Они могут быть как исполнительными, так и законодательными органами. Роль государственных органов в обеспечении безопасности незаменима. В целях обеспечения информационной безопасности в стране государственные органы должны оценивать состояние информационной сферы, разрабатывать и принимать новые нормы и программы информационной безопасности, периодически информировать общественность о состоянии информационной безопасности и о работе государственных органов в этой сфере, защищать интересы и права граждан, общества и государства[8]. Общество должно принять участие в общем процессе развития, определяя нормы международного права в этой области, новые критерии и принципы.

Государственные органы должны раскрывать внутренние и внешние угрозы информационной сферы, определять направление этих угроз. При учете интересов субъектов информационных отношений обеспечение безопасности подразумевает создание благоприятных условий, позволяющих реализовать интересы субъектов информационных отношений.

Кроме того, здесь подчеркиваются жизненные интересы и ценности участников. В контексте информационных отношений ценности проявляются средствами обеспечения потребностей, интересов и целей безопасности. Выработку политики информационной безопасности, подготовку законодательных актов и нормативных документов, контроль над выполнением установленных норм обеспечения безопасности информации осуществляют государственные органы, структура которых приведена на рис. 2.

 

Рис. 2. Структура государственных органов, обеспечивающих проведение политики информационной безопасности в РФ

Возглавляет государственные органы обеспечения информационной безопасности Президент РФ. Он руководит Советом Безопасности и утверждает указы, касающиеся обеспечения безопасности информации в государстве.

Общее руководство системой информационной безопасности, наряду с другими вопросами государственной безопасности страны, осуществляют Президент и Правительство Российской Федерации[9].

Органом исполнительной власти, непосредственно занимающимся вопросами государственной безопасности, является Совет Безопасности при Президенте РФ. В состав Совета Безопасности входит Межведомственная комиссия по информационной безопасности. Комиссия готовит указы Президента, выступает с законодательной инициативой, координирует деятельность руководителей министерств и ведомств в области информационной безопасности государства.

Рабочим органом Межведомственной комиссии по информационной безопасности является Государственная техническая комиссия при Президенте РФ. Эта комиссия осуществляет подготовку проектов законов, разрабатывает нормативные документы, (решения Государственной технической комиссии), организует сертификацию средств защиты информации (за исключением криптографических средств), лицензирование деятельности в области производства средств защиты и обучения специалистов по защите информации. Гостехкомиссия руководит аттестацией КС, предназначенных для обработки информации, представляющей государственную тайну, или управляющих экологически опасными объектами[10]. Она координирует и направляет деятельность государственных научно-исследовательских учреждений, работающих в области защиты информации, обеспечивает аккредитацию органов лицензирования и испытательных центров (лабораторий) по сертификации. Эта комиссия обеспечивает также работу Межведомственной комиссии по защите государственной тайны.

На Межведомственную комиссию по защите государственной тайны возложена задача руководства лицензированием предприятий, учреждений и организаций, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации, а также оказанием услуг по защите гостайны. Кроме того, эта комиссия осуществляет координацию работы по организации сертификации средств защиты информации[11].

Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) обеспечивает правительственную связь и информационные технологии государственного управления. Агентство осуществляет сертификацию всех средств, используемых для организации правительственной связи и информатизации государственного управления, а также лицензирует все предприятия, учреждения и организации, занимающиеся производством таких средств. Кроме того, в исключительном ведении ФАПСИ находятся вопросы сертификации и лицензирования в области криптографической защиты информации.

В министерствах и ведомствах создаются иерархические структуры обеспечения безопасности информации, которые, как правило, совпадают с организационной структурой министерства (ведомства). Называться они могут по-разному, но функции выполняют сходные[12].

**1.3 Методы и инструменты государственных органов по защите информационной безопасности**

Законы и нормативные акты исполняются только в том случае, если они подкрепляются организаторской деятельностью соответствующих структур, создаваемых в государстве, в ведомствах, учреждениях и организациях. При рассмотрении вопросов безопасности информации такая деятельность относится к организационным методам защиты информации.

Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации технологических средств для обеспечения заданного уровня безопасности информации.

Организационные методы защиты информации тесно связаны с правовым регулированием в области безопасности информации. В соответствии с законами и нормативными актами в министерствах, ведомствах, на предприятиях (независимо от форм собственности) для защиты информации создаются специальные службы безопасности (на практике они могут называться и иначе). Эти службы подчиняются, как правило, руководству учреждения. Руководители служб организуют создание и функционирование систем защиты информации. На организационном уровне решаются следующие задачи обеспечения безопасности информации:

* организация работ по разработке системы защиты информации;
* ограничение доступа на объект и к ресурсам КС;
* разграничение доступа к ресурсам КС;
* планирование мероприятий;
* разработка документации;
* воспитание и обучение обслуживающего персонала и пользователей;
* сертификация средств защиты информации;
* лицензирование деятельности по защите информации;
* аттестация объектов защиты;
* совершенствование системы защиты информации;
* оценка эффективности функционирования системы защиты информации;
* контроль выполнения установленных правил работы.

Организационные методы являются стержнем комплексной системы защиты информации. Только с помощью этих методов возможно объединение на правовой основе технических, программных и криптографических средств защиты информации в единую комплексную систему. Конкретные организационные методы защиты информации будут приводиться при рассмотрении отражения угроз безопасности информации[14]. Наибольшее внимание организационным мероприятиям уделяется при изложении вопросов построения и организации функционирования комплексной системы защиты информации.

В своей деятельности по развитию и совершенствованию системы информационной безопасности, государственные органы преследуют следующие цели:

* укрепление системы вертикального управления, и централизация сил информационной безопасности на федеральном, межрегиональном, региональном и муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;
* совершенствование форм и методов взаимодействия сил информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем проведения регулярных учений;
* совершенствование информационно-аналитических и научно-технических аспектов функционирования системы информационной безопасности;
* повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при выполнении задач информационной безопасности.

Доктрина по информационной безопасности реализуется в соответствии с отраслевыми документами стратегического планирования Российской Федерации. Для обновления этих документов Совет безопасности Российской Федерации составляет перечень среднесрочных приоритетных направлений информационной безопасности с учетом положений стратегической перспективы Российской Федерации[15].

**2. Анализ эффективности системы информационной безопасности в Российской Федерации**

**2.1 Анализ современного состояния информационной безопасности в РФ**

Российская модель информационной безопасности заключается в создании благоприятной внутренней информационной среды за счет использования медиахолдингов для манипулирования общественным мнением. Эта модель направлена против потенциальных и реальных внутренних и внешних информационно-психологических угроз, но менее эффективна против кибератак.

Основными характеристиками проблем в исследовании информационной безопасности являются: непродуманности и неясность законодательства, непрозрачность отношений между правительством и СМИ, отсутствие баланса между правящей и оппозиционных СМИ, политизация СМИ. Представитель центра исследования конфликтов К. Джайлз отметил, что российские взгляды на природу, потенциал и использование киберпространства существенно отличаются от западного консенсуса.

В частности, у России вызывает глубокую озабоченность принцип неконтролируемого обмена информацией в киберпространстве, и презумпция ограниченности национальных границ. Распространение информации, представляющей угрозу обществу или государству, и суверенитет “национального интернета” являются ключевыми проблемами безопасности в России. Россия продолжит продвигать международные соглашения, регулирующие киберпространство, в русле уже достигнутого консенсуса с государствами-единомышленниками в ОДКБ, ШОС и БРИКС[16].

Новым толчком к разработке национальной стратегии информационной безопасности России стал документ "Основы государственной политики Российской Федерации в сфере Международной информационной безопасности до 2020 года", который был подписан президентом РФ в 2013 году в качестве ответа на Международную стратегию США по Киберпространству, обнародованную Белым домом в 2011 году[23]. Документ разработан Российской Федерацией Совета безопасности в сотрудничестве с профильными министерствами, включая Министерство иностранных дел, Министерство обороны, Министерство связи и массовых коммуникаций и Министерство юстиции.

Следует подчеркнуть, что это первый официальный документ, юридически закрепляющий политику информационной безопасности России. В частности, доктрина включает четыре основные угрозы информационной безопасности для Российской Федерации:

1) Использование ИКТ в качестве информационного оружия в военно-политических целях;

2) Использование ИКТ в террористических акциях;

3) Осуществление киберпреступлений;

4) Использование Интернет-технологий с целью вмешательства во внутренние дела государства, провоцирования беспорядков общественного порядка, пропаганды насилия и разжигания вражды.

В документе предусмотрено активное сотрудничество России с международными партнерами в рамках ШОС, БРИКС и инициирование процесса принятия международных норм поведения в Интернете, которые функционировали бы на основе единой системы сетевого управления, в целях противодействия информационным угрозам[17]. Министерство обороны Российской Федерации, Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Федеральной службы безопасности, Объединенного Комитета по информационной безопасности при Совете Безопасности Российской Федерации и управления МВД РФ фактически вовлечены в изучение проблемы информационной войны.

Отношения Запада с Россией вступили в новую, более холодную фазу. Улучшение отношений потребует от российского руководства изменения восприятия международной действительности и мышления, основанного на политике силы и сферах влияния, а также отказа от стремления очертить новые цивилизационные границы.

Международное сотрудничество как инструмент продвижения российских внешнеполитических интересов после введения международных санкций странами ЕС и США, а также поддержки их действий рядом других развитых стран, Россия может постепенно оказаться в экономическом и политическом вакууме, который приведет к внутреннему кризису. Для смягчения последствий санкций Российская Федерация запускает пропагандистскую кампанию в мировых СМИ с целью дискредитации украинской политической власти. Кроме того, для Российской Федерации важно найти союзников, в частности страны БРИКС. Хотя де-юре Бразилия, Индия, Китай и Южно-Африканская Республика заняли нейтральную позицию в вопросе обострения отношений между Россией и Украиной, де-факто эти страны продолжали расширять экономическое сотрудничество с Российской Федерацией[18].

Таким образом, Россия через потенциал БРИКС получила эффективный инструмент реализации собственных внешнеполитических инициатив и национальных интересов, одним из которых является возвращение постсоветских позиций на международной арене. Для этого, Россия официально выступает за координацию усилий и единства позиции среди стран БРИКС по вопросам глобальной стабильности, международной и региональной безопасности, укрепление координирующей роли ООН в области борьбы с международным терроризмом, борьба с незаконным оборотом наркотиков, сотрудничество в интересах обеспечения международной информационной безопасности и развития сотрудничества для управления кибертерроризмом и киберпреступностью, и так далее.

В настоящее время российские инициативы по международной информационной безопасности стимулируется не только на уровне ООН, ШОС и БРИКС, а также в рамках СНГ, где Российская Федерация выступает за объединение информационного пространства с целью более эффективной реализации общих интересов, особенно в сфере информационной безопасности[19].

Предусматривается осуществление сотрудничества государств-участников СНГ в форме взаимных консультаций, координации и сотрудничества в области научных исследований, разработки и производства соответствующих средств информационной безопасности. В частности, планируется разработать международно-правовой механизм запрещения в рамках СНГ незаконного информационного воздействия на личное и общественное сознание; создание компетентных правоохранительных органов по предупреждению компьютерной преступности; предупреждению и пресечению преступлений в информационной сфере. Подобные инициативы не были реализованы в рамках СНГ, хотя основные элементы Российской концепции информационной безопасности реализуются в рамках двустороннего сотрудничества, так и на уровне национального законодательства.

Значительная роль и место информационного противоборства в системе обеспечения национальной безопасности постепенно растет. Российская Федерация, для достижения своих внешнеполитических целей, в настоящее время наращивает свой информационный потенциал. Более того, в настоящее время отсутствуют международно-правовые нормы, согласно которым информационному противостоянию может быть придан такой же статус, как и преступлению.

В связи с ускоренным развитием электронных СМИ резко возросла роль общественного мнения, что существенно влияет на социально-политические процессы, специфику функционирования информационно-психологической среды, психическое здоровье военнослужащих в период вооруженных конфликтов. Таким образом, система формирования общественного мнения также является одним из основных объектов информационно-психологической безопасности Российской Федерации.

В настоящее время Россия в целях поддержки и поддержания собственных внешнеполитических интересов активно начала использовать информационные инструменты средств массовой информации и социальных сетей. Понимание российскими властями преимуществ таких инструментов привело к формированию законов в области информационной безопасности, регулирующих процессы управления русскоязычным информационным пространством[20]. Стратегия Российской Федерации в использовании современных информационных инструментов для оказания информационного влияния на оппонента не новая, но принята со стороны США и стран ЕС, дополнена Советским опытом, поэтому методы противодействия таким информационным операциям также хорошо известны. Барьером на пути эффективного противодействия информационно-пропагандистским кампаниям являются:

* непоследовательность позиций политической и военной элиты относительно ситуации в государстве,
* практический дефицит информационных материалов в информационном поле страны, призванных сформировать консолидированную национальную идею,
* поддержка искусственного разделения страны на «инсайдеров и аутсайдеров» политической элитой и др.

Таким образом, каждая страна может использовать и использует информационный арсенал для продвижения собственных внешнеполитических интересов; однако страны, против которых направлена такая «информационная агрессия», должны иметь возможность не только защищать, но и проводить собственные информационные операции.

**2.2 Анализ деятельности государственных органов по обеспечению информационной безопасности в РФ**

Очевидно, что устойчивая работа информационных систем, средств коммуникации и связи, их защищённость имеют для страны стратегическое значение. Это важный фактор обеспечения суверенитета, обороноспособности, безопасности государства, эффективного развития экономики, социальной сферы, государственного управления на базе передовых, в том числе цифровых, технологий.

Три года назад на заседании Совета Безопасности 1 октября 2014 года всесторонне была рассмотрена эта тема, где определялись ближайшие и перспективные задачи. За прошедшее время, конечно, многое сделано для обеспечения надёжной работы информационной инфраструктуры, особенно это касается государственных органов.

В декабре 2016 года утверждена Доктрина информационной безопасности России. С 1 января 2018 года вступает в силу Федеральный закон о безопасности критической информационной инфраструктуры России. Таким образом, заложен правовой фундамент для дальнейших практических шагов на этом направлении [22].

Успешно действуют федеральные органы, наделённые полномочиями контроля в этой сфере. Имея в виду Федеральную службу по техническому и экспортному контролю, а также ФСБ, которые обеспечивают государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы; активно работают и специалисты Роскомнадзора.

Между тем нужно учитывать, что уровень угроз в информационном пространстве повышается, число рисков увеличивается, а негативные последствия разного рода кибератак носят уже не локальный, а действительно глобальный характер и масштаб. Например, в результате распространения вируса «Вонна Край» в мае–июне 2017 года пострадали информационные ресурсы в 150 странах мира, в том числе и в России.

Внешнее вторжение в электронные системы в сфере обороны и госуправления, жизнеобеспечивающей инфраструктуры и финансов, утечка электронных документов могут обернуться самыми тяжёлыми последствиями.

Можно отметить, что ряд стран уже фактически поставили информационные технологии на военную службу: формируют свои кибервойска, а также активно используют информационное поле для ослабления конкурентов, продвижения своих экономических и политических интересов, решения геополитических задач в целом, в том числе в качестве фактора так называемой мягкой силы.

В этой связи государство должно чётко представлять тенденции развития глобальной информационной сферы, прогнозировать потенциальные угрозы и риски. И главное – наметить дополнительные меры, которые позволят не просто своевременно выявлять угрозы, а активно реагировать на них.

На чём в первую очередь необходимо сконцентрировать усилия.

* Совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России. Это в том числе касается механизмов взаимодействия её ведомственных сегментов.
* Повышение защищённости информационных систем и сетей связи государственных органов. Нужно усилить персональную ответственность руководителей за обеспечение информационной безопасности.
* Максимально снизить риски, связанные с объективной необходимостью использовать иностранные программы и телекоммуникационное оборудование.
* Нужно последовательно реализовывать проекты импортозамещения, и такая программа работает уже несколько лет.
* Следует повысить безопасность и устойчивость работы инфраструктуры российского сегмента интернета. Если для этого потребуется принять дополнительные нормативные акты. Речь может идти не об ограничении доступа законопослушных граждан к ресурсам глобальной сети, и о каких-то тотальных барьерах и фильтрах. Необходимо строго соблюдать и уважать конституционное право на получение и распространение информации.
* Необходимо бороться с теми, кто использует информационное пространство для пропаганды радикальных идей, оправдания терроризма, экстремизма, решительно пресекать попытки размещения материалов, угрожающих безопасности нашего государства, общества в целом и отдельных граждан.
* Следует активнее содействовать созданию системы международной информационной безопасности, развивать сотрудничество с партнёрами на глобальных и региональных площадках, таких как ООН, БРИКС, ШОС, АТЭС, и других, проводить межведомственные консультации и переговоры.

В 2017 году законодательство усилило ответственность за организацию сайтов, призывающих детей и подростков к суициду. Наши правоохранительные органы и спецслужбы стали гораздо чаще выявлять и пресекать деятельность вербовщиков в террористические группировки, в том числе в ряды запрещённой в России ИГИЛ и в другие подобные организации[21].

Так же жёстко в рамках закона нужно действовать и в отношении других лиц и групп, использующих интернет, информационное пространство в преступных целях.

**2.3 Новая платежная система - ответ на западные санкции и защита финансового фонда России**

Все мы отлично знакомы с банковскими картами системы VISA и MasterCard. Можно сказать, что они стали монополией платежных систем во всем мире. Чтобы защитить пользователей банковских карт в России была создана новая система, которая принимает эстафету у этих компаний. Система «МИР» в 2018 году начинает свое функционирование во всех российских банках.

Международное сообщество пытается контролировать финансовые потоки внутри всех стран. И когда возникает ситуация, при которой кому-то из западных правительств не нравится происходящее внутри той или иной страны, они перекрывают обслуживание банковских карт своих систем.

Это уже происходило в России в 2014 году, и тогда многие люди не смогли получить свои зарплаты или сбережения. Во избежание подобных инцидентов была создана новая платежная система «Мир», главной целью которой стала защита населения от агрессивной политики западных стран и разорения мирных граждан.

Использовать эту карту внутри страны может каждый. Все российские банки обязуются обеспечивать функционирование данной системе в связке с другими системами, распространенными по всему миру. И все же, стоит задуматься о том, нужно ли доверять иноземным интервентам, или все-таки воспользоваться услугами своих соотечественников.

Некоторые международные банки выступили против этой системы, ведь «Мир» охватывает только одну страну. Часть банкиров, защищая свои вложения, стараются доказать, что это ограничит население в возможностях проведения всевозможных оплат, аргументируя это техническими сложностями.

В отличие от них, более опытные и лояльно настроенные к русским банки не собираются мешать стране в создании собственной системы безналичного расчета. Более того, они готовы помогать в развитии и поддерживать новое начинание. Иметь в стране собственную систему может далеко не любой народ, русским же это доступно и нужно для защиты финансового фонда от внешних недругов.

Создание системы «Мир» позволит снять монополию на использование денежных средств русских с прежних операторов. Это невыгодно для некоторых западных банков, зато поможет стабилизировать финансовую систему в нашей стране.

Известно, что некоторые международные системы согласны подписать кобейджинговые соглашения для выпуска совместных карт. К ним относится и MasterCard. Их новая карта будет представлена под названием «Maestro – Мир». От такого соглашения отказалась только одна из систем, представленных в нашей стране: VISA.

Первые предложения разработать и ввести национальную платежную сеть были озвучены несколько лет назад. Точная дата – 2014 год. Причина – вероятность прекращения действия на территории нашей страны систем Виза и МС из-за введенных санкций.

Изначально планировалось: новая платежная система заработает исключительно на территории России. Позже приняли другое решение: к одному счету можно привязать сразу две карты: обычную и международную (Маэстро).

Вдобавок банки планируют наладить выпуск кобейджинговых кредиток, способных работать за пределами нашей родины. Пока же, наблюдаются некоторые проблемы, связанные с выпуском Мир-Maestro. Объяснение этому – ограничение числа банков-эмитентов.

Это временные трудности. В 2018 году они будут решены.

**3. Предложения и пути по совершенствованию системы информационной безопасности РФ**

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

* Противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;
* Пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;
* Повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;
* Повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;
* Повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;
* Повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;
* Обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет Повышения защищенности соответствующих информационных технологий;
* Совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;
* Повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;
* Нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

**ЗАКЛЮЧЕНИЕ**

Свобода и информация являются основополагающими характеристиками социальных и национальных субъектов. Задача реализации основополагающих жизненных интересов социально-национального субъекта информации приводит к актуальной проблеме защиты конституционных прав и свобод человека и гражданина, а также к эффективной защите информации в сфере доступа к информации. Таким образом, информационная безопасность - это состояние общества, в котором надежная и всесторонняя защита личности, общества и государства обеспечивается всевозможными информационными угрозами и радикальными политическими и социальными силами. Анализируя вышеизложенную концепцию информационной безопасности, можно сделать следующие выводы:

1. Информационный сектор, как координирующий фактор социальной и национальной жизни, требует выявления потребностей в информационной и психологической безопасности личности, общества и государства, перестройки существующей правовой базы, обеспечивающей надлежащую защиту интересов личности, общества и государства в сфере информации.

2. Несмотря на то, что большинство исследователей уделяют внимание вопросам информационной безопасности в РФ, ощутимого прогресса в области их социофилософского осмысления не наблюдается. Как уже отмечалось выше, ряд методологических аспектов данного вопроса недостаточно проработан, что затрудняет создание эффективной системы информационной безопасности.

3. Термин «Информационная безопасность» имеет более широкое значение в официальном понятии. Это обусловлено односторонним сочетанием понятий национальной безопасности и информационной безопасности.

4. Анализ вопросов информационной безопасности должен включать выявление интересов субъектов информационных отношений, связанных с использованием информационных систем. Риск для информационной безопасности - это только противоположный сайт использования информационных технологий.

5. Картирование интересов субъектов, связанных с использованием информационных технологий, можно разделить на компоненты обеспечения доступности, целостности и конфиденциальности информации и вспомогательную инфраструктуру. Ключевым моментом в различных видах деятельности в сфере информационной безопасности является эффективная и комплексная защита социальных, национальных и государственных интересов субъектов информационных отношений.

6. Эффективная государственная политика в сфере информационной безопасности во многом зависит от правильного выбора исследовательских приоритетов национальных проблем, уровня междисциплинарных и философских подходов к их решению.

# Список использованных источников

1. [Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"](http://www.consultant.ru/document/cons_doc_LAW_208191/)

2. "Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года" (утв. Президентом РФ 24.07.2013 N Пр-1753)

3. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2015. — 136 c.
4. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2016. — 324 c.
5. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 c.
6. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга… — М.: ЮНИТИ-ДАНА, 2015. — 239 c.
7. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 c.
8. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2016. — 536 c.
9. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2015. — 558 c.
10. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2015. — 280 c.
11. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2014. — 432 c.
12. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2014. — 296 c.
13. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2014. — 277 c.
14. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2015. — 336 c.
15. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2015. — 416 c.
16. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2015. — 702 c.
17. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2016. — 544 c.
18. Ярочкин, В.И. Информационная безопасность. 5-е изд. / В.И. Ярочкин. — М.: Академический проект, 2016. — 544 c.

19. Скородумова О. Б. Хакеры // Знание. Понимание. Умение. — 2015. — № 4. — С. 159161. 6.

20. В.А.Каймин. Информатика. учебное пособие. 2-ое изд. М.РИОР,2007, 129с. ISBN 536900179-0 7.

21. Щербаков А. Ю., Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.:Книжный мир, 2015. — 352 с — ISBN 978-5-8041-03782. 8.

22. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2015. — 176 с — ISBN 978985-463-258-2. 9.

23. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2014. — 208 с — ISBN 5-8459-0323-8, ISBN 1-5787-0264-X.