Перевод

ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МОЛДОВА

ПОСТАНОВЛЕНИЕ №992

от 10 октября 2018 г.
Кишинэу

О проекте постановления Парламента об утверждении Стратегии информационной безопасности Республики Молдова на 2019-2024 годы и Плана действий по ее внедрению

В целях исполнения статьи 3 Закона № 299/2017 об утверждении Концепции информационной безопасности Республики Молдова (Официальный монитор Республики Молдова, 2018 г., № 48-57, ст. 122) Правительство ПОСТАНОВЛЯЕТ:

1. Одобрить и представить Парламенту на рассмотрение проект постановления Парламента об утверждении Стратегии информационной безопасности Республики Молдова на 2019-2024 годы и Плана действий по ее внедрению (прилагается).

2. Финансирование мер, предусмотренных в Плане действий по внедрению Стратегии информационной безопасности Республики Молдова на 2019-2024 годы, осуществлять за счет и в пределах средств, утвержденных в бюджетах ответственных за реализацию учреждений. Примерная стоимость действий будет корректироваться в ходе внедрения Плана действий, исходя из объема доступных средств в государственном бюджете.

Премьер-министр **ПАВЕЛ ФИЛИП**

Контрасигнуют:

Министр финансов Октавиан Армашу

Министр юстиции Виктория Ифтоди

Проект
Перевод

ПАРЛАМЕНТ РЕСПУБЛИКИ МОЛДОВА

ПОСТАНОВЛЕНИЕ
об утверждении Стратегии информационной безопасности Республики Молдова на 2019-2024 годы и Плана действий по ее внедрению

Парламент принимает настоящее постановление.

Ст. 1. – Утвердить:

1) Стратегию информационной безопасности Республики Молдова на 2019-2024 годы согласно приложению № 1;

2) План действий по внедрению Стратегии информационной безопасности Республики Молдова на 2019-2024 годы согласно приложению № 2.

Ст. 2. – Министерствам, учреждениям и другим центральным административным органам, начиная с 2020 года, ежегодно, до 1 марта, представлять Службе информации и безопасности Республики Молдова информацию о выполнении Плана действий по внедрению Стратегии информационной безопасности Республики Молдова на 2019-2024 годы, согласно установленным компетенциям.

Ст. 3. – Службе информации и безопасности Республики Молдова представлять Парламенту ежегодно, до 31 марта, отчет о внедрении Стратегии и выполнении Плана действий, указанных в статье 1, и размещать на официальной странице отчет о результатах ее внедрения.

Ст. 4. – Мониторинг и оценка внедрения Стратегии информационной безопасности Республики Молдова на 2019-2024 годы осуществлять посредством предусмотренных ею инструментов.

Председатель Парламента

Приложение № 1

СТРАТЕГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ МОЛДОВА НА 2019-2024 ГОДЫ

I. ВВЕДЕНИЕ

1. Информационные технологии, информационные ресурсы и системы электронной коммуникации стали неотъемлемой частью всех сфер деятельности человека, общества и государства. Благодаря их стремительному развитию информационные технологии ведут к существенным социальным преобразованиям, являясь причиной возникновения и укрепления информационного общества на национальном, региональном и международном уровнях, что выходит за юридические рамки государственных границ или сообществ государств.

2. Информационное пространство стало жизненной сферой деятельности для государства, экономики, науки, общества и человека, новым пространством для регулирования прав и основных свобод человека, с прямым и косвенным вовлечением в механизмы проведения политик национальной безопасности и обороны в демократическом обществе.

3. На протяжении последнего десятилетия Республика Молдова реализовала много государственных стратегий, программ и политик для развития информационного общества на национальном уровне в соответствии с рекомендациями европейских и международных форумов в области информационных технологий и электронных коммуникаций, прав и основных свобод человека в онлайн- и офлайн-среде.

4. Согласно Годовому отчету о мониторинге развития информационного общества на мировом уровне «Измерение информационного общества 2017 г.», представленному Международным союзом телекоммуникаций, Республика Молдова находится на 59-ом месте из 176 государств, включенных в рейтинг. На европейском уровне Республика Молдова продвинулась по отношению к глобальным и региональным средствам массовой информации, заняв место в первой десятке государств с наиболее динамичным развитием на мировом уровне[1]. В непрерывный процесс развития внедрено более 21 программ[2] и онлайн-проектов инфраструктуры и цифровых государственных услуг, запущены отраслевые стратегии в области информационных технологий и политики технологической модернизации управления.

---

[1] www.mei.gov.md/ro/content/republica-moldova-urcat-4-pozitii-raportul-mondial-privind-evolutia-societatii;

[2] Согласно пункту 2.3.1 раздела 2.3 главы II Национальной стратегии развития информационного общества «Цифровая Молдова 2020», утвержденной Постановлением Правительства № 857/2013

5. Взаимодействие информационных технологий с многообразием информационного содержания, с одной стороны, и слияние сетей общественной и социальной коммуникации с правительственными электронными системами, с другой стороны, способствуют расширению и взаимодействию информационного пространства с центральными сферами национальной безопасности и обороны, ответственными за обеспечение суверенности, независимости и территориальной целостности Республики Молдова.

6. Информационные технологии способствуют изменению объема информирования и коммуникации, которые стремительно преобразуются в мультимедийную платформу, развивая новые компоненты и средства онлайн- и оффлайн-коммуникации, а свободный оборот информации и идей на местном, региональном и мировом уровнях становится необходимостью для создания и продвижения информированного общества в демократическом и правовом государстве.

7. Тенденции постоянного развития взаимодействия технологического измерения с информационным измерением во всех структурных и функциональных формах индивидуального, общественного, частного или государственного характера на национальном или мировом уровне приводит к возникновению новой конфигурации коммуникации и обмена данными в государственных и частных сферах, от которой зависит уровень и отраслевое либо общее состояние безопасности.

8. Наряду с неоспоримыми преимуществами современных технологий, информационное пространство подвержено ряду уязвимостей, рисков и угроз безопасности, что способствует несправедливой конкуренции, конфронтации и шпионажу, дезинформации и пропаганде, терроризму и преступности, а нарушения конфиденциальности ведут к распространению новых форм ненависти и подстрекательства к насилию, в частности, по половым, расовым, национальным, этническим, языковым, религиозным, политическим признакам или по любым иным критериям, которые остаются недооцененными, и редко удается смягчить их или противодействовать им.

9. Распространение информации без учета национальных границ, помимо очевидных преимуществ, может привести к повышению способности влияния со стороны иностранных или неправительственных и правительственных субъектов с достаточными ресурсами.

10. Киберпреступления, шпионаж, пропаганда, разнообразие и избыточное использование персональных данных в сетях электронной коммуникации являются основными инструментами на всех этапах зарождения гибридной угрозы безопасности и призывают к коллективному

и организованному ответу, основывающемуся на координированных механизмах и действиях по внедрению политик в данной сфере, технической и правовой помощи с точки зрения императивных норм безопасности, нацеленных на создание информационной среды, являющейся благоприятной и безопасной для граждан, для деловой среды любого уровня и для государства.

11. Кампании по дезинформации направлены на усиление недоверия, недоразумения и дестабилизацию общественно-политической ситуации в государстве, воздействие на существующие мнения и предпочтения различных социальных общностей. Это может привести к контролю поведения части общества различными субъектами, а также повлиять на внутреннюю и внешнюю политику государства.

12. Увеличение количества пользователей Интернета и развитие сопутствующих информационных технологий создает ощутимые вызовы для состояния безопасности, общественного порядка и обороны, предотвращения преступности и применения закона для защиты прав в информационном пространстве.

13. Концепция информационной безопасности (далее – *Концепция*), утвержденная Законом № 299/2017, представляет собой основополагающий документ для разработки настоящей Стратегии и документ политик, который охватывает центральные и второстепенные сферы информационного пространства, представляет понятия, определяет принципы организации на уровне государства, общества и человека и подробно описывает правовые, организационно-технические, экономические и контринформационные методы обеспечения информационной безопасности Республики Молдова.

14. Целью Стратегии информационной безопасности Республики Молдова на 2019-2024 годы (*далее – Стратегия*) является (правовая) связка и системная интеграция приоритетных областей с обязанностями и компетенцией по обеспечению информационной безопасности на национальном уровне на основе кибернетической устойчивости, мультимедийного многообразия и институциональной конвергенции в области безопасности, направленных на защиту суверенитета, независимости и территориальной целостности Республики Молдова.

15. Настоящая Стратегия описывает текущую ситуацию в области информационной безопасности с точки зрения зарегистрированных достижений и тенденций развития информационного общества на национальном уровне, существующие и возможные в будущим проблемы, порождающие и создающие риски и угрозы безопасности, в том числе

гибридные. Комплекс мер в соответствии с указанными целями и задачами подразделяется на четыре раздела:

1) Раздел I. Обеспечение безопасности информационно-кибернетического пространства и расследование преступлений в области компьютерной информации;

2) Раздел II. Обеспечение безопасности информационно-медийного пространства;

3) Раздел III. Укрепление операционных возможностей;

4) Раздел IV. Повышение эффективности процесса внутреннего координирования и международного сотрудничества в области информационной безопасности.

16. Цель и задачи настоящей Стратегии будут реализовываться на основании Плана действий по внедрению Стратегии информационной безопасности Республики Молдова на 2019-2024 годы.

II. ОПИСАНИЕ СИТУАЦИИ

17. Республика Молдова как неотъемлемая часть европейского пространства находится в процессе перехода к обществу информационного типа. В соответствии с положениями Соглашения об ассоциации между Республикой Молдова, с одной стороны, и Европейским союзом и Европейским сообществом по атомной энергии и их государствами-членами, с другой стороны[3], установлены приоритеты по стимулированию и продвижению применения инструментов информационно-коммуникационных технологий *(далее – ИКТ)* для лучшего управления, электронного обучения (e-learning) и исследований, государственных медицинских услуг, перевода на цифровую основу культурного наследия, развития цифрового содержания и электронной торговли, а также «повышения уровня безопасности персональных данных и защиты конфиденциальности в электронных коммуникациях».

18. Оценка силы и эффективности системы национальной безопасности в информационном обществе, не принимая во внимание информационные системы и порядок эксплуатации информации (сбор, защита, транспортировка, управление и ограничение доступа к информации) представляет собой серьезный риск, поскольку центр тяжести действий смещается от материального измерения к информационному. С одной стороны, использование информационных технологий способствует значительному повышению силы и эффективности системы национальной безопасности, а с другой стороны, это представляет собой фактор риска в случае незащищенной информационной инфраструктуры.

3 Глава 18 «Информационное общество», Статья 98 Соглашения об ассоциации между РМ и ЕС.

19. Развитие информационной инфраструктуры в процессе глобализации, в который включаются также медийные структуры, ведет к возможности все более и более усовершенствованной коммуникации. Понятие классической войны уступает место информационной войне, которая уже проявляется в нескольких формах/измерениях: психологическая война, имиджелогическая война, командно-контрольная война, электронная война.

20. Политическая, экономическая, социальная и военная сферы являются целями информационной войны, направленной, в первую очередь, на воздействие на процессы принятия решений. В этих условиях обеспечение информационной безопасности является существенным для укрепления социального здравомыслия, сплоченности и интересов общества. Обеспечение информационной безопасности необходимо также для противодействия сверхкоммуникации и злоупотреблению информацией, что приводит к нонкоммуникации и псевдокоммуникации, порождающим социальные расколы и разногласия в гражданском обществе.

21. Взаимодействие в кибернетическом пространстве облегчается различными субъектами: физическими и юридическими лицами, государственными органами и неправительственными структурами, формальными и неформальными группами, персонализированными и анонимными пользователями. Одни из них подключают пользователей, разрешают обработку информации, размещают веб-услуги, в том числе созданное пользователями содержание, другие собирают информацию и разрешают осуществлять поиск, предоставляя доступ к содержанию, носителю, индикаторам и услугам, создаваемым или обрабатываемым третьими лицами. Другая категория субъектов содействует продаже товаров и услуг, в том числе аудиовизуальных, и разрешает осуществлять иные коммерческие, рекламные и платежные операции.

22. Защита прав и свобод физических лиц в отношении обработки персональных данных требует принятия соответствующих технических и организационных мер. В связи с этим контролер персональных данных должен разработать внутренние политики и предпринять меры, которые бы, в частности, соответствовали принципу защиты данных, начиная с момента создания, и принципу защиты данных по умолчанию в соответствии с законодательством о защите персональных данных.

23. Субъекты из кибернетического пространства могут модерировать и размещать содержание, в том числе путем автоматической обработки персональных данных, а также осуществлять иные формы контроля, влияющие на онлайн-доступ пользователей к информации в подобных медиа режимах либо могут выполнять функции, подобные редакторским.

Информационные онлайн-услуги предоставляются также традиционными средствами массовой информации посредством созданных для этой цели электронных платформ.

24. Осознавая важность продвижения сферы ИКТ для развития прогрессивного информационного общества в Республике Молдова, создания и развития интегрированной и эффективной информационно-коммуникационной инфраструктуры, направленной на рост конкурентоспособности национальной экономики, и обеспечения доступа всех граждан к услугам информационного общества, были изменены, дополнены и даже разработаны нормативные акты, недостаточно хорошо регулировавшие отношения субъектов информационного пространства.

25. Основными документами политик, имеющимися на момент разработки настоящей Стратегии, действительными до 2020 года, касательно информационной безопасности, которые должны проецировать на национальный уровень европейскую модель развития информационного общества, являются: Национальная стратегия развития информационного общества «Цифровая Молдова 2020», утвержденная Постановлением Правительства № 857/2013, и Национальная программа кибербезопасности Республики Молдова на 2016-2020 годы, утвержденная Постановлением Правительства № 811/2015.

26. Согласно Плану действий по внедрению Национальной программы кибербезопасности Республики Молдова на 2016-2020 годы, на соответствующий период предусмотрены для реализации 50 мер. Меры из вышеуказанного Плана распределены на следующие области, требующие вмешательств:

1) обработка, хранение и безопасный доступ к данным, в том числе представляющим общественный интерес;
2) безопасность и целостность сетей и услуг в области электронных коммуникаций;
3) развитие способности по предотвращению и срочному реагированию на национальном уровне (создание национальной сети CERT);
4) предотвращение и борьба с информационными преступлениями;
5) укрепление способностей киберзащиты;
6) непрерывное образование, обучение и информирование в области кибербезопасности;
7) международное сотрудничество и взаимодействие в областях, связанных с кибербезопасностью.

27. В то же время, в пункте 26 Программы отмечается, что сфера киберзащиты Республики Молдова должны быть внедрена в Стратегию информационной безопасности Республики Молдова как составная часть. В

связи с этим Стратегия предлагает регулирование и решение некоторых сегментов информационной безопасности, не затрагиваемых ранее.

28. Следовательно, устанавливаем, что применимое законодательство на данный момент не регламентирует предотвращение и борьбу с попытками дезинформации и/или манипуляционного информирования, защиту частной жизни и персональных данных при размещении информации в Интернете из соображений того, что действие этих законов является ограниченным и/или они преследуют другую цель регламентирования.

29. В этих условиях Закон № 299/2017 можно считать отправной точкой для укрепления защиты интересов лиц, общества и государства в информационной сфере, предотвращения и противодействия комплексным и постоянным угрозам информационной безопасности, жизненно и стратегически важных задач для национальной безопасности, обеспечения защиты информации, отнесенной к государственной тайне, предупреждения и борьбы с преступностью в области компьютерной информации.

30. Анализ эволюции социально-медийного феномена и электронной прессы выявляет недостаточное регламентирование компонента защиты медийного пространства от угроз гибридного характера и компонента безопасности. В связи с этим подтверждается важность и необходимость Стратегии, которая бы включала в себя обширное регламентирование всех векторов информационной безопасности.

31. Процесс внедрения информационных технологий во все сферы экономической, общественной и иной жизни Республики Молдова повлек за собой и рост преступности в области компьютерной информации. В результате этого в последние годы было установлено, что информационные системы, сети и данные все чаще используются в преступных целях, а материалы, которые могли бы являться доказательствами этих преступлений, хранятся и передаются преступниками посредством этих же сетей.

32. Риски в киберпространстве пропорциональны степени информированности общества, а борьба с таким явлением, как киберпреступность должна стать первостепенным приоритетом для всех задействованных субъектов. Виртуальная среда способствует совершению преступлений, предоставляет в распоряжение преступника как новый объект (информация, содержащаяся и обрабатываемая информационными системами), так и новый инструмент. Она предоставляет широкий диапазон техник и стратегий для совершения преступлений, создавая новые тенденции преступлений.

33. Информационное мошенничество, информационные атаки, мошенничество с электронными средствами оплаты и детская порнография в глобальной сети Интернет – это типы преступлений, требующие специализированного расследования, соответствующей подготовки и оснащения правоохранительных органов. Информационная преступность – это преступный феномен, связанный, в свою очередь, с множеством рисков и кризисов в киберпространстве, а предотвращение и борьба с информационной преступностью должны стать первоочередным приоритетом всех задействованных субъектов, в особенности на институциональном уровне, где концентрируется ответственность за разработку и применение соответствующих политик в данной области.

34. Принятие Стратегии обусловлено необходимостью защиты интересов лиц, общества, государства в информационном пространстве, тяжестью и многочисленностью угроз для информационной безопасности в современном обществе, необходимостью поддержания равновесия между интересами лиц, общества и государства для обеспечения информационной безопасности. Одновременно, глобальный характер информационных систем и сетей электронной коммуникации требует тесного сотрудничества между всеми ответственными учреждениями, как на национальном, так и на мировом уровне.

III. ОПРЕДЕЛЕНИЕ ПРОБЛЕМ

3.1 Компонент кибербезопасности и расследование преступности в области компьютерной информации.

35. В настоящее время несанкционированный доступ к сетям и услугам электронных коммуникаций, несанкционированное изменение, удаление или повреждение информационных данных, неправомерное ограничение доступа к этим данным и кибершпионаж являются проблемами мирового уровня. Ежегодные доклады международных специализированных агентств устанавливают рост суммарной стоимости киберпреступлений, при этом экономический ущерб оценивается в сотни миллиардов долларов США.

36. Угрозы и риски, кибератаки и инциденты, а также иные события в киберпространстве выражаются в использовании человеческой, технической и процессуальной уязвимости. За последние годы в Республике Молдова установлен рост следующих показателей: количество информационных преступлений и правонарушений; количество кибератак на информационные ресурсы, опубликованные в глобальной сети Интернет, при этом слабые места приложений использовались в целях хищения/изменения/удаления информации.

1) недостаточность квалифицированных специалистов в области информационных технологий и низкий уровень оплаты труда, в частности, в публичном секторе;

2) отсутствие специализированных учебных программ для сотрудников с полномочиями по расследованию и уголовному преследованию, прокуроров, судей, специалистов и судебных экспертов в данной области в правоприменительных структурах, а также для технического персонала государственных учреждений, осуществляющих свою деятельность в области кибербезопасности;

3) недостаточное оснащение специализированным оборудованием и программным обеспечением для расследования информационных преступлений;

4) сокращенное финансирование участия специалистов в международных проектах и событиях по укреплению потенциала и обмену передовым опытом.

42. В ходе расследования информационных преступлений было установлено, что все чаще используются технологии, облегчающие совершение информационных преступлений:

1) средства анонимизации (скрывающие технические идентификационные данные пользователя), пункты беспроводного доступа с неограниченным (открытым) доступом к глобальной сети Интернет в общественных местах;

2) использование асимметричных комплексных алгоритмов для шифрования критической информации при вымогательстве финансовых средств при помощи информационных технологий;

3) использование деконцентрированных платежных систем на основе криптоалгоритмов (криптовалюта);

4) сети прямого обмена данными между пользователями, где не остается никаких следов деятельности в содержании истории, зарегистрированной в информационной системе, или в логах поставщиков услуг;

5) использование веб-хостинга преступниками;

6) «малые» поставщики услуг не обеспечивают даже минимальный уровень кибербезопасности собственной сети и зачастую не ведут учет пользователей услуг и не регистрируют метаданные о доступе к сети Интернет;

7) услуги фиксированного доступа к Интернету, оказываемые на территории Республики Молдова, не контролируются эффективно конституционными органами.

43. Укрепление информационных систем и систем специальных электронных коммуникаций в едином механизме для их надежного и правильного функционирования не может осуществляться без наличия

обновленных нормативных рамок, предусматривающих продвижение развития этих систем. На данный момент нормативные рамки содержат некоторые положения, препятствующие нормальному функционированию информационных систем и систем специальных электронных коммуникаций, в том числе правительственных, как жизненно важных информационных систем для безопасности государства путем введения определенных ограничений в их управление, развитие и обеспечение их безопасности.

44. Ресурсы, имеющиеся у государственных учреждений, являются недостаточными для подготовки и обучения квалифицированных специалистов, а также для их поощрения, что приводит к оттоку специалистов в частный сектор и негативным последствиям для внедрения кибербезопасности.

45. В то же время, система национальной обороны, равно как и прочие сферы стали зависимы от сферы ИКТ. Некоторые компоненты ИКТ национальной системы обороны интегрированы с глобальной сетью Интернет, а информационные сети в сфере обороны созданы на стандартных коммерческих технологиях. Следовательно, они также подвержены рискам кибератак путем использования определенных уязвимостей.

46. На данном этапе технологического прогресса и процесса информатизации экономической, политической, социальной и иных сфер жизни функционирование основных механизмов государства осуществляется путем использования программных продуктов и обмена оцифрованными данными, которые в совокупности образуют критическую информационную инфраструктуру. В данном контексте важно разработать и/или оценить уже существующее законодательство сквозь призму положений Директивы 2008/114/CE «Об идентификации и обозначении европейских критических инфраструктур и оценке необходимости улучшения их защиты», принятой 8 декабря 2008 г., опубликованной в Официальном журнале Европейского союза L345/75 от 23 декабря 2008 г.

3.2 Компонент безопасности медийного пространства

47. Обеспечение информационной безопасности государства является приоритетом для национальной безопасности, являясь одной из главных задач, поставленных во многих законодательных и нормативных актах Республики Молдова, и требует достаточного финансирования.

48. В соответствии с пунктом 4.7 Стратегии национальной безопасности Республики Молдова, утвержденной Постановлением Парламента № 153/2011, информационной безопасности государства

касаются и провокации медийного характера, направленные против Республики Молдова в виде дезинформации и/или манипуляционного информирования извне.

49. На протяжении своего государственного становления, укрепления и развития Республика Молдова неоднократно подвергалась информационной дискредитации, в частности, внешнему воздействию, что оказало существенное отрицательное влияние на население.

50. Интенсификация пропаганды и дезинформации происходят, в частности, во время различных событий, представляющих национальный интерес, в целях оказания влияния на политические решения, как государства, так и граждан. В зависимости от различных внутренних/внешних эволюций упор делается на создание состояния национального недовольства.

51. Острая необходимость защиты безопасности национального информационного пространства осознается как на уровне государственных органов, так и является целью гражданского общества.

52. Озабоченность относительно усиления посягательств извне на информационную безопасность была выражена, в том числе, в Постановлении Парламента № 12/2018, которое устанавливает, что медиа-атаки извне направлены на дискредитацию Республики Молдова, некоторых учреждений и официальных лиц и – что хуже всего – опорочивание граждан страны.

53. Таким образом, Парламент установил, что «пропаганда превратилась в настоящий инструмент дискредитации Республики Молдова, о чем свидетельствуют многочисленные доклады, представленные общественности гражданским обществом и независимыми международными организациями, в особенности на протяжении последнего года, указывающие на угрожающий размах этого явления».

54. В то же время, данный вопрос является актуальным, как на международном, так и на региональном уровнях. В этом смысле в своей Резолюции от 23 ноября 2016 года о стратегическом сообщении Европейского союза для противодействия пропаганде против него третьими лицами *(2016/2030 (INI))* Европейский Парламент заявляет, что «ЕС, его государства-члены и граждане находятся под растущим систематическим давлением при противостоянии информационным и дезинформационным кампаниям и пропаганде со стороны некоторых стран и негосударственных субъектов, таких как соседние транснациональные террористические и криминальные организации, намеревающиеся подорвать само понятие объективного информирования или этической

журналистики, распространяя всю информацию предвзято или в качестве инструмента политической власти, а также нацеливающуюся на демократические ценности и интересы».

55. Технологии информационной войны используются для узаконивания действий, подрывающих суверенность, независимость и территориальную целостность, в связи с чем государства-члены ЕС и их партнеры должны осуществлять «критическую оценку порядка, в котором следует относиться к источникам средств массовой информации с доказанным прошлым неоднократного вовлечения в стратегию обмана или преднамеренной дезинформации, в частности, в новых средствах информации, социальных сетях и цифровой сфере».

56. На данном этапе пропаганда, дезинформация и/или манипулятивное информирование являются чрезвычайно динамичными, а ресурсы, выделяемые для этой цели третьими лицами, намного превышают способности ответа и борьбы Республики Молдова с данным явлением.

57. Для того, чтобы справиться с данными вызовами, Республика Молдова пользуется поддержкой Европейского союза, который увеличил бюджет на следующие годы для борьбы с пропагандой и дезинформацией, при этом отдельный акцент сделан на государства-члены Восточного партнерства.

58. Осознание рисков, возникающих вследствие влияния пропаганды извне, влечет за собой меры по гармонизации национальных политик, а принятие настоящей Стратегии должно содействовать достижению этой цели.

3.3 Компонент контринформации и безопасности

59. Информационное оружие, выступая в качестве существенного компонента гибридных угроз, используется иностранными подрывными центрами (спецслужбы, неправительственные организации под руководством государственных и негосударственных субъектов, контролируемые средства массовой информации и т.п.) при осуществлении информационных операций или кибератак, подчиняющихся определенной стратегической цели.

60. В соответствии с Резолюцией Европейского Парламента от 23 ноября 2016 года о стратегическом сообщении Европейского союза (2016/2030 (INI), «службы безопасности и информации пришли к выводу, что некоторые негосударственные субъекты способны и намерены осуществлять операции, нацеленные на дестабилизацию государств, подчеркивая, что зачастую это происходит в форме оказания поддержки

политическим экстремистам и широкомасштабных кампаний массовой информации и дезинформации». Следует отметить, что подобные общества СМИ существуют и осуществляют свою деятельность и в Республике Молдова.

61. Анализ внутренней и региональной среды безопасности отображает обширное использование различными субъектами средств вмешательства во внутренние дела Республики Молдова путем пропаганды и медийной агрессии, а также информационно-психологического воздействия в целях дестабилизации общественно-политической ситуации и подрыва суверенности и территориальной целостности Республики Молдова.

62. В эти мероприятия информационно-пропагандистского характера по части медийного пространства вовлечены ассоциативные структуры, информационно-аналитические центры, агентства печати, а также индивидуальные группы граждан, финансируемые подрывными центрами и спецслужбами иностранных государств, которые при помощи информационных технологий используют гибридные инструменты «мягкой силы» (soft power).

63. Опасность таких типов угроз весьма высока благодаря различным тактикам, действиям и средствам, используемым для достижения своих целей. Таким образом, можно говорить о специфических угрозах безопасности, знание которых поможет предпринять эффективные меры по предотвращению и/или ограничению нежелательных последствий.

64. С другой стороны, исламистские террористические организации активно проводят кампании по информированию в целях подрыва и повышения уровня ненависти к европейским ценностям и интересам. Следует отметить широкое использование этими организациями социальных медиа-инструментов и, в частности, социальных сетей для пропаганды и рекрутинга, особенно в кругах молодежи.

65. В связи с этим на европейском уровне уже рационализирована необходимость включения «антипропагандистской стратегии против исламистских террористических организаций» в более полную и обширную региональную стратегию, сочетающую в себе дипломатические, общественно-экономические инструменты, инструменты развития и инструменты для предотвращения конфликтов.

3.4 Определение проблем правового характера

66. Некоторые государственные и негосударственные субъекты пользуются отсутствием международной правовой базы в области

кибербезопасности, отсутствием ответственности относительно регламентирования средств массовой информации в Интернете и используют любые недостатки в этих вопросах.

67. Что касается кибербезопасности, Республика Молдова ратифицировала Конвенцию Совета Европы о преступности в сфере компьютерной информации на основании Закона № 6/2009. В то же время был принят Закон № 20/2009 о предупреждении и борьбе с преступностью в сфере компьютерной информации, были внесены изменения и дополнения в Уголовный кодекс Республики Молдова № 985/2002 в соответствии с положениями ратифицированной Конвенции. Вместе с тем, не были полностью внедрены многие положения материального и процессуального характера, а также не были внедрены положения, связанные с развитием контактного пункта сети 24/7.

68. Дополнительно следует отметить, что до настоящего времени не существует законодательной базы относительно разграничения и согласования компетенций и ответственности государственных и частных учреждений в области кибербезопасности, не применяется обязательный механизм аудита кибербезопасности в государственных и частных учреждениях, посредством которого могут быть выявлены кибернетические уязвимости, риски и угрозы с целью предотвращения или уменьшения при помощи специальных мер воздействия произошедших в киберпространстве атак, инцидентов и других событий, происхождение которых трудно определить.

69. В результате анализа национального законодательства в области предупреждения и борьбы с преступностью в сфере компьютерной информации был обнаружен ряд барьеров и пробелов нормативного характера, в том числе:

1) Уголовный кодекс Республики Молдова № 985/2002:

a) ст. 178 «Нарушение тайны переписки» не предусматривает уголовную ответственность за деяния, совершенные в отношении электронной переписки (обмена сообщениями), поскольку понятие «почтовые отправления» согласно Закону о почтовой связи № 36/2016 предусматривает только пересылаемые и получаемые предметы;

b) ст. 208^1 «Детская порнография» не наказывается сознательное получение доступа посредством информационно-коммуникационных технологий к детской порнографии, хоть это и предусмотрено в Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия, заключенной в Лансароте 25 октября 2007 г., ратифицированной Законом № 263/2011;

c) большинство преступлений, предусмотренных в главе XI Особенной части Уголовного кодекса (Преступления в сфере компьютерной информации и преступления в сфере телекоммуникаций)

имеют материальную составляющую и наказуемы только в случае причинения ущерба в крупном размере;

2) Уголовно-процессуальный кодекс Республики Молдова №122/2003:

a) не регламентируется процедура «информационного обыска», предусмотренная Конвенцией Совета Европы о преступности в области компьютерной информации (Будапешт, 2001 г.);

b) отсутствует такое специальное розыскное мероприятие, как перехват информационных данных;

c) законодательная база не позволяет осуществление необходимых специальных розыскных мероприятий при документировании преступлений в области компьютерной информации;

d) не предусмотрено ограничение доступа к веб-страницам, в том числе размещенным соответствующим поставщиком, которые содержат информацию, представляющую угрозу для жизни, здоровья и нормального развития детей, пропагандирующую войну или терроризм, призывающую к ненависти или национальной, расовой или религиозной дискриминации, вражде или насилию.

70. Также установлено отсутствие нормативной базы, регулирующей национальную критическую инфраструктуру, а также отсутствие четкой классификации информационных систем в зависимости от типа содержащихся в них данных, типа доступа к ним и их назначения, определения инцидентов кибербезопасности, анализа и оценки причиненного данными инцидентами ущерба, а также применяемых в связи с этим санкций, в том числе определения действий, которые могут стать причиной инцидентов кибербезопасности. Отсутствует нормативное регулирование механизма обмена информацией об инцидентах кибербезопасности между юридическими лицами вне зависимости от их формы собственности и между юридическими и физическими лицами.

3.5 Определение проблем массовой осознанности

71. В данной главе необходимо выделить важность информирования, обучения медийной и кибернетической грамотности в Республике Молдова для того, чтобы позволить гражданам критически анализировать медийное содержание с целью идентификации пропаганды.

72. Отсутствие способности защиты против такого явления, как диффамация посредством онлайн-платформ, мешает осуществлению прав и основных свобод человека. В этих условиях приведение национальной законодательной базы в соответствие с европейскими стандартами в части соблюдения прав человека в информационном пространстве является безусловным приоритетом для Республики Молдова.

73. Для этого необходимо проводить мероприятия по укреплению базы знаний на всех уровнях образовательной системы, а также мотивировать/призывать граждан к активности и развитию своей осознанности в качестве потребителей средств массовой информации.

74. Другим элементом, который необходимо осознать, является центральная роль инструментов, предоставляемых Интернетом (в частности, социальными сетями), в котором распространение ложной информации и проведение дезинформационных кампаний легко осуществимы, зачастую без каких-либо препятствий.

75. На протяжении 2017 года проблема ложных новостей стала темой заседаний Европейской комиссии, которая приняла решение о создании рабочей группы на высоком уровне для разработки и представления стратегии по борьбе с ложными новостями в 2018 г., за год до европейских выборов. По ее оценкам «противодействие пропаганде пропагандой является контрпродуктивным» и государства-члены ЕС должны бороться с ней только путем прекращения дезинформационных кампаний и использования позитивных сообщений и информации. В связи с этим эксперты рекомендуют «развитие эффективной стратегии, которая не будет принята в зависимости от характера субъектов, распространяющих пропаганду»[5].

IV. ВИДЕНИЕ И ЦЕЛИ СТРАТЕГИИ

76. Правительство Республики Молдова, органы публичного управления, учреждения, государственные предприятия, вне зависимости от их форм собственности, и гражданское общество установили следующее стратегическое видение:

Республика Молдова обеспечит безопасное информационное пространство для всех субъектов права путем гармонизации законодательной базы и ее внедрения, таким образом, защищая права и основные свободы человека и укрепляя демократию и правовое государство.

77. Для реализации этого стратегического видения были установлены основные задачи, действия по его внедрению и показатели результативности.

[5] В соответствии с п. 46 Стратегической коммуникации ЕС о противодействии пропаганде против него третьими лицами.

4.1. Раздел I. Обеспечение безопасности информационно-кибернетического пространства и расследование преступлений в области компьютерной информации;

78. Задача № 1. Создание интегрированной системы сообщения и оценки угроз информационной безопасности и разработки оперативных мер противодействия

Данная задача будет выполнена путем осуществления следующих действий:

1) создание/назначение учреждения, которое будет выполнять роль Национального центра реагирования на инциденты кибербезопасности и представлять собой единую точку отчетности по инцидентам кибербезопасности для компетентных органов публичной власти и физических и юридических лиц:

2) назначение учреждения, которое будет выполнять роль Правительственного центра реагирования на инциденты кибербезопасности и представлять собой точку отчетности по инцидентам кибербезопасности Правительства и установление его взаимодействия с Национальным центром реагирования на инциденты кибербезопасности;

3) установление Национальным центром реагирования на инциденты кибербезопасности показателей из области кибербезопасности, систематизация статистических данных с сфере кибербезопасности, их анализ и оценка;

4) разработка механизмов создания и укрепления внутриведомственных центров реагирования на инциденты кибернетической и информационной безопасности как публичного, так и частного права;

5) разработка нормативной базы для обеспечения высокого уровня безопасности информационных сетей и систем на национальном уровне на основе лучших практик ЕС;

6) установление политики относительно порядка отчетности, хранения и обработки информации по инцидентам и угрозам информационной безопасности.

79. Задача № 2. Постоянный мониторинг и обеспечение высокого уровня кибербезопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) установление и устранение источников угроз безопасности лиц, общества и государства в киберпространстве;

а) проведение аудита кибербезопасности инфраструктур информационных технологий национального интереса, а также других кибернетических инфраструктур национального интереса в целях

установления нарушений и уязвимостей, и предоставление решений/рекомендаций по их устранению;

b) внедрение результатов аудита кибербезопасности;

2) обеспечение применения минимальных требований кибербезопасности II уровня в рамках предоставления публичных электронных услуг, определение основных направлений деятельности для предотвращения и пресечения соответствующих угроз;

3) разработка механизмов и методов по предупреждению и пресечению угроз в киберпространстве, вызванных информационными услугами, оказываемыми физическими и юридическими лицами;

4) установление законного механизма взаимодействия между компетентными органами публичной власти и физическими и юридическими лицами, независимо от типа собственности, в целях предоставления ими доступа к исходному коду приложений, разработанных, реализованных и распределенных для органов публичной власти;

5) согласование с Национальным центром по защите персональных данных мер по защите персональных данных, обеспечивающих применение принципа защиты данных, начиная с момента понимания и подразумеваемой защиты данных, когда разрабатываются, планируются, отбираются и используются приложения, услуги и продукты, основывающиеся на обработке персональных данных, или которые обрабатывают персональные данные в соответствии с законодательством о защите персональных данных.

80. Задача № 3. Укрепление потенциала по киберзащите

Данная задача будет выполнена путем осуществления следующих действий:

1) разграничение и распределение ролей и ответственности относительно киберзащиты, системы органов безопасности государства и национальной системы защиты;

2) разработка мер по киберзащите для защиты национальной критической инфраструктуры, а также в рамках других приоритетных отраслей государства;

3) разработка и внедрение мер по защите информационных систем, обрабатывающих информацию, относящуюся к государственной тайне, и компонента ИТС системы национальной обороны.

81. Задача № 4. Защита сетей специальной связи Республики Молдова и информации ограниченного доступа с целью поддержания жизненно важных функций государства

Данная задача будет выполнена путем осуществления следующих действий:

1) развитие механизмов защиты специальных систем электронных коммуникаций посредством применения средств криптографической и технической защиты информации;

2) осуществление контроля над специальными системами электронных коммуникаций и сообщение ответственному органу о технических и организационно-технических мерах, предпринятых для обеспечения кибербезопасности;

3) обновление нормативной базы в области специальных систем электронных коммуникаций;

4) разработка системы аттестации объектов информатизации (размещение статей в глобальной сети Интернет, на информационных веб-страницах, в базах данных или других источниках информационного характера) на соответствие требованиям по обеспечению защиты информации при проведении работ, связанных с обработкой и хранением информации ограниченного доступа, в особенности той, которая относится к государственной тайне;

5) установление мер по обеспечению безопасности персональных данных в контексте обеспечения кибербезопасности;

6) продвижение нормативной базы относительно обучения подразделений, ответственных за защиту персональных данных в рамках органов публичного и частного права.

82. Задача № 5. Обеспечение контроля за импортом, сертификацией и применением средств защиты информации

Данная задача будет выполнена путем осуществления следующих действий:

1) сертификация средств технической и криптографической защиты информации;

2) развитие систем мониторинга импорта средств защиты информации;

3) согласование нормативной базы в сфере криптографической защиты информации с европейскими нормами;

4) создание базы данных относительно средств технической и криптографической защиты информации;

5) осуществление контроля в области применения всех типов электронных подписей.

83. Задача № 6. Борьба с информационной преступностью

Данная задача будет выполнена путем осуществления следующих действий:

1) повышение потенциала (увеличение эффективности механизма) по борьбе с преступностью в области компьютерной информации;

2) предоставление методико-практической помощи территориальным подразделениям относительно расследования информационных преступлений;

3) внедрение новых механизмов на уровне учреждений, вовлеченных в борьбу с преступностью в области компьютерной информации (привлечение частных компаний и независимых экспертов, развитие лабораторий);

4) усовершенствование законодательной базы, регламентирующей оплату труда персоналу, специализирующемуся на борьбе с информационной преступностью и расследовании информационных преступлений.

84. Задача № 7. Защита детей в онлайн-пространстве от любой формы насилия

Данная задача будет выполнена путем осуществления следующих действий:

1) борьба с феноменом детской порнографии в Интернете;

2) борьба с феноменом груминга и сексуального домогательства детей в Интернете;

3) продвижение более безопасного Интернета для детей посредством онлайн-консультаций и поощрения информирования путем специальных информационных проектов.

85. Задача № 8. Борьба с мошенничеством посредством использования электронных средств оплаты

Данная задача будет выполнена путем осуществления следующих действий:

1) обмен информацией между Центром по борьбе с информационными преступлениями и департаментами безопасности финансовых учреждений;

2) продвижение мер повышенной безопасности в отношении МТО на уровне аппаратного и программного обеспечения;

3) установление общих механизмов по борьбе с мошенничеством по операциям с и без присутствия карт.

86. Задача № 9. Развитие институционального потенциала в борьбе с информационной преступностью

Данная задача будет выполнена путем осуществления следующих действий:

1) развитие специализированных подразделений в Генеральном инспекторате полиции Министерства внутренних дел, Генеральной прокуратуре, Службе информации и безопасности Республики Молдова с

целью выявления и противодействия преступным попыткам в данной области;

2) создание национальной базы данных относительно развития феномена информационной преступности;

3) корректировка деятельности, осуществляемой в области информационной преступности в Центральном банке данных автоматизированной информационной системы «Реестр криминалистической и криминологической информации»;

4) разработка нормативной базы, регламентирующей создание Автоматизированной информационной системы «е-Судебное дело» в органах, вовлеченных в проведение уголовного преследования и судебного рассмотрения дела, а также ее внедрение, развитие и подключение.

87. Задача № 10. Осуществление научно-прикладных исследований в области информационной безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) планирование и развитие научно-исследовательской деятельности в области информационно-коммуникационных технологий;

2) создание/укрепление лабораторий кибербезопасности в учреждениях высшего образования и научно-исследовательских учреждениях.

88. Задача № 11. Развитие информационной и кибернетической устойчивости и повышение уровня культуры в области ИТС

Данная задача будет выполнена путем осуществления следующих действий:

1) проведение действий по осведомлению и информированию общества относительно угроз, уязвимостей и рисков кибербезопасности;

2) проведение Национальным центром реагирования на инциденты кибебезопасности стратегического анализа инцидентов кибебезопасности и согласование ответных действий на инциденты безопасности, в том числе посредством организации специальных курсов квалифицированными экспертами;

3) проведение общих занятий и тренировок по укреплению потенциала реагирования на кибератаки, в том числе по блокировке ложных кибератак;

4) организация и проведение рабочих семинаров в области кибербезопасности для персонала публичного и частного секторов, владельцев элементов критической инфраструктуры;

5) сертификация специалистов в области кибербезопасности специализированными организациями/компаниями, исходя из

применяемых стандартов и утвержденных минимальных обязательных требований по кибербезопасности;

6) создание веб-платформ по осведомлению и информированию относительно угроз в киберпространстве и мер защиты, которые могут быть приняты физическими и юридическими лицами;

7) введение и продвижение куррикулярного содержания об информационной безопасности в национальных учебных программах;

8) организация, в том числе совместно с иностранными партнерами, тематических учебных курсов в области кибербезопасности для работников государственных учреждений;

Приоритеты раздела I	**Показатели результативности**
1. Создание Национального центра реагирования на инциденты кибербезопасности (национальный CERT)	1. Создан Национальный центр, разрабатывающий документы политик и обеспечивающий взаимодействие между всеми компонентами обеспечения кибербезопасности
2. Назначение органа, выполняющего роль Правительственного центра реагирования на инциденты кибербезопасности Правительства (Правительственный CERT)	2. Обеспечение Правительственным центром функционирования и защиты специальных сетей на уровне Правительства и органов публичной власти
3. Укрепление сотрудничества национального CERT, правительственного CERT и частных CERT	3. Соглашения о сотрудничестве и обеспечении устойчивости в целях предотвращения и устранения инцидентов кибербезопасности

4.2. Раздел II. Обеспечение безопасности информационно-медийного пространства

89. Задача № 1. Развитие механизмов стратегической коммуникации для реализации национальных интересов Республики Молдова

Данная задача будет выполнена путем осуществления следующих действий:

1) определение уязвимых секторов медийного компонента системы информационной безопасности;

2) развитие политик стратегической коммуникации на внутреннем плане и подключение к внешним платформам стратегической

коммуникации структур системы безопасности, обороны и общественного порядка для обеспечения информационной безопасности и продвижения национальных интересов Республики Молдова;

3) создание в Республике Молдова информационного ресурса/платформы стратегической коммуникации, содержащей информацию:

a) об инцидентах информационной безопасности;

b) руководствах стратегической коммуникации по субъектам национального интереса;

c) попытках и действиях дезинформации и/или манипулятивной подачи информации, затрагивающих информационную безопасность и общее состояние безопасности.

90. Задача № 2. Гражданский контроль и укрепление сотрудничества гражданского общества с органами публичной власти с функциями обеспечения информационной безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) создание механизма привлечения экспертов из рядов гражданского общества, неправительственных организаций и средств массовой информации в области информационной безопасности путем:

a) назначения существующего совета или создание коллективного органа из гражданского общества с полномочиями по оценке экспертов, неправительственных организаций и средств массовой информации с точки зрения их привлечения в процесс обеспечения информационной безопасности;

b) сертификация Советом гражданского общества экспертов и представителей гражданского общества и средств массовой информации, осуществляющих мониторинг степени обеспечения информационной безопасности на национальном уровне;

2) привлечение представителей гражданского общества, сертифицированных Советом гражданского общества, в состав Координационного совета по обеспечению информационной безопасности;

3) улучшение или создание механизмов привлечения гражданского общества к процессам определения, разработки, мониторинга и оценки политик обеспечения информационной безопасности, проводимых компетентными в области обеспечения информационной безопасности органами;

4) разработка и организация тематических учебных курсов для радиовещателей, распространителей услуг, субъектов, формирующих общественное мнение, журналистов и профильных неправительственных организаций о техниках дезинформации и/или манипулятивной подачи

информации, используемых для причинения вреда информационной безопасности государства.

91. Задача № 3. Определение правового статуса периодических изданий, агентств печати и иных субъектов, осуществляющих свою деятельность в медийном пространстве Интернета

Данная задача будет выполнена путем осуществления следующих действий:

1) оценка Интернет-пространства с перспективы установления субъектов, вовлеченных в производство и распространение медиасодержания онлайн, и других посредников и дополнительных услуг, оказывающих отрицательное влияние на информационную безопасность;

2) разработка и корректировка функциональной законодательной базы в целях правового регламентирования отношений между субъектами средств массовой информации, собирающими и распространяющими информацию в Интернете, обществом и уполномоченными органами с функциями в области обеспечения информационной безопасности, в соответствии с рекомендациями Европейской комиссии и надлежащими европейскими практиками;

3) внедрение нормативной базы, установленной общими действиями по вмешательству и управлению медиапространством онлайн и офлайн.

92. Задача № 4. Обеспечение финансовой прозрачности в деятельности органов публичной власти, общественных объединений и коммерческих обществ в контексте обеспечения информационной безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) разработка под руководством Координационного совета по обеспечению информационной безопасности критериев квалификации информации как продукта дезинформации, манипуляции и пропаганды, направленных на подрыв информационной безопасности, с целью выявления заказчиков, источников финансирования и исполнителей;

2) изменение законодательной базы в целях повышения эффективности сбора данных для установления происхождения финансовых средств и собственности субъектов, вовлеченных в деятельность по дезинформации, манипулированию и пропаганде, подрывающую информационную безопасность;

3) взаимодействие с правовыми учреждениями в сфере анализа рисков и угроз в области масс-медиа, в целях контроля развития обнаруженных угроз, исследования подрывной или уголовной

деятельности в информационном пространстве, установления источников финансирования факторов риска.

Приоритеты раздела II	Показатели результативности
1. Развитие инструментов гражданского контроля для обеспечения информационной безопасности	1. Механизм взаимодействия и привлечения экспертов с целью обеспечения безопасности информационного пространства
2. Разработка законодательной базы для определения правового статуса периодических изданий, агентств печати и иных субъектов, осуществляющих свою деятельность в медийном пространстве Интернета	2. Закон о внесении изменений/дополнений в существующую правовую базу
3. Создание информационного ресурса/информационной платформы стратегической коммуникации	3. Создан ресурс для стратегической коммуникации и информирования

4.3. Раздел III. Укрепление операционных возможностей

93. Задача № 1. Развитие механизмов предупреждения, выявления, смягчения и ответа на национальном уровне для обеспечения информационной безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) создание на национальном уровне подразделения, владеющего компетенциями по продвижению и согласованию политик информационной безопасности в демократическом обществе, в зависимости от развития технологии, правовых и другого характера отношений сектора информационного общества на национальном и международном уровне (Координационный совет по обеспечению информационной безопасности):

а) установление и интеграция существующих компонентов с функциями и полномочиями в кибернетической, медийной области и органов местного публичного управления и тех, которые будут созданы в процессе;

b) установление направления деятельности для каждого компонента, включенного в подразделение, в зависимости от выполняемых функций и полномочий из перспективы обеспечения информационной безопасности;

c) разработка и утверждение нормативно-законодательной базы взаимодействия для реализации задач по обнаружению, предупреждению и пресечению рисков и угроз информационной безопасности;

2) разработка, продвижение и согласование политик информационной безопасности согласно Концепции, настоящей Стратегии и другим документам политик на национальном и международном уровне относительно информационной безопасности;

3) информирование населения относительно способов предупреждения и пресечения рисков и угроз системным компонентам информационной безопасности, в том числе новых возникших феноменов на национальном уровне.

94. Задача № 2. Развитие потенциала реагирования в случае гибридных угроз безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) создание специального аналитико-информационного компонента по гибридным угрозам безопасности в рамках Службы информации и безопасности;

2) создание национальной сети органов, ответственных за борьбу с гибридными угрозами безопасности;

3) разработка операционных протоколов взаимодействия между ответственными органами и руководящими органами в случае некоторых гибридных угроз безопасности;

4) укрепление степени познания и понимания концепции гибридных угроз безопасности на уровне органов, уполномоченных в области информационной безопасности и общей среды безопасности;

5) проведение подготовки для развития потенциала органов, специализирующихся на борьбе с гибридными угрозами безопасности;

6) ассоциация Республики Молдова к Европейскому центру совершенства в борьбе с гибридными угрозами и к Центру совершенства стратегической коммуникации НАТО.

95. Задача № 3. Развитие операционного потенциала по кибероборонe

Данная задача будет выполнена путем осуществления следующих действий:

1) создание подразделения, ответственного за кибероборону на уровне Вооруженных сил;

2) укрепление потенциала по киберобразованию и обучению посредством участия в межгосударственных и международных тренингах по кибероборонe;

3) установление, предупреждение и пресечение факторов риска с информативно-подрывным потенциалом киберзащиты Республики Молдова посредством внедрения интегрированного менеджмента виртуального пространства и развития системы по преждевременному предупреждению относительно элементов риска объектов инфраструктуры.

96. Задача № 4. Мониторинг информационного пространства и выявление внутренних и внешних действий по дезинформации и/или манипулятивной подачи информации

Данная задача будет выполнена путем осуществления следующих действий:

1) пересмотр существующей правовой базы в части установления и уравнивания понятий относительно дезинформации, ложных новостей и/или манипулятивной подачи информации, а также предупреждение ее распространения посредством медиаплатформ. Установление секторов национальной безопасности, нарушение которых (посредством дезинформации) создает высокие риски для функциональности государства;

2) установление полномочий (компетентных органов) для обнаружения и пресечения манипулятивных и дезинформационных сообщений из информационного пространства (Интернет);

3) установление некоторых фильтров по обнаружению и/или блокированию информационных ресурсов, содержащих элементы риска национальной безопасности, а также разработка, утверждение соответствующей нормативной базы.

97. Задача № 5. Повышение потенциала защиты национальных критических инфраструктур

Данная задача будет выполнена путем осуществления следующих действий:

1) разработка и утверждение законной базы относительно установления и обозначения национальных критичных инфраструктур, в том числе относительно жизненно важных информационных систем;

2) оценка и информирование относительно состояния и уровня безопасности объектов инфраструктуры из перспективы обеспечения информационной безопасности.

98. Задача № 6. Развитие потенциала по предупреждению, выявлению и противодействию экстремистским, террористическим и

иного рода действиям, представляющим угрозу информационной безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) синхронизация и рациональное распределение сил учреждений Республики Молдова на предварительное выявление действий, совершаемых извне и/или внутри страны с целью сложных диверсий против информационной безопасности;

2) предоставление Службе информации и безопасности информации о ситуации риска государственными учреждениями, компетентными в данной области.

Приоритеты раздела III	**Показатели результативности**
1. Создание на национальном уровне Координационного совета по обеспечению информационной безопасности, в рамках которого будут выявляться процедуры стратегической коммуникации	1. Разработанная и утвержденная нормативная база о создании Координационного совета по обеспечению информационной безопасности
2. Создание органа, ответственного за киберзащиту, на уровне Вооруженных сил	2. Нормативная база о создании на национальном уровне органа, ответственного за киберзащиту, на уровне Вооруженных сил
3. Создание платформы, специализирующейся на гибридных угрозах безопасности	3. Созданная функциональная платформа
4. Разработка и внедрение законодательной базы по регламентированию национальной критической инфраструктуры	4. Разработанная и утвержденная законодательная база

4.4. Раздел IV. Повышение эффективности процесса внутреннего согласования и международного сотрудничества в области информационной безопасности

99. Задача № 1. Развитие системы подготовки кадров в области информационной безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) оценка актуального уровня подготовки кадров в области информационной безопасности по каждому разделу в отдельности:

средства массовой информации, информационные технологии, оборона, общественный порядок и контринформация;

2) установление категорий бенефициаров, которые, приоритетным образом, должны быть включены в новые программы обучения человеческих ресурсов в указанной области;

3) разработка новых программ по подготовке кадров в данной области;

4) разработка и внедрение учебных программ для сотрудников с полномочиями по расследованию и уголовному преследованию, прокуроров, судей, специалистов и судебных экспертов в данной области в правоприменительных структурах, а также для технического персонала государственных учреждений.

100. Задача № 2. Согласование деятельности органов публичного управления, публичных и частных учреждений, выполняющих задачи обеспечения информационной безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) установление нормативной базы, регламентирующей полномочия органов публичного управления, публичных и частных учреждений относительно обеспечения информационной безопасности и ее корректировки, исключая пропуски и дублирование компетенций;

2) точное регламентирование в законодательстве полномочия по согласованию деятельности органов публичной власти, публичных и частных учреждений в части относительно исполнения полномочий по обеспечению информационной безопасности, а также механизма ее реализации назначенным органом публичной власти;

3) разработка и заключение соглашений о многостороннем межведомственном сотрудничестве, устанавливающих порядок согласование деятельности в части относительно исполнения полномочий по обеспечению информационной безопасности.

101. Задача № 3. Обеспечение международного сотрудничества в области информационной безопасности

Данная задача будет выполнена путем осуществления следующих действий:

1) оценка нынешнего уровня сотрудничества Республики Молдова с международными организациями, осуществляющими свою деятельность в области обеспечения информационной безопасности, и разработка действий по усилению соответствующего сотрудничества;

2) установление сотрудничества с государствами-партнерами, в частности, из Европейского Союза, относительно обмена информацией,

опытом и анализа в целях предупреждения, обнаружения и пресечения гибридных угроз безопасности в информационном пространстве;

3) продвижение на международном плане, в двустороннем режиме, необходимости заключения международных договоров, которые бы объединили понятие «информационное оружие», запрещая его разработку, распространение и применение в отношениях между государствами;

4) согласование и внедрение существующих международных инструментов, обеспечивающих предупреждение, выявление и противодействие несанкционированному доступу к информации ограниченного доступа из банковских электронных сетей коммуникации и из систем электронной торговли, к информации международных правовых органов.

102. Задача № 4. Развитие национального и международного сотрудничества в области кибероборонь

Данная задача будет выполнена путем осуществления следующих действий:

1) создание/внедрение режима институционального сотрудничества в области кибероборонь;

2) укрепление сотрудничества с внешними партнерами по развитию относительно обмена информацией и опытом в области киберзащиты;

3) подписание соглашений о сотрудничестве (взаимопомощи) в области кибероборонь.

103. Задача № 5. Укрепление международного сотрудничества в области предотвращения информационной преступности

Данная задача будет выполнена путем осуществления следующих действий:

1) укрепление механизмов международного сотрудничества между государственными органами с полномочиями по борьбе с преступностью в области компьютерной информации и специализированной международной службой EMAS (Europol Malware Analysis Service) ЕВРОПОЛА;

2) использование на национальном уровне инструментов и методов идентификации жертв, в том числе путем использования Информационной системы «Защита детей» и базы данных «Сексуальное насилие в отношении детей» Международной организации уголовной полиции ИНТЕРПОЛА;

3) сотрудничество в рамках национальных контактных пунктов 24/7 на основании Конвенции Совета Европы об информационной преступности (Будапешт, 2001 г.) и 24/7 G7;

4) развитие существующих партнерств NCMEC (Национальный центр США для пропавших и эксплуатируемых детей) и присоединение к другим подобным инициативам;

5) развитие партнерств в целях установления, блокировки, наложения ареста и конфискации продуктов и инструментов трансграничных преступлений;

6) участие в международных событиях в области предупреждения и борьбы с информационной преступностью в целях формирования специализированного персонала.

Приоритеты раздела IV	**Показатели результативности**
1. Развитие и внедрение учебных программ для сотрудников с полномочиями по расследованию и уголовному преследованию в информационном пространстве	1. Специалисты, обученные на основе практик ЕС
2. Развитие национального и международного сотрудничества в области киберзащиты	2. Правовая база сотрудничества обсуждена и заключена
3. Установление механизмов международного сотрудничества между органами государства с полномочиями по борьбе с преступностью в области компьютерной информации и международными органами в части обеспечения информационной безопасности	3. Ряд консультаций; двусторонние/многосторонние соглашения подписаны и заключены

V. ОЦЕНКА РЕЗУЛЬТАТОВ И СТОИМОСТИ ВНЕДРЕНИЯ СТРАТЕГИИ

104. Качественное внедрение положений Стратегии повысит степень защиты и безопасности в информационном пространстве.

105. Результаты реализации проявляются в:

1) обеспечении конституционных прав и свобод граждан при обработке информации;

2) защите и развитии партиципативной и плюралистической демократии;

3) развитие национального информационного общества во всех формах структуры и функционирования, индивидуального, публичного, частного или государственного характера;

4) обеспечение эффективного предотвращения и расследования преступлений в области компьютерной информации;

5) защита от деструктивного информационного и психологического воздействия;

6) защита общества от деструктивной дезинформации с целью подстрекательства к национальной и религиозной ненависти, смены конституционного строя;

7) развитие механизмов коллективной борьбы с гибридными угрозами безопасности, влияющими на информационную безопасность и общую среду безопасности;

8) обеспечение защиты предприятий, учреждений и организаций при доступе к правильной и объективной информации;

9) обеспечение свободного оборота информации, мультимедийного плюрализма и информационных онлайн- и оффлайн-платформ, за исключением предусмотренных законом случаев;

10) развитие и защита национальной информационной инфраструктуры;

11) укрепление принципов информирования диаспоры о ситуации в Республике Молдова;

12) надежное функционирование и развитие национального информационного пространства, его интеграция в европейское и мировое информационное пространство;

13) развитие системы стратегической коммуникации Республики Молдова;

14) эффективное взаимодействие органов публичной власти и гражданского общества в процессе формирования и внедрения государственной политики в области информации;

15) обеспечение развития информационно-коммуникационных технологий и информационных ресурсов Республики Молдова;

16) защита информации ограниченного доступа и иной информации, требования по защите которой установлены законом;

17) возложение обязанности на контролеров персональных данных за порядок обработки персональных данных;

18) защита персональных данных, а также лиц, особенно детей, в онлайн-среде;

19) определение правового статуса субъектов медийного онлайн-пространства (информационного в Интернете).

106. Для достижения вышеизложенных результатов необходимо, в первую очередь, повышение ответственности органов публичного управления, учреждений, государственных предприятий вне зависимости от их организационной формы и осуществление их деятельности в едином направлении.

107. Настоящая стратегия предусматривает выделение финансовых средств для всего периода ее внедрения.

108. Финансирование Стратегии осуществляется из государственного бюджета (общие ресурсы, накопленные доходы и ресурсы проектов, финансируемых из внешних источников) и из иных источников согласно законодательству.

109. Будут использованы возможности поддержки и поощрения деятельности в области информационных технологий, предоставляемые международными и региональными организациями.

110. Характер настоящей Стратегии обуславливает возникновение рисков разглашения данных, классифицированных сквозь призму оценки финансовых средств, выделяемых для выполнения определенных ключевых задач и мероприятий из Плана действий, что требует определения в индивидуальном порядке сумм, необходимых на уровне органов, и их отдельного указания для каждого бюджетного года.

111. В целях обеспечения защиты данных с точки зрения разработки нормативных актов, политик и планирования мероприятий, в том числе выделяемых финансовых средств, органы/учреждения в индивидуальном порядке оценят и примут решение об отображении данных, квалифицируемых как отнесенная к государственной тайне информация.

VI. ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ И ПОКАЗАТЕЛИ ПРОГРЕССА

112. Внедрение настоящей Стратегии способствует идентификации инновационных подходов к созданию системы по защите и развитию информационного пространства в условиях глобализации и свободного оборота информации, а именно:

1) будут разработаны специальные технические решения для повышения надежности коммуникационных сетей в критических ситуациях;

2) будут созданы архивы и фонды электронных документов в целях безопасного хранения баз данных национального значения в соответствии с установленным законодательством режимом накопления, хранения и учета;

3) будут укреплены механизмы защиты персональных данных во избежание их использования в незаконных целях;

4) будет развит национальный потенциал для осуществления безопасного обмена и накопления информации, быстрой и эффективной передачи потока информации, в том числе классифицированной на внутреннем и внешнем уровне, в случае различных кризисов или чрезвычайных ситуаций;

5) будет создан механизм расширения участия гражданского общества в приоритетных областях обеспечения информационной безопасности;

6) будут разработаны эффективные механизмы мониторинга, контроля и внедрения с целью сокращения существующих разногласий и провокаций, защиты общества от возможных попыток дезинформации и/или манипулятивной подачи информации извне;

7) будут установлены специфические гарантии для наиболее эффективной защиты персональных данных, личной, семейной и частной жизни лиц, в частности, в онлайн-среде;

8) будут обеспечены меры по предупреждению и борьбе с преступностью в области компьютерной информации.

113. Центральным элементом настоящей Стратегии является создание Координационного совета по обеспечению информационной безопасности, коллективного органа с консультативными и операционными полномочиями, который будет нести ответственность и обеспечивать системную целостность компонентов информационного пространства и оказывать поддержку, направленную на высокий уровень информационной безопасности.

1) В соответствии с условиями настоящей Стратегии предлагается, чтобы Координационный совет по обеспечению информационной безопасности состоял из следующих 4 основных секторов:

a) *Кибернетический сектор*, включающий в себя представителей Национального центра реагирования на инциденты кибербезопасности, Правительственного центра реагирования на инциденты кибербезопасности и частного центра реагирования на инциденты кибербезопасности, а также экспертов отделов кибербезопасности иных учреждений публичного и частного права, осуществляющих свою деятельность в сфере информационных технологий, которые могут содействовать обеспечению информационной безопасности Республики Молдова;

b) *Медийный сектор*, включающий в себя представителей национального медийного пространства, в частности, традиционных средств массовой информации (радиоканалы, телеканалы и печать), а также средств массовой информации из Интернета, включенных в зависимости от характера издательской политики, которые будут заниматься процессами, связанными с обеспечением безопасности медийного пространства;

c) *Операционный сектор* будет создан, в частности, из представителей органов публичной власти с полномочиями и компетенциями в области защиты, информации, контринформации, расследования и процессуальной деятельности согласно прерогативам обеспечения безопасности информационного пространства;

d) *Частно-общественный сектор* будет состоять из представителей гражданского общества согласно рекомендациям Совета гражданского общества, объединений, представляющих национальную сферу информационных технологий, компаний частного права из области информационных технологий, а также из международных экспертов из числа нынешних и будущих стратегических партнеров Республики Молдова, специализирующихся в области повышения кибернетической и информационной безопасности на региональном, европейском и международном уровнях;

2) Координационный совет по обеспечению информационной безопасности будет осуществлять свою деятельность на основании устава, который будет разработан вследствие принятия настоящей Стратегии, в его основную структуру будут входить вышеуказанные компоненты с возможностью внесения изменений для улучшения;

3) Порядок назначения органов управления на уровне Координационного совета по обеспечению информационной безопасности будет предусмотрен в уставе и будет основываться на принципе последовательной ротации;

4) Вышеуказанные секторы будут осуществлять свою деятельность несколькими способами: отдельно, совместно, путем привлечения экспертов из других секторов или интегрировано на уровне всего Координационного совета по обеспечению информационной безопасности, с назначением органа управления из числа компонентов с приоритетными полномочиями и компетенциями, исходя из рассматриваемой проблематики;

5) Приоритетной деятельностью Совета будет рассмотрение инцидентов информационной безопасности, решение которых требует интегрированного подхода, с фокусированием на оперативность при рассмотрении дел, определении мер раннего реагирования, предупреждения, противодействия или устранения последствий.

6) Служба информации и безопасности Республики Молдова выступит в качестве координатора деятельности Координационного совета по обеспечению информационной безопасности, будучи ответственной за получение уведомлений об инцидентах информационной безопасности и их представление руководителям секторов.

VII. ПРОЦЕДУРЫ МОНИТОРИНГА И ОЦЕНКИ

114. Мониторинг Стратегии имеет целью:

1) наблюдение за порядком внедрения Стратегии, степенью выполнения поставленных задач и мер, а также за необходимостью ее изменения в зависимости от эволюции определенных внутренних или внешних факторов;

2) обеспечение прозрачности и распространение информации о проведенных мероприятиях и полученных результатах.

115. Процесс внедрения Стратегии сопровождается постоянным мониторингом выполнения намеченных действий и полученных результатов, с внесением, в случае необходимости, соответствующих изменений в продвигаемые Правительством публичные политики в отношении данной Стратегии.

116. Мониторинг и координирование процесса реализации настоящей Стратегии и Плана действий по ее внедрению возлагается на Службу информации и безопасности Республики Молдова.

117. Министерства, учреждения и прочие органы центрального управления обеспечат, в пределах возложенных компетенций, проведение необходимых мероприятий в целях полного и своевременного выполнения действий, включенных в План действий по выполнению настоящей Стратегии.

Приложение № 2

ПЛАН ДЕЙСТВИЙ
по внедрению Стратегии информационной безопасности Республики Молдова на 2019-2024 годы

№ п/п	Задачи	Наименование действий	Ответственные учреждения	Партнеры	Источники финансирования/ стоимость	Срок выполнения	Показатели достижения
1.	2.	3.	4.	5.	6.	7.	8.
РАЗДЕЛ I. Обеспечение безопасности информационно-кибернетического пространства и расследование преступлений в области компьютерной информации							
1.	Создание интегрированной системы сообщения и оценки угроз информационной безопасности и разработки оперативных мер противодействия	1) создание/назначение учреждения, которое будет выполнять роль Национального центра реагирования на инциденты кибербезопасности и представлять собой единую точку отчетности по инцидентам кибербезопасности для компетентных органов публичной власти и физических и юридических лиц: a) разработка и продвижение нормативной базы; b) создание Национального центра реагирования ан инциденты кибербезопасности	Служба информационных технологий и кибернетической безопасности; Государственная канцелярия; Министерство финансов, Министерство экономики и инфраструктуры	Служба информации и безопасности; Национальное агентство по регулированию в области электронных коммуникаций и информационных технологий; Министерство внутренних дел; Министерство обороны; Генеральная прокуратура; Национальный центр по защите персональных данных; Агентство электронного управления; Государственное агентство по интеллектуальной	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2019-2021 гг.	Нормативная база разработана и утверждена; Национальный центр реагирования создан

1.	2.	3.	4.	5.	6.	7.	8.
				собственности; поставщики коммуникационных услуг			
		2) назначение учреждения, которое будет выполнять роль Правительственного центра реагирования на инциденты кибербезопасности и представлять собой точку отчетности по инцидентам кибербезопасности Правительства и установление его взаимодействия с Национальным центром реагирования на инциденты кибербезопасности	Служба информационных технологий и кибернетической безопасности; Государственная канцелярия	Национальный центр по защите персональных данных; Министерство экономики и инфраструктуры; Служба информации и безопасности; Министерство внутренних дел; Генеральная прокуратура	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2019-2020 гг.	Нормативная база утверждена (акт о назначении)
		3) установление Национальным центром реагирования на инциденты кибербезопасности показателей в области кибербезопасности: а) систематизация, анализ и оценка статистических данных в сфере кибербезопасности	Служба информационных технологий и кибернетической безопасности	Служба информации и безопасности; Министерство внутренних дел; Министерство обороны; Генеральная прокуратура; Национальный центр по защите персональных данных	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2023 гг.	Нормативные акты разработаны и утверждены; продукт анализа относительно состояния в сфере национальной кибербезопасности
		4) разработка механизмов создания и	Служба информационных	Служба информации и	Бюджет учреждений, в	2021-2023 гг.	Механизмы установлены и

1.	2.	3.	4.	5.	6.	7.	8.
		укрепления внутриведомственных центров реагирования на инциденты кибернетической и информационной безопасности как публичного, так и частного права	технологий и кибернетической безопасности	безопасности; Министерство обороны; Министерство внутренних дел; Генеральная прокуратура; Национальный центр по защите персональных данных	пределах утвержденных ассигнований; внешняя помощь		утверждены
		5) разработка нормативной базы для обеспечения высокого уровня безопасности информационных сетей и систем на национальном уровне на основе лучших практик ЕС	Министерство экономики и инфраструктуры	Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Нормативная база утверждена
		6) установление политики относительно порядка отчетности, хранения и обработки информации по инцидентам и угрозам информационной безопасности	Служба информационных технологий и кибернетической безопасности	Служба информации и безопасности; Генеральная прокуратура	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2022 гг.	Нормативная база утверждена
2.	Постоянный мониторинг и обеспечение высокого уровня кибербезопасности	1) установление и устранение источников угроз безопасности лиц, общества и государства в киберпространстве; а) проведение аудита кибербезопасности инфраструктур информационных технологий и Системы телекоммуникаций органов	Агентство электронного управления; Служба информационных технологий и кибернетической безопасности	Служба информации и безопасности; Агентство государственных услуг; Министерство экономики и инфраструктуры; Министерство внутренних дел;	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Отчет аудита состояния кибербезопасности разработан; отчет о внедрении предложений аудита выполнен

1.	2.	3.	4.	5.	6.	7.	8.
		местного публичного управления, а также других кибернетических инфраструктур национального интереса, в целях установления нарушений и уязвимостей, и предоставление решений/рекомендаций по их устранению; b) внедрение результатов аудита кибезбезопасности		Генеральная прокуратура			
		2) обеспечение применения Минимальных требований кибербезопасности II уровня в рамках предоставления публичных электронных услуг	Агентство электронного управления	Органы публичного управления	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Отчет о порядке применения Минимальных требований безопасности
		3) разработка механизмов и методов по предупреждению и пресечению угроз в киберпространстве, вызванных информационными услугами, оказываемыми физическими и юридическими лицами	Служба информации и безопасности	Министерство экономики и инфраструктуры; Служба информационных технологий и кибернетической безопасности; Министерство внутренних дел; Национальный центр по защите персональных данных	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Механизмы разработаны
		4) установление законного механизма взаимодействия между	Служба информации и безопасности; Министерство	Служба информационных технологий и	Бюджет учреждений, в пределах	2020-2022 гг.	Нормативная база разработана и утверждена

1.	2.	3.	4.	5.	6.	7.	8.
		компетентными органами публичной власти и физическими и юридическими лицами, независимо от типа собственности, в целях предоставления ими доступа к исходному коду приложений, разработанных, реализованных и распределенных для органов публичной власти	внутренних дел	кибернетической безопасности; Министерство экономики и инфраструктуры	утвержденных ассигнований; внешняя помощь		
		5) согласование с Национальным центром по защите персональных данных мер по защите персональных данных, обеспечивающих применение принципа защиты данных, начиная с момента понимания и подразумеваемой защиты данных, когда разрабатываются, планируются, отбираются и используются приложения, услуги и продукты, основывающиеся на обработке персональных данных, или которые обрабатывают персональные данные в соответствии с законодательством о защите персональных данных	Органы публичного управления	Национальный центр по защите персональных данных	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Нормативная база изменена и дополнена

1.	2.	3.	4.	5.	6.	7.	8.
3.	Укрепление потенциала по киберзащите	1) разграничение и распределение ролей и ответственности относительно киберзащиты системы органов безопасности государства и национальной системы защиты	Министерство обороны; Служба информации и безопасности	Министерство внутренних дел; Генеральная прокуратура	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Нормативная база изменена и дополнена
		2) разработка мер по киберзащите для защиты национальной критической инфраструктуры, а также в рамках других приоритетных отраслей государства	Служба информации и безопасности; Министерство обороны	Министерство внутренних дел; Генеральная прокуратура; Министерство экономики и инфраструктуры; Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2023 гг.	Меры кибернетической защиты для защиты национальной критической инфраструктуры разработаны и утверждены
		3) разработка и внедрение мер по защите информационных систем, обрабатывающих информацию, относящуюся к государственной тайне, и компонента ИТС системы национальной обороны	Служба информации и безопасности	Министерство обороны; Министерство внутренних дел; Генеральная прокуратура; Министерство экономики и инфраструктуры; Служба информационных технологий и кибернетической безопасности; Национальный центр по защите	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2022 г.	Меры защиты информационных систем, обрабатывающих информацию, относящуюся к государственной тайне, разработаны и утверждены

1.	2.	3.	4.	5.	6.	7.	8.
				персональных данных			
4.	Защита сетей специальной связи Республики Молдова и информации ограниченного доступа с целью поддержания жизненно важных функций государства	1) развитие механизмов защиты специальных систем электронных коммуникаций посредством применения средств криптографической и технической защиты информации	Служба информации и безопасности	Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Механизмы внедрены
		2) осуществление контроля над специальными системами электронных коммуникаций и сообщение ответственному органу о технических и организационно-технических мерах, предпринятых для обеспечения кибербезопасности	Служба информации и безопасности	Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Количество выполненных проверок
		3) обновление нормативной базы в области специальных систем электронных коммуникаций	Служба информации и безопасности	Министерство внутренних дел (Служба информационных технологий)	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2023 гг.	Нормативная база изменена и дополнена
		4) разработка системы аттестации объектов информатизации на соответствие требованиям по обеспечению защиты информации при проведении работ, связанных с обработкой и	Служба информации и безопасности		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2024 г.	Система аттестации разработана и внедрена

1.	2.	3.	4.	5.	6.	7.	8.
		хранением информации ограниченного доступа, в особенности той, которая относится к государственной тайне					
		5) установление мер по обеспечению безопасности персональных данных в контексте обеспечения кибербезопасности	Национальный центр по защите персональных данных	Министерство внутренних дел; Служба информации и безопасности; Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Нормативная база изменена и дополнена
		6) продвижение нормативной базы относительно обучения подразделений, ответственных за защиту персональных данных в рамках органов публичного и частного права	Национальный центр по защите персональных данных	Органы публичного управления	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020 г.	Нормативная база продвинута
5.	Обеспечение контроля за импортом, сертификацией и применением средств защиты информации	1) сертификация средств технической и криптографической защиты информации	Служба информации и безопасности	Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований	Постоянно	Количество сертифицированных средств
		2) развитие систем мониторинга импорта средств защиты информации	Таможенная служба; Служба информации и безопасности	Министерство экономики и инфраструктуры	В пределах бюджета учреждений	2020-2023 гг.	Система разработана и внедрена
		3) согласование нормативной базы в сфере криптографической защиты информации с	Служба информации и безопасности	Министерство юстиции; Министерство иностранных дел и	В пределах бюджета учреждений	2021 г.	Нормативная база изменена и дополнена

1.	2.	3.	4.	5.	6.	7.	8.
		европейскими нормами		европейской интеграции; Министерство экономики и инфраструктуры			
		4) создание базы данных относительно средств технической и криптографической защиты информации	Служба информации и безопасности	Служба информационных технологий и кибернетической безопасности; Агентство электронного управления; Министерство экономики и инфраструктуры	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2022 гг.	База данных создана и дополнена
		5) осуществление контроля в области применения всех видов электронной подписи.	Служба информации и безопасности		Бюджет учреждений, в пределах утвержденных ассигнований;	Постоянно	Реестр дополнен
6.	Борьба с информационной преступностью (расследование информационных преступлений)	1) повышение потенциала (увеличение эффективности механизма) по борьбе с преступностью в области компьютерной информации	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура		Бюджет учреждений, в пределах утвержденных ассигнований	Постоянно	Количество обученного персонала
		2) предоставление методико-практической помощи территориальным подразделениям относительно расследования информационных преступлений	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура		Бюджет учреждений, в пределах утвержденных ассигнований	Постоянно	Количество обученного персонала из территориальных подразделений

1.	2.	3.	4.	5.	6.	7.	8.
		3) внедрение новых механизмов на уровне вовлеченных учреждений в борьбе с информационной преступностью (привлечение частных компаний и независимых экспертов, развитие лабораторий)	Генеральная прокуратура; Министерство внутренних дел (Генеральный инспекторат полиции)	Служба информации и безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Функциональные механизмы внедрены
		4) усовершенствование законодательной базы, регламентирующей оплату труда персоналу, специализирующемуся на борьбе с информационной преступностью и расследовании информационных преступлений	Министерство финансов; Министерство внутренних дел;	Министерство здравоохранения, труда и социальной защиты	Бюджет учреждений, в пределах утвержденных ассигнований	2020 г.	Законодательная база утверждена относительно увеличения на 30% чистой заработной платы
7.	Защита детей в онлайн-пространстве от любой формы насилия	1) борьба с феноменом детской порнографии в Интернете	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура	Министерство здравоохранения, труда и социальной защиты; Министерство образования, культуры и исследований; неправительственные организации; гражданское общество, масс-медиа	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Количество реализованных мер/расследованных случаев
		2) борьба с феноменом груминга и сексуального домогательства детей в Интернете	Министерство внутренних дел (Генеральный инспекторат	Министерство образования, культуры и исследований;	Бюджет учреждений, в пределах утвержденных	Постоянно	Количество реализованных мер/расследованных случаев

1.	2.	3.	4.	5.	6.	7.	8.
			полиции); Генеральная прокуратура	неправительственные организации; гражданское общество; Министерство здравоохранения, труда и социальной защиты; поставщики услуг	ассигнований; внешняя помощь		
		3) продвижение более безопасного Интернета для детей посредством онлайн-консультаций и поощрения информирования путем специальных информационных проектов	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура	Министерство образования, культуры и исследований; неправительственные организации; гражданское общество; Министерство здравоохранения, труда и социальной защиты	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Количество кампаний по информированию
8.	Борьба с мошенничеством посредством использования электронных средств оплаты	1) обмен информацией между Центром по борьбе с информационными преступлениями и департаментами безопасности финансовых учреждений	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура	Национальный банк Молдовы; финансовые учреждения	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Соглашение об обмене информацией
		2) продвижение мер повышенной безопасности в отношении МТО на уровне аппаратного и программного обеспечения	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура	Национальный банк Молдовы; финансовые учреждения	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Количество внедренных мер безопасности

1.	2.	3.	4.	5.	6.	7.	8.
		3) установление общих механизмов по борьбе с мошенничеством по операциям с и без присутствия карт	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура	Национальный банк Молдовы; финансовые учреждения	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Механизм установлен и внедрен
9.	Развитие институционального потенциала в борьбе с информационной преступностью	1) развитие специализированных подразделений в Генеральном инспекторате полиции Министерства внутренних дел, Генеральной прокуратуре, Службе информации и безопасности Республики Молдова с целью выявления и противодействия преступным попыткам в данной области	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура; Служба информации и безопасности		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Количество созданных/ специализированных подразделений
		2) создание национальной базы данных относительно развития феномена информационной преступности	Генеральная прокуратура; Служба информации и безопасности; Министерство внутренних дел	Национальный совет по борьбе с коррупцией; Таможенная служба; Национальный центр по защите персональных данных	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2022 г.	База данных создана

1.	2.	3.	4.	5.	6.	7.	8.
		3) корректировка деятельности, осуществляемой в области информационной преступности в Центральном банке данных автоматизированной информационной системы «Реестр криминалистической и криминологической информации»	Министерство внутренних дел (Служба информационных технологий)	Генеральная прокуратура; Служба информации и безопасности, Таможенная служба; Национальный совет по борьбе с коррупцией; Национальный центр по защите персональных данных	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Механизмы скорректированы/ внедрены
		4) разработка нормативной базы, регламентирующей создание Автоматизированной информационной системы «е-Судебное дело» в органах, вовлеченных в проведение уголовного преследования и судебного рассмотрения дела, а также ее внедрение, развитие и подключение	Генеральная прокуратура	Министерство внутренних дел; Служба информации и безопасности; Таможенная служба; Национальный совет по борьбе с коррупцией; Национальный центр по защите персональных данных	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2019-2021 гг.	Нормативная база разработана
10.	Осуществление научно-прикладных исследований в области информационной безопасности	1) планирование и развитие научно-исследовательской деятельности в области информационно-коммуникационных технологий	Министерство образования, культуры и исследований; Академия наук Молдовы; Национальное агентство по исследованиям и		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	План действий разработан и утвержден

1.	2.	3.	4.	5.	6.	7.	8.
			развитию				
		2) создание/укрепление лабораторий кибербезопасности в учреждениях высшего образования и научно-исследовательских учреждениях	Академия наук Молдовы	Служба информационных технологий и кибернетической безопасности; частный сектор	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2022-2024 гг.	Количество созданных и укрепленных лабораторий кибербезопасности
11.	Развитие информационной и кибернетической устойчивости и повышение уровня культуры в области ИТС	1) проведение действий по осведомлению и информированию общества относительно угроз, уязвимостей и рисков кибербезопасности	Служба информационных технологий и кибернетической безопасности	Агентство электронного управления; Служба информации и безопасности; Министерство образования, культуры и исследований; Министерство экономики и инфраструктуры	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Количество реализованных кампаний по информированию
		2) проведение Национальным центром реагирования на инциденты кибебезопасности стратегического анализа инцидентов кибебезопасности и согласование ответных действий на инциденты безопасности, в том числе посредством организации специальных курсов квалифицированными экспертами	Служба информационных технологий и кибернетической безопасности	Служба информации и безопасности; Агентство электронного управления; Национальный центр по защите персональных данных	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Отчет об инцидентах кибербезопасности разработан
		3) проведение общих занятий и тренировок по	Служба информационных	Министерство обороны;	Бюджет учреждений, в	2020-2024 гг.	Количество реализованных

1.	2.	3.	4.	5.	6.	7.	8.
		укреплению потенциала реагирования на кибератаки, в том числе по блокировке ложных кибератак	технологий и кибернетической безопасности	Агентство электронного управления; Министерство внутренних дел; Служба информации и безопасности; Генеральная прокуратура; Национальный центр по защите персональных данных	пределах утвержденных ассигнований; внешняя помощь		занятий
		4) организация и проведение рабочих семинаров в области кибербезопасности для персонала публичного и частного секторов, владельцев элементов критической инфраструктуры	Служба информационных технологий и кибернетической безопасности	Министерство обороны; Агентство электронного управления; Служба информации и безопасности; Министерство внутренних дел; Генеральная прокуратура; Национальный центр по защите персональных данных; частная среда, гражданское общество	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Количество организованных рабочих семинаров
		5) сертификация специалистов в области кибербезопасности специализированными организациями/компаниями, исходя из применяемых	Агентство электронного управления	Министерство экономики и инфраструктуры; Служба информационных технологий и	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Количество сертифицированных специалистов

1.	2.	3.	4.	5.	6.	7.	8.
		стандартов и утвержденных минимальных обязательных требований по кибербезопасности		кибернетической безопасности; органы публичного управления			
		6) создание веб-платформ по осведомлению и информированию относительно угроз в киберпространстве и мер защиты, которые могут быть приняты физическими и юридическими лицами	Служба информационных технологий и кибернетической безопасности	Агентство электронного управления; Министерство внутренних дел; Генеральная прокуратура; частный сектор	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2022 гг.	Платформы созданы
		7) введение и продвижение куррикулярного содержания об информационной безопасности в национальных учебных программах	Министерство образования, культуры и исследований	Служба информационных технологий и кибернетической безопасности; Агентство электронного управления; Служба информации и безопасности; Министерство внутренних дел; Генеральная прокуратура; Национальный центр по защите персональных данных; гражданское общество	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Количество учебных заведений, в которых включены куррикулярные содержания

1.	2.	3.	4.	5.	6.	7.	8.
		8) организация, в том числе совместно с иностранными партнерами, тематических учебных курсов в области кибербезопасности для работников государственных учреждений	Агентство электронного управления	Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Количество реализованных учебных курсов
РАЗДЕЛ II: Обеспечение безопасности информационно-медийного пространства							
12.	Развитие механизмов стратегической коммуникации для реализации национальных интересов Республики Молдова	1) определение уязвимых секторов медийного компонента системы информационной безопасности	Органы публичного управления		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Отчет об оценке уязвимых секторов стратегической коммуникации
		2) развитие политик стратегической коммуникации на внутреннем плане и подключение к внешним платформам стратегической коммуникации структур системы безопасности, обороны и общественного порядка для обеспечения информационной безопасности и продвижения национальных интересов Республики Молдова	Координационный совет по телевидению и радио	Органы публичного управления; гражданское общество; организации массовой информации	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Соглашения разработаны и утверждены
		3) создание в Республике Молдова информационного ресурса/платформы стратегической	Служба информации и безопасности	Гражданское общество; организации массовой информации	Бюджет учреждений, в пределах утвержденных ассигнований;	2021-2024 гг.	Информационный ресурс/платформа создан и представлен

1.	2.	3.	4.	5.	6.	7.	8.
		коммуникации, содержащей информацию: a) об инцидентах информационной безопасности; b) руководствах стратегической коммуникации по субъектам национального интереса; c) попытках и действиях дезинформации и/или манипулятивной подачи информации, затрагивающих информационной безопасности и общее состояние безопасности			внешняя помощь		
13.	Гражданский контроль и укрепление сотрудничества гражданского общества с органами публичной власти с функциями обеспечения информационной безопасности	1) создание механизма привлечения экспертов из гражданского общества, неправительственных организаций и средств массовой информации в области информационной безопасности путем: a) назначения существующего Совета или создание коллективного органа из рядов гражданского общества с полномочиями по оценке экспертов, неправительственных организаций и средств массовой информации с точки зрения их	Гражданское общество; организации массовой информации	Государственные органы системы безопасности и обороны	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	

1.	2.	3.	4.	5.	6.	7.	8.
		привлечения в процесс обеспечения информационной и национальной безопасности; b) сертификация Советом гражданского общества экспертов и представителей гражданского общества и средств массовой информации, осуществляющих мониторинг степени обеспечения информационной безопасности на национальном уровне					
		2) привлечение представителей гражданского общества, сертифицированных Советом гражданского общества, в состав Координационного совета по обеспечению информационной безопасности	Гражданское общество; организации массовой информации	Государственные органы системы безопасности и обороны	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Период внедрения Стратегии	
		3) улучшение или создание механизмов привлечения гражданского общества к процессам определения, разработки,	Гражданское общество, Организации массовой информации	Государственные органы системы безопасности и обороны	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Период внедрения Стратегии	

1.	2.	3.	4.	5.	6.	7.	8.
		мониторинга и оценки политик обеспечения информационной безопасности, проводимых компетентными в области обеспечения информационной безопасности органами;					
		4) разработка и организация тематических учебных курсов для радиовещателей, распространителей программ, субъектов, формирующих общественное мнение, журналистов и профильных неправительственных организаций о техниках дезинформации и/или манипулятивной подачи информации, используемых для причинения вреда информационной безопасности государства.	Гражданское общество, Организации массовой информации	Государственные органы системы безопасности и обороны	Бюджет учреждений, в пределах утвержденных ассигнований; Внешняя помощь	Период внедрения Стратегии	
14.	Определение правового статуса периодических	1) оценка Интернет-пространства с перспективы установления	Служба информации и безопасности, Министерство	Гражданское общество; организации	Бюджет учреждений, в пределах	2020-2024 гг.	Отчет/исследование реализованы

1.	2.	3.	4.	5.	6.	7.	8.
	изданий, агентств печати и иных субъектов, осуществляющих свою деятельность в медийном пространстве Интернета	субъектов, вовлеченных в производство и распространение медиасодержания онлайн, и других посредников и дополнительных услуг, оказывающих отрицательное влияние на информационную безопасность	внутренних дел; Служба информационных технологий и кибернетической безопасности; органы публичного управления	массовой информации	утвержденных ассигнований; внешняя помощь		
		2)разработка и корректировка функциональной законодательной базы в целях правового регламентирования отношений между субъектами средств массовой информации, собирающими и распространяющими информацию в Интернете, обществом и уполномоченными органами с функциями в области обеспечения информационной безопасности, в соответствии с рекомендациями Европейской комиссии и надлежащими европейскими практиками	Служба информации и безопасности; Министерство юстиции; Координационный совет по телевидению и радио; органы публичного управления	Гражданское общество; организации массовой информации	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Нормативная база разработана и утверждена
		3) внедрение нормативной базы, установленной общими	Органы публичного управления; гражданское	Частная среда	Бюджет учреждений, в пределах	2021-2024 гг.	Отчет о степени внедрения нормативной базы

1.	2.	3.	4.	5.	6.	7.	8.
		действиями по вмешательству и управлению медиапространством онлайн и офлайн	общество		утвержденных ассигнований; внешняя помощь		утвержден
15.	Обеспечение финансовой прозрачности в деятельности органов публичной власти, общественных объединений и коммерческих обществ в контексте обеспечения информационной безопасности	4) разработка под руководством Координационного совета по обеспечению информационной безопасности критериев квалификации информации как продукта дезинформации, манипуляции и пропаганды, направленных на подрыв информационной безопасности, с целью выявления заказчиков, источников финансирования и исполнителей	Служба информации и безопасности; Министерство юстиции; Национальный совет по борьбе с коррупцией; Координационный совет по телевидению и радио	Гражданское общество; организации массовой информации	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Критерии по квалификации разработаны
		5) корректировка законодательной базы в целях повышения эффективности сбора данных для установления происхождения финансовых средств и собственности субъектов, вовлеченных в деятельность по дезинформации, манипулированию и пропаганде, подрывающую	Служба информации и безопасности; Министерство юстиции; Национальный совет по борьбе с коррупцией; Координационный совет по телевидению и радио	Гражданское общество; организации массовой информации	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2019-2024 гг.	Нормативная база разработана и утверждена

1.	2.	3.	4.	5.	6.	7.	8.
		информационную безопасность					
		6) взаимодействие с правовыми учреждениями в сфере анализа рисков и угроз в области масс-медиа, в целях контроля развития обнаруженных угроз, исследования подрывной или уголовной деятельности в информационном пространстве,, установления источников финансирования факторов риска	Служба информации и безопасности	Служба информации и безопасности, Генеральная прокуратура; Министерство внутренних дел; Национальный совет по борьбе с коррупцией	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Механизм сотрудничества внедрен; нормативно-законодательная база разработана и утверждена
Раздел III: Укрепление операционных возможностей							
16.	Развитие механизмов предупреждения, выявления, смягчения и ответа на национальном уровне для обеспечения информационной безопасности	1) создание на национальном уровне подразделения, владеющего компетенциями по продвижению и согласованию политик информационной безопасности в демократическом обществе, в зависимости от развития технологии, правовых и другого характера отношений сектора информационного общества на национальном и международном уровне (Координационный совет	Служба информации и безопасности	Служба информационных технологий и кибернетической безопасности; органы публичного управления; гражданское общество, организации массовой информации; частный сектор	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2019-2021 гг.	Нормативный акт по созданию подразделения разработан и утвержден

1.	2.	3.	4.	5.	6.	7.	8.
		по обеспечению информационной безопасности): a) установление и интеграция существующих компонентов с функциями и полномочиями в кибернетической, медийной области и органы публичного управления и тех, которые будут созданы в процессе. b) установление сферы деятельности для каждого компонента, включенного в подразделение, в зависимости от выполняемых функций и полномочий из перспективы обеспечения информационной безопасности; c) разработка и утверждение нормативно-законодательной базы взаимодействия для реализации задач по обнаружению, предупреждению и пресечению рисков и угроз информационной безопасности					
		2) разработка, продвижение и согласование политик информационной безопасности согласно	Служба информации и безопасности	Служба информационных технологий и кибернетической безопасности;	Бюджет учреждений, в пределах утвержденных ассигнований;	2021-2024 гг.	Четкие механизмы международного взаимодействия разработаны и утверждены

1.	2.	3.	4.	5.	6.	7.	8.
		Концепции, настоящей Стратегии и другим документам политик на национальном и международном уровне относительно информационной безопасности		органы публичного управления; гражданское общество; организации массовой информации; частный сектор	внешняя помощь		
		3) информирование населения относительно способов предупреждения и пресечения рисков и угроз системным компонентам информационной безопасности, в том числе новых возникших феноменов на национальном уровне	Служба информации и безопасности	Органы публичного управления; гражданское общество; организации массовой информации	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Количество кампаний по информированию
17.	Развитие потенциала реагирования в случае гибридных угроз безопасности	1) создание специального аналитико-информационного компонента по гибридным угрозам безопасности в рамках Службы информации и безопасности	Служба информации и безопасности	Министерство иностранных дел и европейской интеграции; Министерство внутренних дел; Генеральная прокуратура; Министерство обороны	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Акт разработан и утвержден относительно аналитико-информационного компонента
		2) создание национальной сети органов, ответственных за борьбу с гибридными угрозами безопасности	Служба информации и безопасности		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Соглашение о создании национальной сети

1.	2.	3.	4.	5.	6.	7.	8.
		3) разработка операционных протоколов взаимодействия между ответственными органами и руководящими органами в случае некоторых гибридных угроз безопасности	Служба информации и безопасности	Органы публичного управления; гражданское общество; организации массовой информации; частный сектор	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Количество разработанных и подписанных протоколов
		4) укрепление степени познания и понимания концепции гибридных угроз безопасности на уровне органов, уполномоченных в области информационной безопасности и общей среды безопасности	Служба информации и безопасности	Органы публичного управления; гражданское общество; организации массовой информации; частный сектор	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Количество заключенных межведомственных протоколов
		5) проведение занятий для развития потенциала органов, специализирующихся на борьбе с гибридными угрозами безопасности	Служба информации и безопасности	Органы публичного управления; гражданское общество; организации массовой информации; частный сектор	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Количество занятий по проведению исследований и экспертиз
		6) ассоциация Республики Молдова к Европейскому центру совершенства в борьбе с гибридными угрозами и к Центру совершенства стратегической коммуникации НАТО	Служба информации и безопасности	Органы публичного управления; гражданское общество; организации массовой информации; частный сектор	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2022-2024 гг.	Нормативный акт (соглашение) разработан и завершен
18.	Развитие операционного потенциала по	1) создание подразделения, ответственного за	Министерство обороны	Служба информационных технологий и	Бюджет учреждений, в пределах	2021 г.	Подразделение создано

1.	2.	3.	4.	5.	6.	7.	8.
	кибероборонe	кибероборону на уровне Вооруженных сил		кибернетической безопасности; Служба информации и безопасности; Министерство внутренних дел	утвержденных ассигнований; внешняя помощь		
		2) укрепление потенциала по киберобразованию и обучению посредством участия в межгосударственных и международных занятиях по кибероборонe	Министерство обороны; Служба информации и безопасности	Министерство иностранных дел и европейской интеграции; Министерство внутренних дел (Служба информационных технологий)	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2019-2024 гг.	Количество обученного персонала; проведенные занятия
		3) установление, предупреждение и пресечение факторов риска с информативно-подрывным потенциалом киберзащиты Республики Молдова посредством внедрения интегрированного менеджмента виртуального пространства и развития системы по преждевременному предупреждению относительно элементов риска объектов инфраструктуры	Служба информации и безопасности	МО, Служба информационных технологий и кибернетической безопасности; Министерство экономики и инфраструктуры	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Отчет об установленных и/или наступивших рисках
19.	Мониторинг информационного пространства и	1) пересмотр существующей правовой базы в части установления	Министерство юстиции; Координационный	Служба информации и безопасности	Бюджет учреждений, в пределах	2020-2024 гг.	Нормативная база пересмотрена; сводки об

1.	2.	3.	4.	5.	6.	7.	8.
	выявление внутренних и внешних действий по дезинформации и/или манипулятивной подаче информации	и уравнивания понятий относительно дезинформации, ложных новостей и/или манипулятивной подачи информации, а также предупреждение ее распространения посредством медиаплатформ. Установление секторов национальной безопасности, нарушение которых (посредством дезинформации) создает высокие риски для функциональности государства	совет по телевидению и радио		утвержденных ассигнований; внешняя помощь		установленных секторов риска национальной безопасности
		2) установление полномочий (компетентных органов) для обнаружения и пресечения манипулятивных и дезинформационных сообщений из информационного пространства (Интернет)	Служба информации и безопасности	Академия наук Молдовы; организации гражданского общества, масс-медиа	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Законодательная база изменена
		3) установление некоторых фильтров по обнаружению и/или блокированию информационных ресурсов, содержащих элементы риска национальной безопасности, а также	Служба информации и безопасности	Академия наук Молдовы; организации гражданского общества; масс-медиа	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Законодательная база разработана и утверждена

1.	2.	3.	4.	5.	6.	7.	8.
		разработка, утверждение соответствующей нормативной базы					
20.	Повышение потенциала защиты национальных критичных инфраструктур	1) разработка и утверждение законной базы относительно установления и обозначения национальных критичных инфраструктур, в том числе относительно жизненно важных информационных систем	Служба информации и безопасности	Органы публичного управления	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2019-2021 гг.	Законодательная база разработана и утверждена
		2) оценка и информирование относительно состояния и уровня безопасности объектов инфраструктуры из перспективы обеспечения информационной безопасности	Служба информации и безопасности	Органы публичного управления	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2021-2024 гг.	Механизм оценки и отчетности реализован
21.	Развитие потенциала по предупреждению, обнаружению и пресечению экстремистских, террористических и иного рода действиям, ставящих под угрозу информационную	1) синхронизация и рациональное распределение сил учреждений Республики Молдова на предварительное выявление действий, совершаемых извне и/или внутри страны с целью сложных диверсий против	Служба информации и безопасности	Министерство внутренних дел; Генеральная прокуратура; Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2022 гг.	Механизмы межведомственного взаимодействия разработаны; систематический обмен информацией внедрен

1.	2.	3.	4.	5.	6.	7.	8.
	безопасность	информационной безопасности					
		2) предоставление Службе информации и безопасности информации о ситуации риска государственными учреждениями, компетентными в данной области	Органы публичного управления	Служба информации и безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Количество переданных/ полученных отчетов
Раздел IV: Повышение эффективности процесса внутреннего согласования и международного сотрудничества в области информационной безопасности							
22.	Развитие системы подготовки кадров в области информационной безопасности	1) оценка актуального уровня подготовки кадров в области информационной безопасности по каждому разделу в отдельности: средства массовой информации, информационные технологии, оборона, общественный порядок и контринформация	Органы публичного управления; Координационный совет по телевидению и радио; Министерство экономики и инфраструктуры; Министерство обороны; Министерство внутренних дел; Генеральная прокуратура; Служба информации и безопасности; неправительственные организации	Министерство образования, культуры и исследований	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Исследование проведено
		2) установление категорий бенефициаров, которые, приоритетным образом, должны быть	Органы публичного управления	Координационный совет по телевидению и радио;	Бюджет учреждений, в пределах утвержденных	2021 г.	Количество установленных и обученных бенефициаров

1.	2.	3.	4.	5.	6.	7.	8.
		включены в новые программы обучения человеческих ресурсов в указанной области		Министерство экономики и инфраструктуры; МО, Министерство внутренних дел; Генеральная прокуратура; Служба информации и безопасности; неправительственные организации из области масс-медиа	ассигнований; внешняя помощь		
		3) разработка новых программ по подготовке кадров в данной области	Министерство образования, культуры и исследований; Академия наук Молдовы	Координационный совет по телевидению и радио; Министерство экономики и инфраструктуры; Министерство обороны; Министерство внутренних дел; Генеральная прокуратура; Служба информации и безопасности; Национальный центр по защите персональных данных, неправительственные организации из области масс-медиа	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2022 г.	Количество разработанных программ

1.	2.	3.	4.	5.	6.	7.	8.
		4) разработка и внедрение учебных программ для сотрудников с полномочиями по расследованию и уголовному преследованию, прокуроров, судей, специалистов и судебных экспертов в данной области в правоприменительных структурах, а также для технического персонала государственных учреждений	Академия наук Молдовы; Национальный институт юстиции; Министерство внутренних дел – (Академия Штефан чел Маре)	Министерство образования, культуры и исследований; Координационный совет по телевидению и радио; Министерство экономики и инфраструктуры; Министерство обороны; Генеральная прокуратура; Служба информации и безопасности; Национальный центр по защите персональных данных; неправительственные организации неправительственные организации из области масс-медиа	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2022-2024 гг.	Количество разработанных программ
23.	Согласование деятельности органов публичного управления, публичных и частных учреждений, выполняющих задачи обеспечения информационной безопасности	1) установление нормативной базы, регламентирующей полномочия органов публичного управления, публичных и частных учреждений относительно обеспечения информационной безопасности и ее	Органы, указанные в Концепции, в пределах их компетенции		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020 г.	Нормативная база пересмотрена

1.	2.	3.	4.	5.	6.	7.	8.
		корректировки, исключая недочеты и дублирование компетенций					
		2) точное регламентирование в законодательстве полномочия по согласованию деятельности органов публичной власти, публичных и частных учреждений в части относительно исполнения полномочий по обеспечению информационной безопасности, а также механизма ее реализации назначенным органом публичной власти	Органы, указанные в Концепции, в пределах их компетенции		Бюджет учреждений, в пределах утвержденных ассигнований; Внешняя помощь	2020 г.	Нормативная база пересмотрена, деятельность ответственного учреждения регламентирована
		3) разработка и заключение соглашений о многостороннем межведомственном сотрудничестве, устанавливающих порядок согласование деятельности в части относительно исполнения полномочий по обеспечению информационной безопасности	Органы, указанные в Концепции, в пределах их компетенции		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2021 гг.	Количество заключенных соглашений о сотрудничестве
24.	Обеспечение международного сотрудничества в области	1) оценка актуального уровня сотрудничества Республики Молдова с международными	Органы публичного управления		Бюджет учреждений, в пределах утвержденных	2020-2021 гг.	Исследование по оценке разработано

1.	2.	3.	4.	5.	6.	7.	8.
	информационной безопасности	организациями, осуществляющими свою деятельность в области обеспечения информационной безопасности, и разработка действий по укреплению соответствующего сотрудничества			ассигнований; внешняя помощь		
		2) установление сотрудничества с государствами-партнерами, в особенности, из Европейского Союза, относительно обмена информацией, опытом и анализа в целях предупреждения, обнаружения и пресечения гибридных угроз безопасности в информационном пространстве	Органы публичного управления	Министерство иностранных дел и европейской интеграции	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Количество организованных консультаций
		3) продвижение на международном плане, в двустороннем режиме, необходимости заключения международных договоров, которые бы объединили понятие «информационное оружие», запрещая его разработку, распространение и	Органы публичного управления	Министерство иностранных дел и европейской интеграции	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Количество согласованных/ подписанных международных договоров

1.	2.	3.	4.	5.	6.	7.	8.
		применение в отношениях между государствами					
		4) согласование и внедрение существующих международных инструментов, обеспечивающих предупреждение, выявление и противодействие несанкционированному доступу к информации ограниченного доступа из банковских электронных сетей коммуникации и из систем электронной торговли, к информации международных правовых органов	Органы публичного управления	Министерство юстиции; Министерство иностранных дел и европейской интеграции	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Нормативно-законодательная база изменена и дополнена
25.	Развитие национального и международного сотрудничества в области кибероборонь	1) создание/внедрение режима институционального сотрудничества в области кибероборонь	Министерство обороны; Служба информации и безопасности; Министерство экономики и инфраструктуры; Служба информационных технологий и кибернетической безопасности; Генеральная прокуратура; Министерство	Органы публичного управления	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Количество организованных консультаций

1.	2.	3.	4.	5.	6.	7.	8.
			внутренних дел				
		2) укрепление сотрудничества с внешними партнерами по развитию относительно обмена информацией и опытом в области киберзащиты	Министерство обороны	Министерство иностранных дел и европейской интеграции; Служба информации и безопасности; Министерство экономики и инфраструктуры; Служба информационных технологий и кибернетической безопасности	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Количество согласованных/ подписанных соглашений
		3) подписание соглашений о сотрудничестве (взаимопомощи) в области кибероборонь	Министерство обороны; Служба информации и безопасности	Национальный центр реагирования на инциденты кибербезопасности; Министерство иностранных дел и европейской интеграции	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	2020-2024 гг.	Количество согласованных/ подписанных соглашений
26.	Укрепление международного сотрудничества в области предотвращения информационной преступности	1) укрепление механизмов международного сотрудничества между государственными органами с полномочиями по борьбе с преступностью в области компьютерной информации и специализированной	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура	Министерство иностранных дел и европейской интеграции	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Установленные/ укрепленные механизмы

1.	2.	3.	4.	5.	6.	7.	8.
		международной службой EMAS (Europol Malware Analysis Service) ЕВРОПОЛА					
		2) использование на национальном уровне инструментов и методов идентификации жертв, в том числе путем использования Информационной системы «Защита детей» и базы данных «Сексуальное насилие в отношении детей» Международной организации уголовной полиции ИНТЕРПОЛА	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Инструменты и методы установлены и использованы
		3) сотрудничество в рамках национальных конатктных пунктов 24/7 на основании Конвенции Совета Европы об информационной преступности (Будапешт 2001 г.) и 24/7 G7	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура	Министерство иностранных дел и европейской интеграции	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Акт о сотрудничестве установлен
		4) развитие существующих партнерств NCMEC (Национальный центр США для пропавших и эксплуатируемых детей) и присоединение к другим подобным инициативам	Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура	Министерство иностранных дел и европейской интеграции	Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	По необходимости	Количество установленных соглашений и партнерств
		5) развитие партнерств в целях установления; блокировки, наложения	Генеральная прокуратура; Министерство	Министерство иностранных дел и европейской	Бюджет учреждений, в пределах	2021 г.	Механизм установлен и внедрен

1.	2.	3.	4.	5.	6.	7.	8.
		ареста и конфискации продуктов и инструментов трансграничных преступлений	внутренних дел; Служба информации и безопасности	интеграции	утвержденных ассигнований; внешняя помощь		
		б) участие в международных событиях в области предупреждения и борьбы с информационной преступностью в целях формирования специализированного персонала	Министерство иностранных дел и европейской интеграции; Министерство внутренних дел (Генеральный инспекторат полиции); Генеральная прокуратура; Служба информации и безопасности		Бюджет учреждений, в пределах утвержденных ассигнований; внешняя помощь	Постоянно	Количество посещенных событий; обученные эксперты

Пояснительная записка
к проекту Стратегии информационной безопасности Республики Молдова на 2019-2024 годы и Плану действий по ее внедрению

I. Автор проекта и причины, обусловившие его разработку

Закон № 299 от 21.12.2017 года об утверждении Концепции информационной безопасности Республики Молдова устанавливает в статье 3, что в шестимесячный срок со дня вступления в силу должна быть разработана и представлена на рассмотрение Стратегия информационной безопасности Республики Молдова и План действий по ее внедрению.

В этом контексте в целях реализации действий, установленных Законом № 299/2017, была создана Межведомственная рабочая группа, состоящая из 12 органов/учреждений. Задача созыва рабочей группы была возложена на Службу информации и безопасности Республики Молдова.

Осознавая значимость, сложность и первостепенную задачу, предложенную документов политик, Рабочая группа, созванная на несколько заседаний, разработала – проекты Стратегии информационной безопасности Республики Молдова на 2019-2024 годы (*в дальнейшем – Стратегия*) и Плана действий по ее внедрению (*в дальнейшем – План*).

Принимая во внимание положения Концепции информационной безопасности, Рабочей группой было принято решение по разработке проекта Стратегии на пятилетний период, 2019-2024 гг.

Цель Стратегии состоит в ***правовом взаимодействии и системной интеграции приоритетных областей с ответственностью и компетенциями по обеспечению информационной безопасности на национальном уровне, основанная на кибернетической устойчивости, мультимедийном плюрализме и институциональном сближении в сфере безопасности, предназначенных для защиты суверенности, независимости и территориальной целостности Республики Молдова.***

Также, Закон № 299/2017 предусматривает в статье 2 разработку Программы мер по внедрению Концепции информационной безопасности, а Стратегия 2018-2023 гг. является неотъемлемой частью данного документа. В качестве определяющего процесса Программа предусматривает действия по отчетности, гармонизации и повышению эффективности документа, а в период 2019-2024 гг. будет проведена полная оценка степени реализации цели, мер и действий, предложенных Стратегией.

Стратегия состоит из **7 Глав** и **117 пунктов**.

Глава I – Введение

Описывает текущее развитие информационных технологий и систем электронной коммуникации на мировом, европейском и национальном уровнях и устанавливает путь Республики Молдова в части развития и реализации программ и политик развития в информационном пространстве, раскрывает неоспоримую пользу современных технологий, а

также выявляет основные уязвимые места, риски и угрозы информационному обществу и национальной и общей среде безопасности.

Глава II – Описание Ситуации

Вторая глава содержит подробное описание пути Республики Молдова в части развития информационного общества, национальных и международных актов, принятых по настоящее время, регламентирующих совокупность правовых отношений между субъектами, объектом и взаимодействием информационного пространства.

При описании ситуации были указаны основные документы политик, регламентирующие области информационного общества, существующие на момент разработки настоящей Стратегии, касающиеся масштаба информационной безопасности, в особенности: *Национальная стратегия развития информационного общества «Цифровая Молдова 2020», утвержденная Постановлением Правительства № 857 от 31.10.2013 года и Национальная программа кибербезопасности Республики Молдова на 2016-2020 годы, утвержденная Постановлением Правительства № 811 от 29.10.2015 года.*

При описании ситуации ссылались на первостепенную значимость утверждения Стратегии, которая обусловлена необходимостью защиты интересов населения, общества, государства в информационном пространстве, серьезностью и многочисленными угрозами информационной безопасности в современном обществе, необходимостью поддержания равновесия между интересами населения, общества и государства для обеспечения информационной безопасности.

Также, применимое в настоящее время законодательство не регламентирует и, соответственно, не обеспечивает в достаточной мере такие требования как попытки дезинформации и/или манипулятивной подачи информации, охрана частной жизни и персональных данных при размещении информации в Интернете, так как действие этих законов ограничено и/или они преследуют другую цель, нежели регламентирование.

Таким образом, сохранение равновесия между основными компонентами в правовом государстве может быть достигнуто только при условии существования и функционирования законодательно-нормативной базы в области, инструментов и четких методов, механизмов системного взаимодействия на национальном уровне и эффективного сотрудничества на международном уровне.

Глава III – Определение Проблем

Делая полный синтез проекта Стратегии, выделяем прямое подкрепление главы III и главы IV, а именно в части относительно описания реальных проблем Республики Молдова в сфере обеспечения безопасности информационного пространства и предложения решений по улучшению (*путем конкретных задач и мер*). В этом смысле, указанная цель Стратегии по правовому взаимодействию и систематической интеграции состоит в следующем:

1) Одной из первостепенных проблем является отсутствие интегрированной системы менеджмента кибербезопасности, типа CERT (Центр реагирования на инциденты кибербезопасности), в рамках которой осуществляется согласование, планирование и использование доступных ресурсов, установление уязвимых мест и рисков вследствие аудита кибербезопасности. Соответственно, предложенными в Стратегии действиями следует разработать мероприятия, необходимые для снижения отрицательного влияния преступности, атак и киберинцидентов на безопасное развитие информационного общества.

Механизмы, установленные в Разделе I Стратегии, предлагают создание эффективной законодательной базы, обеспечивающей безопасность государства в аспекте каждого установленного компонента, снижение рисков, угроз или даже их исключение в перспективе, и создание или назначение учреждения на национальном уровне типа CERT и разработку механизмов по созданию и укреплению внутриведомственных центов реагирования на инциденты кибернетической и информационной безопасности публичного или частного права.

2) Неавторизованный доступ к сетям и услугам электронных коммуникаций, неавторизованное изменение, удаление или повреждение информационных данных, незаконное ограничение доступа к этим данным и кибернетический шпионаж представляют собой виды давления на мировом уровне. В этом контексте выявляются проблемы, с которыми сталкивается Республика Молдова, а именно: рост количества информационных преступлений и правонарушений, количества кибернетических атак информационных ресурсов, опубликованных в глобальной сети Интернет, а также дефицита компетентных человеческих кадров.

В этом смысле, действия, указанные в Разделе I и частично в Разделе IV, представленные в Стратегии, предлагают внести некоторые изменения в основные законодательные акты по предупреждению и борьбе с информационной преступностью, в целях гармонизации законодательства в области, а также развития отраслевых программ, предназначенных для сотрудников с функциями расследования и уголовного преследования.

3) Особое внимание было посвящено компоненту безопасности медийного пространства. В этом контексте, дезинформация, пропаганда и манипулятивная подача информации извне представляют собой основные проблемы.

В качестве решений по улучшению, установленных в Разделе II, предлагается разработка и корректировка некоторых функциональных законных механизмов в целях пресечения феномена дезинформации и/или манипулятивной подачи информации, который напрямую угрожает безопасности информационного пространства.

4) Контрразведывательный компонент и компонент безопасности устанавливают проблемы относительно расширения в широком масштабе различными субъектами использования средств вмешательства во внутренние отношения Республики Молдова посредством пропаганды и медийной агрессии, а также средств информационно-психологического

давления, в целях дестабилизации общественно-политической ситуации и подрыва суверенитета и территориальной целостности Республики Молдова. Также, отмечаются активные кампании по информированию, реализованные международными террористическими организациями в целях подрыва и роста уровня ненависти к интересам правового государства и ценностям, всемирно принятым международным сообществом.

Решения, представленные в Разделе III, предлагают оформить правовую базу в целях обнаружения, предупреждения и пресечения действий по продвижению различных информационных продуктов и/или информационных ресурсов, содержащих элементы риска, и которые могут вызвать угрозу национальной безопасности.

5) Значимость осведомления и воспитания общества в духе ценностей является одной из прерогатив, установленной в Стратегии, которая должна в перспективе быть распространена и развита. В настоящий момент подтверждается отсутствие возможности защититься от феномена клеветы посредством онлайн-платформ, что отрицательно влияет на осуществление прав человека и основных свобод. Также выявляется значимость осведомления, воспитания, медийной и кибернетической компетенции в Республике Молдова, чтобы у граждан была возможность критически проанализировать медийное содержание в целях установления пропаганды.

В этом смысле авторы Стратегии предлагают выполнение действий в сторону улучшения проблем в этой части с помощью действий, указанных в Разделе II и IV. Таким образом, прерогатива гармонизации нормативной базы и разработка коммуникационных политик между государственными органами и гражданским обществом, позволила бы укрепить вовлечение всех правовых субъектов в процесс консультаций и принятия решений. В результате вырастет степень доверия в действия государственных органов в контексте защиты прав и основных свобод граждан, а также позволит им осознать необходимость в принятии гражданского поведения.

Глава IV - Видение и задачи стратегии

Данная Глава регламентирует стратегическое видение документа политик, устанавливающее, что в контексте успешного внедрения **Республика Молдова обеспечит безопасное информационное пространство для всех правовых субъектов путем гармонизации законодательной базы и ее внедрения, таким образом, защищая права и основные свободы человека и продвигая демократию и правовое государство.**

Здесь же описываются задачи[1] и конкретные действия для реализации цели Стратегии, которые разделены на 4 раздела, установленные из перспективы основных компонентов структуры и функциональности информационного общества. Следует отметить, что вследствие подробного анализа ситуации среды информационной безопасности, Рабочая группа установила комплекс реальных действий,

[1] Задачи в большей части взяты из Концепции информационной безопасности.

которые должны исправить проблемы, установленные и раскрытые в Главе III. Соответственно, была выявлена необходимость избежать поверхностный подход и представление недействующих механизмов, в особенности, в контексте, когда обеспечение информационной безопасности представляет собой одно из требований и на международном уровне.

Таким образом, **Раздел I** предусматривает обеспечение безопасности информационно-кибернетического пространства и расследования информационной преступности, которое реализуется посредством 11 специфических задач.

Среди основных приоритетов, установленных в Разделе I, представлены:

- Создание Национального центра реагирования на инциденты кибербезопасности (национальный CERT), который обеспечит взаимодействие между всеми компонентами обеспечения кибербезопасности.
- Назначение подразделения, выполняющего роль Правительственного центра реагирования на инциденты кибербезопасности (Правительственный CERT), который обеспечит функционирование и защиту специальных сетей на уровне Правительства и публичных органов власти.
- Укрепление сотрудничества Национального CERT, Правительственного CERT и частных CERT в целях предупреждения и решения инцидентов кибербезопасности.

Раздел II указывает на обеспечение безопасности информационно-медийного пространства посредством 3 специфических задач.

Меры, указанные в данном Разделе, создают и развивают способность государства реагировать в полезное время посредством специализированных органов на поступившие угрозы, которую в настоящий момент трудно обеспечить, а именно угрозы медийного пространства из Интернета, телевидения и радио.

Вследствие реализации действий, установленных в Разделе II, создается:

- Механизм взаимодействия и вовлечения экспертов в целях обеспечения безопасности информационного пространства путем развития гражданского контроля в области обеспечения информационной безопасности.
- Законодательная база для установления правового статуса периодических изданий, агентств печати и других субъектов, действующих в медиапространстве Интернета, в целях установления субъектов, вовлеченных в производство и распространение медиасодержания онлайн, и других посредников и дополнительных услуг, оказывающих отрицательное влияние на информационную безопасность.
- Информационный коммуникационный ресурс и стратегического информирования, а также единая система защиты информации, соблюдающая законны, организационные, технические, технологические и физические меры защиты.

Раздел III относится к укреплению операционных возможностей, которое реализуется посредством 6 специфических задач.

Принимая во внимание, что информационная безопасность представляет собой неотделимый компонент национальной безопасности, она может быть обеспечена только путем эффективного сотрудничества всех государственных органов в пределах установленных законом компетенций. В Разделе III предлагает реализовать следующие приоритетные задачи:

- Создание на национальном уровне подразделения, владеющего компетенциями по продвижению и согласованию политик информационной безопасности в демократическом обществе, в зависимости от развития технологии, правовых и другого характера отношений сектора информационного общества на национальном и международном уровне – Координационный совет по обеспечению информационной безопасности.
- Создание подразделения, ответственного за кибероборону на уровне Вооруженных сил, с функцией согласования на стратегическом уровне деятельности, предназначенной для защиты кибербезопасности Республики Молдова.
- Создание платформы, специализирующейся на гибридных угрозах безопасности, важный элемент из перспективы создания системы пресечения гибридных угроз информационного общества, которая сопоставит доступную информацию и облегчит прямой ответ в случае кризисной ситуации соответствующих органов.
- Разработка и продвижение законной базы регламентирования национальных критичных инфраструктур, в целях увеличения возможностей по защите национальных критичных инфраструктур, развития потенциала по предупреждению, обнаружению и пресечению экстремистских, террористических и других действий, ставящих под угрозу информационную безопасность.

В контексте разработки Стратегии особый акцент ставится на необходимость повышения качества процесса внутреннего согласования и международного сотрудничества в области информационной безопасности.

В этом смысле, Раздел **IV** включает 5 специфических задач, цель которых состоит в:

- Усовершенствование и согласование деятельности органов публичной власти, ответственных за обеспечение безопасности информационного пространства.
- Создание отраслевых программ обучения человеческих ресурсов в области информационной безопасности, по каждому отделу в отдельности: масс-медиа, информационная технология, оборона, общественный порядок и контринформация.
- Обеспечение и развитие международного сотрудничества по двум областям: область кибероборонны и область информационной преступности.

Глава V – Оценка влияния и расходов на внедрение Стратегии.

Глава V Стратегии описывает влияние и расходы на ее внедрение. Таким образом, качественное внедрение положений Стратегии увеличит степень защиты и безопасности в информационном пространстве, а расходы будут покрыты за счет внутренних и внешних, публичных и частных финансовых средств.

Характер настоящей Стратегии вызывает определенные риски разглашения некоторых классифицированных данных в аспекте оценки финансовых ассигнований для реализации определенных ключевых задач и деятельности из Плана действий, что требует установления, в индивидуальном порядке, сумм, необходимых на уровне органов власти, а также отдельного включения в каждый бюджетный год.

Главы VI – Ожидаемые результаты и показатели достижений и VII – Процедуры мониторинга и оценки, описывают ожидаемые результаты, показатели достижений, механизм мониторинга и оценки Стратегии. Внедрение настоящей Стратегии ведет к установлению инновационных подходов к формированию системы защиты и развития информационного пространства в условиях глобализации и свободного оборота информации. Одним из центральных элементов Стратегии является создание Координационного совета по обеспечению информационной безопасности, коллективного органа с консультативными и операционными функциями, который будет нести ответственность и обеспечивать системную целостность компонентов информационного пространства и поддержку, направленную на высокий уровень информационной безопасности

Процесс внедрения Стратегии сопровождается постоянным мониторингом за реализацией предложенных действий и полученными результатами, с внесением, в случае необходимости, обязательных изменений в политику, продвигаемую Государственной канцелярией в контексте настоящей Стратегии.

Авторы проекта предлагают, чтобы в качестве ответственного органа за процесс мониторинга и внедрения Плана действий к Стратегии информационной безопасности Республики Молдова на 2019-2024 годы была назначена Государственная канцелярия.

Со ссылкой на План действий по внедрению Стратегии информационной безопасности Республики Молдова на 2019-2024 годы.

План действий разделен на разделы и задачи, согласно их перечислению в тексте Стратегии. Одновременно, в целях реализации каждой цели предусмотрены конкретные действия и меры, установлены ответственные учреждения и партнеры. Также, для каждого действия установлены конкретные сроки для реализации.

В заключение, исходя из выше указанного, принятие настоящей Стратегии обусловлено необходимостью защиты интересов населения, общества, государства в информационном пространстве, серьезностью и

многочисленными угрозами информационной безопасности в современном обществе, необходимостью поддержания равновесия между интересами населения, общества и государства для обеспечения информационной безопасности. Также, глобальный характер информационных систем и сетей электронных коммуникаций требует тесного сотрудничества между всеми ответственными учреждениями, как на национальном, так и на мировом уровне, вследствие чего уважительно просим поддержать соответствующий проект.

II. Порядок включения проекта в систему действующих нормативных актов

Проект интегрируется в систему законодательства и соотносится с положениями действующих законодательных актов, с которыми связан, а предложенные изменения и дополнения не оказывают отрицательного воздействия на общую концепцию.

III. Финансово-экономическое обоснование

Предложенные для реализации действия покрываются за счет бюджета учреждений, в пределах утвержденных ассигнований, а также от внешней помощи в этой части. Предполагаемые расходы на действия будут скорректированы в период внедрения Плана, учитывая объем ассигнований, доступных в государственном бюджете.

Авторы проекта установили, что в целях обеспечения защиты данных из перспективы разработки нормативных актов, политик и планирований действий, в том числе финансовых ассигнований, органы/учреждения оценят и примут решение, в индивидуальном порядке, относительно данных, которые могут быть квалифицированы как информация, относящаяся к государственной тайне.

IV. Согласование и публичное обсуждение

В целях соблюдения положений Закона № 239 от 13.11.2008 года о прозрачности процесса принятия решений, проект Постановления был размещен на веб-странице Службы по адресу www.sis.md, в папке «Прозрачность», раздел «Прозрачность процесса принятия решений».

V. Заключение антикоррупционной экспертизы

На основании пункта а) части (2) статьи 28 Закона о неподкупности № 82 от 25.05.2017 года, публичные субъекты, обладающие правом законодательной инициативы, другие публичные субъекты, разрабатывающие и продвигающие проекты законодательных и нормативных актов, а также Секретариат Парламента в случае законодательных инициатив депутатов обязаны подвергать антикоррупционной экспертизе проекты своих актов, за исключением – программных документов.

В этом контексте, проект Стратегии и Плана не подлежит антикоррупционной экспертизе.

VI. Заключение экспертизы на предмет соответствия

Исходя из того, что целью проекта акта не является гармонизация национального законодательства с законодательством Европейского Союза, а также, что он противоречит законодательству ЕС, экспертиза на предмет соответствия не проводится.

VII. Заключение правовой экспертизы

Проект Стратегии информационной безопасности Республики Молдова на 2019-2024 годы и Плана действий по ее внедрению был подвержен правовой экспертизе, были представлены рекомендации, принятые авторами во внимание

VIII. Заключения других экспертиз

Проект Стратегии информационной безопасности Республики Молдова на 2019-2024 годы и Плана действий по ее внедрению не был подвержен другим экспертизам. Так как, исходя из предмета регулирования, он не относится к регулированию предпринимательской деятельности или другой экономической деятельности, чтобы было необходимо представить дополнительные заключения специалистов.

Василе БОТНАРЬ
Директор