# ПОСТАНОВЛЕНИЕ СОВЕТА БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

*18 марта 2019 г. № 1*

**О Концепции информационной безопасности Республики Беларусь**

Совет Безопасности Республики Беларусь п о с т а н о в л я е т:

1. Утвердить Концепцию информационной безопасности Республики Беларусь (прилагается).

2. Государственным органам и иным организациям в практической деятельности руководствоваться положениями Концепции информационной безопасности Республики Беларусь.

3. Государственному секретарю Совета Безопасности Республики Беларусь отражать результаты реализации Концепции информационной безопасности Республики Беларусь в ежегодном докладе Президенту Республики Беларусь о состоянии национальной безопасности и мерах по ее укреплению.

***Президент Республики Беларусь*** ***А.Лукашенко***

*УТВЕРЖДЕНО*

*Постановление*
*Совета Безопасности*
*Республики Беларусь*
*18.03.2019 № 1*

# КОНЦЕПЦИЯ
# информационной безопасности Республики Беларусь

## РАЗДЕЛ I
## ОБЩИЕ ПОЛОЖЕНИЯ

### ГЛАВА 1
### МИРОВОЕ ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ СФЕРЫ

1. На нынешнем этапе мирового развития информационная сфера приобретает ключевое значение для современного человека, общества, государства и оказывает всеобъемлющее влияние на происходящие экономические, политические и социальные процессы в странах и регионах. В результате повышения насыщенности и динамики общественных отношений, мировых и региональных событий, роста всеобщего интеллектуального потенциала значительно увеличиваются информационные потребности людей.

Формируемое в глобальном масштабе информационное общество представляет собой новый этап развития цивилизации с преобладанием знаний и информации, воздействием информационных технологий на все сферы человеческой деятельности. Кардинально повышается роль информационных технологий в реализации прав и свобод граждан.

Индустрия телекоммуникации стала одной из наиболее динамичных и перспективных сфер мировой экономики. С процессами информатизации все больше связываются национальные экономические интересы и перспективы инвестиций.

2. Вместе с тем трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства, информационной инфраструктуры, информационных систем и ресурсов.

### ГЛАВА 2
### АКТУАЛЬНОСТЬ И ЗНАЧЕНИЕ КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

3. Формирование в Республике Беларусь информационного общества, обеспечивающего доступность информации, распространение и использование знаний для поступательного и прогрессивного развития, рассматривается как национальный приоритет и общегосударственная задача.

4. Актуальность и значение Концепции информационной безопасности Республики Беларусь (далее – Концепция) обуславливаются следующими факторами:

повышением значимости формирования информационного общества в Республике Беларусь, его роли в социально-экономическом развитии Беларуси как суверенного и независимого государства, безопасности реализации национальных стратегий и планов создания цифровой экономики и научно-технического прогресса в целом;

необходимостью предметной и всесторонне осознанной защиты национальных интересов в информационной сфере, определяемых Концепцией национальной безопасности Республики Беларусь, обобщения практически и научно обоснованных взглядов на обеспечение информационной безопасности, конкретизации и детализации подходов к данной деятельности;

необходимостью рассмотрения информационной безопасности как обособленного феномена и нормативного института, а также правового закрепления основ государственной политики по защите национальных интересов в информационной сфере;

формированием новой сферы общественных отношений по обеспечению информационной безопасности;

важностью улучшения координации и управляемости деятельности субъектов, вовлеченных в развитие информационной сферы и обеспечение ее безопасности, устойчивого и последовательного функционирования механизмов реагирования на риски, вызовы и угрозы информационной безопасности;

необходимостью информирования граждан, а также международного сообщества о принятых в Республике Беларусь взглядах на сферу информационной безопасности и приоритетах ее обеспечения;

интеграцией Беларуси в систему международной информационной безопасности, важностью повышения концептуальной и технологической совместимости и синхронизации целей и задач национальной системы обеспечения информационной безопасности с корреспондирующими системами других государств и организаций.

## ГЛАВА 3
## ПРЕДМЕТ, ЦЕЛЬ, ЗАДАЧИ КОНЦЕПЦИИ, ЕЕ СВЯЗЬ С ДРУГИМИ ДОКТРИНАЛЬНЫМИ ДОКУМЕНТАМИ

5. Концепция представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности.

Концепция обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере.

6. Концепция основывается на Конституции Республики Беларусь, законодательстве Республики Беларусь в областях национальной безопасности, информатизации, развития цифровой экономики, информационного общества, науки и технологий, защиты интеллектуальной собственности, иных актах законодательства.

Концепция базируется на Концепции национальной безопасности Республики Беларусь, а именно:

исходит из понимания основных тенденций современного мира, определенных в ней основных национальных интересов в информационной сфере, потенциальных либо реально существующих угроз национальной безопасности;

конкретизирует цели, задачи и принципы обеспечения национальной безопасности в информационной сфере, основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в данной сфере;

предполагает реализацию этих целей, задач и принципов как неотъемлемую часть функционирования общей системы обеспечения национальной безопасности.

7. Концепция также исходит из геополитических интересов Республики Беларусь, ее места и роли в современном мире, основывается на соглашениях о сотрудничестве в области обеспечения информационной безопасности государств – участников Содружества Независимых Государств, государств – членов Организации Договора о коллективной безопасности, двусторонних соглашениях и иных обязательствах Республики Беларусь в области международной информационной безопасности, учитывает основные положения актов международных организаций, в том числе резолюций Генеральной Ассамблеи Организации Объединенных Наций, рекомендаций Организации по безопасности и сотрудничеству в Европе.

8. Для целей настоящей Концепции используются следующие понятия и их определения:

воздействие на информацию – действие по изменению формы предоставления и (или) содержания информации;

государственная информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств, формируемая или приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

государственный информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах, формируемая или приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

деструктивное информационное воздействие – осуществление информационного влияния на политические и социально-экономические процессы, деятельность государственных органов, а также на физических и юридических лиц в целях ослабления обороноспособности государства, нарушения общественной безопасности, принятия и заключения заведомо невыгодных решений и международных договоров, ухудшения отношений с другими государствами, создания социально-политической напряженности, формирования угрозы возникновения чрезвычайных ситуаций, разрушения традиционных духовных и нравственных ценностей, создания препятствий для нормальной деятельности государственных органов, причинения иного ущерба национальной безопасности;

защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

информационная инфраструктура – совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации;

информационный суверенитет Республики Беларусь – неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность;

информационная сфера – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;

информационное пространство – область деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание и собственно информацию;

кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз;

киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политик безопасности;

кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, а также способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти, либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка;

киберустойчивость – способность информационной системы предвидеть изменения обстановки и своевременно адаптироваться к ним в целях успешного предотвращения негативных последствий или быстрого восстановления после киберинцидента;

международная информационная безопасность – состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

обеспечение информационной безопасности – система мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз;

преступления в информационной сфере – предусмотренные Уголовным кодексом Республики Беларусь преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети;

суверенитет данных – подчиненность отношений по поводу информации в цифровой форме, возникающих на территории Беларуси, национальной юрисдикции Республики Беларусь.

Иные термины в Концепции приведены в значениях, используемых в законодательстве Республики Беларусь и международных актах, участницей которых является Республика Беларусь.

## РАЗДЕЛ II
## СОСТОЯНИЕ И РАЗВИТИЕ ИНФОРМАЦИОННОЙ СФЕРЫ В РЕСПУБЛИКЕ БЕЛАРУСЬ

### ГЛАВА 4
### ГУМАНИТАРНЫЙ АСПЕКТ ИНФОРМАЦИОННОЙ СФЕРЫ

9. Основополагающим национальным интересом Республики Беларусь в информационной сфере с точки зрения гуманитарного аспекта является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, свободу мнений, убеждений и их свободного выражения, а также права на тайну личной жизни.

10. В настоящее время состояние информационной сферы в Республике Беларусь характеризуется высоким уровнем доступа населения страны к массовой информации. Количество национальных средств массовой информации (далее – СМИ) и интернет-ресурсов неуклонно увеличивается, формируется при участии государства и в негосударственном секторе. Белорусское информационное пространство открыто для активной работы иностранных СМИ и интернет-ресурсов. В стране ежегодно увеличиваются пропускная способность внешних каналов доступа в сеть Интернет, количество интернет-пользователей, абонентов сетей электросвязи. Также развивается информационное взаимодействие граждан, создаются сетевые сообщества для коммуникации, обмена информацией, опытом и знаниями, общественного обсуждения проектов нормативных правовых актов, широко применяется практика краудфандинга, повышается роль общественных советов и независимых экспертов в принятии решений государственными органами, формируются институты общественного самоконтроля в целях сохранения исторического, культурного наследия и укрепления правосознания.

В целом белорусскому информационному пространству в полной мере свойственны мировые тренды информатизации, в том числе перевод СМИ в цифровой формат (дигитализация), сочетание их различных типов (мультимедийность), адаптация информационного продукта к распространению через Интернет, сближение и слияние в нем различных типов СМИ (конвергенция).

11. В то же время мировое развитие информационно-коммуникационных технологий (далее – ИКТ) обуславливает постоянное появление новых источников информации, что объективно снижает в информационном пространстве долю отечественного контента и требует более активной работы по его продвижению. Исходя из этого необходимо на государственном уровне предпринимать меры по повышению объема, разнообразия и качества национального контента, скорости его предоставления, доверия населения к

официальной информации и государственным СМИ, адаптации форм распространения информации к первоочередным информационным потребностям граждан, а также достижению баланса интересов личности, общества и государства.

## ГЛАВА 5
## ТЕХНОЛОГИЧЕСКИЙ АСПЕКТ ИНФОРМАЦИОННОЙ СФЕРЫ

12. Основными направлениями информатизации в Республике Беларусь определены развитие эффективной и прозрачной системы государственного управления, обеспечение быстрых, удобных и безопасных коммуникаций между государством, бизнесом и гражданами, модернизация национальной информационной инфраструктуры, внедрение ИКТ в реальном секторе экономики, совершенствование социальной сферы на основе ИКТ, укрепление собственной отрасли информационных технологий.

13. Цифровая трансформация экономики является важнейшей составляющей формирования информационного общества и одним из главных направлений развития Республики Беларусь, в результате которого в ближайшие десятилетия все отрасли, рынки, сферы жизнедеятельности государства должны быть переориентированы на новые цифровые экономические модели. Для решения этой задачи в стране определены структура управления информатизацией и архитектура электронного правительства. Развиваются инновационные цифровые технологии, основанные на системах искусственного интеллекта, нейронных сетей, обеспечивающие работу с разнообразными информационными ресурсами, в том числе массивами больших данных, методах распределенных вычислений (облачные технологии), технологии реестра блоков транзакций (блокчейн).

Беларусь последовательно участвует в процессах информатизации на трансграничном контуре, в том числе в рамках Союзного государства Беларуси и России, Евразийского экономического союза, Содружества Независимых Государств, Европейского союза и иных мировых систем политического и экономического взаимодействия и партнерства.

14. Наряду с этим объем применения информационных технологий в реальном секторе экономики остается невысоким. Степень цифровизации отраслей экономики различна, что снижает ожидаемый синергетический эффект от синхронной информатизации, и с учетом этого следует разрабатывать цифровую политику для конкретных сфер государственной жизнедеятельности, ориентировать пилотные проекты цифровизации на их отраслевое масштабирование, создавать центры компетенции по вопросам цифровой трансформации. Требуется переход электронного правительства от простого предоставления услуг по запросам граждан к проактивной работе с населением. Быстрое развитие ИКТ и увеличение информационных потребностей общества обуславливают необходимость освоения новых стандартов в сфере телекоммуникаций, повышения производительности и надежности сетевой инфраструктуры.

# РАЗДЕЛ III
# ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## ГЛАВА 6
## ЦЕЛИ И НАПРАВЛЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ

15. Целью обеспечения информационной безопасности является достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.

Обеспечение информационной безопасности осуществляется в соответствии с государственной политикой в данной области, которая включает в себя формирование, совершенствование и реализацию организационных, правовых, научно-технических, правоохранительных, экономических мер обеспечения национальной безопасности в информационной сфере. В свою очередь, именно через развитие этой сферы главным образом обеспечивается и ее безопасность.

16. На государственном уровне осуществляются мониторинг, анализ и оценка состояния информационной безопасности, применяются индикаторы оценки ее состояния. Определяются приоритетные направления предотвращения угроз информационной безопасности, минимизации их деструктивного воздействия и локализации последствий. Разрабатывается и реализуется комплекс мер стратегического и тактического характера по предупреждению и нейтрализации информационных рисков, вызовов и угроз.

17. Обеспечивается конституционное право граждан свободно искать, получать, передавать, производить, хранить и распространять информацию любым законным способом, право на тайну личной жизни и иную охраняемую законом тайну, защиту персональных данных и авторских прав, а также соблюдение баланса прав с ограничениями, связанными с обеспечением национальной безопасности. Формируются правовые, организационные и технологические условия для безопасности функционирования национальных средств массовой информации, осуществляется государственный и общественный контроль их деятельности.

Реализуется максимальная доступность для граждан и организаций государственных электронных услуг, административных процедур и информационных ресурсов государственных органов и организаций.

Повышается осведомленность граждан и общества об угрозах национальной безопасности и государственных мерах по ее обеспечению, их вовлеченность в обеспечение безопасности информационной сферы.

18. Государство всесторонне содействует защищенности национальных информационных систем, обеспечению безопасности используемого гражданами и организациями программного обеспечения. В целях улучшения устойчивости государственного сектора к информационным рискам осваиваются передовые технологии, внедряются новые средства и способы обеспечения информационной безопасности.

Разрабатываются стандарты информационной безопасности и с их учетом проводится аудит государственных систем информационной безопасности. Развивается смарт-проектирование решений по обеспечению информационной безопасности. На нормативном уровне выделяется и регламентируется функционирование критически важных объектов информатизации (далее – КВОИ). Поощряется развитие технологий безопасности в бизнесе и жизнедеятельности граждан.

19. Деяния, причиняющие существенный вред правоохраняемым интересам в информационной сфере или создающие опасность его причинения, криминализируются в уголовном законе в соответствии с существующими мировыми подходами. Реализуются шаги по снижению угроз киберпреступности, в том числе кибертерроризма, расследованию и пресечению действий вовлеченных в террористическую деятельность лиц, перекрытию каналов пропаганды терроризма, привлечения и вербовки сторонников, поощрения и провоцирования террористической активности, финансирования терроризма.

Вводятся правовые режимы безопасности информации и информационных ресурсов, технические условия и политики безопасности. Осуществляется выявление и привлечение к установленной законом ответственности лиц, наносящих вред государственным информационным системам, обеспечивается государственная защита интересов граждан и организаций вне зависимости от форм собственности.

20. Развивается взаимодействие государства, общественности, бизнес-сообщества, СМИ в целях своевременного обнаружения рисков и вызовов информационной безопасности, воспрепятствования кибератакам и акциям деструктивного информационного воздействия, повышения эффективности правоохранительной деятельности.

21. Уделяется особое внимание кадровому потенциалу в обеспечении информационной безопасности. На современном образовательном и технологичном уровне осуществляется специальная подготовка, переподготовка и повышение профессиональной квалификации лиц, обеспечивающих информационную безопасность, сотрудничество между государственными органами, учреждениями образования и отраслевыми предприятиями в подборе, подготовке и трудоустройстве таких кадров, интегрирование тематики информационной безопасности в образовательные программы всех уровней обучения. Формируется государственный заказ на подготовку кадров.

22. Производятся средства обеспечения информационной безопасности. Наращивается научный потенциал и финансирование работ по исследованию и созданию новых решений в сфере обеспечения информационной безопасности, в том числе технической защиты информации, криптологии, криминологии, криминалистики. Государство осуществляет финансирование приоритетных направлений обеспечения информационной безопасности, прежде всего в рамках государственных программ. Разрабатываются инновационные методы и технологии защиты информационных ресурсов и систем.

23. Предпринимаются усилия по повышению действенности международного права и соблюдению моральных норм ответственного поведения в информационном пространстве, оказывается содействие разработке и внедрению мер по укреплению доверия в информационном пространстве. Создаются и развиваются каналы международного обмена опытом в области обеспечения информационной безопасности, а также информацией об угрозах национальным интересам, в том числе уязвимостях информационных систем, инцидентах в информационной инфраструктуре.

24. Безопасность информационной сферы и в целом состояние информатизации в Республике Беларусь характеризуются международными рейтингами и иными общепринятыми в мире критериями, индексами и индикаторами, в том числе лежащими в основе показателей социально-экономического развития, обеспечения национальной безопасности и отражающими иную всестороннюю деятельность государства, связанную с данной сферой.

## ГЛАВА 7
## ИНФОРМАЦИОННЫЙ СУВЕРЕНИТЕТ

25. В условиях обострения международных противоречий становится проблематичным выработать эффективные и общепринятые правила поведения мирового сообщества в информационном пространстве. Подходы различных стран к оценке угроз в информационной сфере и противодействию им не совпадают, а по отдельным направлениям поляризируются.

В связи с этим важнейшей целевой установкой обеспечения информационной безопасности является информационный суверенитет Республики Беларусь.

26. Информационный суверенитет достигается, прежде всего, путем формирования системы правового регулирования отношений в информационной сфере, обеспечивающей безопасное устойчивое развитие, социальную справедливость и согласие.

27. В рамках данной системы государство обеспечивает развитие национальных СМИ и телекоммуникаций, современных ИКТ, национальной индустрии производства средств информатизации, а также защиту национальных рынков информационных и телекоммуникационных услуг, снижающих зависимость от технологий иностранного производства и сокращающих цифровое неравенство. В обществе воспитывается и стимулируется критическое отношение к проявлениям неуважения национальных устоев, традиций и нарушениям норм морали и права в информационной сфере, нетерпимость к дезинформации, информационным манипуляциям и иным неявным информационно-психологическим воздействиям.

28. Формируются правовые условия и границы деятельности зарубежных и международных субъектов в национальном информационном пространстве для обеспечения потребностей граждан во внешнем информационном обмене без культурной и информационной экспансии, вмешательства во внутренние дела Республики Беларусь.

29. Создаются необходимые условия для построения и безопасного развития функциональной, технологически самодостаточной, надежной и устойчивой информационной инфраструктуры. Осуществляется защита информационных ресурсов, в том числе государственных секретов, иной охраняемой информации, персональных данных, обеспечивающая политическую самостоятельность государства, защищенность жизненного пространства человека, сохранение духовных и культурных ценностей белорусского общества, научно-технологические преимущества и реализацию иных национальных интересов. Республикой Беларусь реализуется принцип «суверенитета данных».

30. Стремление к информационному суверенитету не расходится с международно-правовыми принципами обеспечения прав и свобод, гарантирующих конкурентное и свободное развитие в условиях мировой цифровой трансформации.

## ГЛАВА 8
## ИНФОРМАЦИОННЫЙ НЕЙТРАЛИТЕТ

31. В международных отношениях информационный суверенитет Республики Беларусь обеспечивается в том числе на основе принципа информационного нейтралитета, предусматривающего проведение миролюбивой внешней информационной политики, уважение общепризнанных и общепринятых прав любого государства в данной сфере, исключение инициативы вмешательства в информационную сферу других стран, направленного на дискредитацию или оспаривание их политических, экономических, социальных и духовных стандартов и приоритетов, а также нанесения вреда информационной инфраструктуре каких бы то ни было государств и участия в их информационном противостоянии. При этом Республика Беларусь отстаивает собственные национальные интересы в информационной сфере с использованием всех имеющихся сил и средств.

32. В целях обеспечения политики информационного нейтралитета повышается степень присутствия Беларуси в мировом информационном пространстве, расширяется международный информационный обмен, поддерживается установление и регулирование

всеобщих правил поведения в данной сфере и осуществляется заключение соглашений по обеспечению международной информационной безопасности.

## ГЛАВА 9
## ГОСУДАРСТВЕННОЕ РЕАГИРОВАНИЕ НА РИСКИ, ВЫЗОВЫ И УГРОЗЫ В ИНФОРМАЦИОННОЙ СФЕРЕ

33. Государство осуществляет реагирование на риски и вызовы в информационной сфере в целях предупреждения их трансформации в угрозы национальной безопасности, развития и масштабирования вредоносного воздействия.

Реагирование на риски и вызовы в информационной сфере осуществляется всеми без исключения государственными органами и организациями в соответствии с областью их деятельности согласно непосредственному предназначению максимально полно и оперативно. Государство в лице этих государственных органов и организаций обеспечивает своевременное принятие мер безопасности, незамедлительно оповещает заинтересованные субъекты, минимизирует ущерб и локализует последствия, определяет причастных лиц и организации, накапливает опыт противодействия угрозам.

34. Государственное реагирование на риски, вызовы и угрозы в информационной сфере предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба). Определяется защищенность и устойчивость объектов информационной безопасности, в том числе информационной инфраструктуры, информационных ресурсов, индивидуального, группового и массового сознания к действию угроз. Выявляются и исключаются условия возникновения и реализации рисков, вызовов и угроз информационной безопасности.

35. Подготавливаются и внедряются сценарии и планы кризисного реагирования на кибератаки, компьютерные инциденты, акты деструктивного информационного воздействия, иные угрозы информационной безопасности, а также проводятся учения и тренировки сил реагирования.

Реализуется политика информационного сдерживания, выражающаяся в демонстрации достоверной готовности к отражению деструктивных информационных воздействий, достаточной возможности технологического, организационного, правового противодействия угрозам в информационной сфере и выявления их источников.

36. В случае существенного осложнения информационной обстановки, связанного в том числе с необходимостью обеспечения военной безопасности государства, осуществляются дополнительные меры защиты информационной сферы правовыми, информационно-технологическими, техническими и иными методами (информационное противоборство), обеспечивается приоритетное взаимодействие военной организации государства и гражданского сектора.

37. Вооруженные Силы Республики Беларусь, иные воинские формирования предпринимают меры по обеспечению информационной безопасности в рамках решения возложенных задач по своему непосредственному предназначению с применением современных, высокотехнологичных сил и средств.

38. Беларусь участвует в международном реагировании на потенциальные риски, вызовы и угрозы информационной безопасности в рамках заключенных договоров и соглашений, осуществляет межгосударственное взаимодействие в анализе рисков,

вызовов и угроз информационной безопасности, обмен опытом и совместные практические мероприятия.

## РАЗДЕЛ IV
## БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА КАК ОДНО ИЗ ВАЖНЕЙШИХ УСЛОВИЙ РАЗВИТИЯ СУВЕРЕННОГО, ДЕМОКРАТИЧЕСКОГО СОЦИАЛЬНОГО ГОСУДАРСТВА

### ГЛАВА 10
### ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

39. Глобальное возрастание роли информации в системе общественных отношений, открытость информационного пространства и повышение уровня информатизации населения обуславливают новые меры безопасности информационной сферы с точки зрения обеспечения государством полноценной реализации своих суверенных прав и интересов социально-экономического развития.

40. Механизмы деструктивного информационно-психологического воздействия на личность, общество и государство постоянно совершенствуются, а масштабное манипулирование массовым сознанием принимает такую же остроту, как борьба за территории, ресурсы и рынки. Через информационное пространство осуществляется преднамеренная дискредитация конституционных основ государств и их властных структур, размывание национального менталитета и самобытности, вовлечение людей в экстремистскую и террористическую деятельность, разжигание межнациональной и межконфессиональной вражды, формирование радикального и протестного потенциала. Информационный фактор играет все более значительную роль в межгосударственных конфликтах и неявных действиях, направленных на нарушение суверенитета, территориальной целостности стран и снижение темпов их развития. В результате информационных воздействий существенно меняются социальные связи человека в обществе, стиль мышления, способы общения, восприятие действительности и самооценка.

Все большее беспокойство вызывает активное распространение в информационном пространстве фальсифицированной, недостоверной и запрещенной информации. Снижение критического отношения потребителей информации к фейковым сообщениям новостных ресурсов, в социальных сетях и на других онлайн-платформах создает предпосылки преднамеренного использования дезинформации для дестабилизации общественного сознания в политических, социально-опасных, иных подобных целях.

41. В связи с этим особое значение приобретает ответственное поведение всех участников информационных процессов, а также выработка общих правил коммуникации в информационном пространстве, основанных на признании идентичности прав и обязанностей в существующей реальности (физическом мире) и виртуальном пространстве.

### ГЛАВА 11
### ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

42. Для Республики Беларусь основными источниками угроз информационно-психологического характера в информационной сфере являются информационное

противоборство между ведущими мировыми центрами силы, целенаправленное формирование внутри и за пределами страны информационных поводов для дискредитации государственной внешней и внутренней политики.

43. С учетом этого главная цель обеспечения безопасности информационно-психологической компоненты информационной сферы состоит в сохранении информационного суверенитета и проведении политики информационного нейтралитета, а также формировании устойчивого иммунитета против деструктивных информационно-психологических воздействий на массовое общественное сознание, а в необходимых случаях – и противодействие им.

44. Для этого главным образом необходимо на государственном уровне обеспечивать формирование, использование и развитие информационного пространства исключительно в целях социального, экономического и культурного развития, а также постоянную, активную и эффективную деятельность государственных органов, организаций, научно-экспертного сообщества в информационном пространстве, особенно наращивать ее в сети Интернет.

45. В приоритетном порядке необходимо поддерживать сохранение в обществе традиционных социальных устоев и ценностей, открытое и всестороннее информационное обеспечение и сопровождение государственной политики, а также воспрепятствование в законном порядке распространению незаконной и недостоверной массовой информации.

## ГЛАВА 12
## СОХРАНЕНИЕ ТРАДИЦИОННЫХ УСТОЕВ И ЦЕННОСТЕЙ

46. Для повышения устойчивости общества к деструктивным информационным воздействиям необходимо сосредоточить усилия на сохранении сформированных в общественном сознании традиционных фундаментальных ценностей народа, выступающих в качестве одного из основных элементов обеспечения его единства и одним из условий неуклонного развития государства.

47. Информационная политика Республики Беларусь нацеливается на продвижение таких жизненных приоритетов, как гуманизм, миролюбие, добрососедство, справедливость, взаимопомощь, крепкие семейные отношения, здоровый образ жизни, созидательный труд, принятые в белорусском обществе нормы морали и нравственности, позитивное правосознание. В информационной сфере в полной мере находят отражение равные права всех без исключения национальностей, населяющих Республику Беларусь, уважительное отношение ко всем традиционным религиям и вероисповеданиям. Важнейшее значение имеет поддержка и всемерное развитие гражданско-патриотической идеологии.

48. Белорусский язык наряду с конституционно закрепленным в государстве двуязычием содействует повышению национального самосознания белорусского общества и формированию его духовности. Расширение социальных функций и коммуникативных возможностей белорусского языка, его полноценное и всестороннее развитие вместе с другими элементами национальной культуры выступают гарантом гуманитарной безопасности государства.

49. Требует дальнейшей последовательной реализации государственная историческая политика, направленная на закрепление в Беларуси и за ее пределами белорусской национальной концепции исторического прошлого страны и белорусской модели памяти, построенной в соответствии с настоящей Концепцией в качестве доминирующей.

## ГЛАВА 13
## ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ И СОПРОВОЖДЕНИЕ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ

50. Информационное обеспечение и сопровождение государственной политики нацелено на развитие массового политического сознания граждан, повышение потенциала и качества государственного управления, усиление восприятия Беларуси в мировом информационном пространстве. Эта деятельность осуществляется через максимально открытое и оперативное доведение до населения Республики Беларусь и мирового сообщества достоверной и полной информации о деятельности органов государственной власти Беларуси, предпринимаемых мерах по совершенствованию социально-экономических отношений, вырабатываемых и принятых законодательных, иных нормативных правовых актах и других решениях во внутри- и внешнеполитической сферах.

51. Государство обеспечивает построение конструктивного и всеобъемлющего информационного взаимодействия между органами власти, средствами массовой информации и общественностью на всех уровнях.

52. Особое значение приобретает конкурентоспособность государственных средств массовой информации, достигаемая в том числе через национальное производство высококачественного контента и формирование современной системы медиаизмерений.

53. Государство оказывает правовую поддержку отечественным СМИ, направленную на повышение качества аудиовизуального продукта и расширение тематического и жанрового разнообразия программ, формирование иных дополнительных возможностей развития, в том числе через законодательное регламентирование объема и качества иностранного вещания в Республике Беларусь, регулирование объема рекламных услуг, определение оптимальных условий регистрации.

54. Органы власти, иные государственные органы и организации, учреждения науки, образования и культуры, должностные лица и представители научно-экспертного сообщества проводят активную, высокотехнологичную и разностороннюю деятельность в информационном пространстве, включая национальные и зарубежные электронные средства массовой информации, иные интернет-ресурсы и средства интернет-коммуникации, а также создают условия для формирования современных отечественных медийных аналитических, научных и дискуссионных площадок.

## ГЛАВА 14
## БЕЗОПАСНОСТЬ МАССОВОЙ ИНФОРМАЦИИ

55. Отношения в области массовой информации основаны на принципах законности, достоверности, уважения прав и свобод человека, многообразия мнений, защиты нравственности и иных. Наряду с конституционным обеспечением свободы слова в Республике Беларусь для соблюдения этих принципов устанавливаются законодательные требования к распространению массовой информации, соответствующие мировой практике и общепринятым социальным стандартам. Осуществляется общественный контроль за распространением в информационном пространстве незаконной и недостоверной информации.

56. Не допускается распространение информации, направленной на пропаганду войны, экстремистской деятельности или содержащей призывы к такой деятельности, потребления наркотических средств и им подобных веществ, порнографии, насилия и

жестокости, иной информации, запрещенной законодательством. На государственном уровне реализуются меры по воспрепятствованию распространению информации, способной нанести вред национальным интересам, и недостоверных сведений, а также по снижению анонимности в информационном пространстве. При трансляции контента не разрешается применение скрытых технологических приемов, воздействующих на подсознание людей или оказывающих вредное влияние на их здоровье.

57. Ограничивается в законодательном порядке распространение информации без знака возрастной категории, а также поощряются меры родительского контроля при использовании детьми информационных технологий.

## РАЗДЕЛ V
## ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

### ГЛАВА 15
### ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

58. Цифровая трансформация экономики и инновации в области ИКТ наряду с мировым развитием и наращиванием технологических возможностей во взаимодействии людей, бизнеса, государственных институтов обуславливают необходимость принятия особых мер, обеспечивающих доверие и безопасность при создании и использовании в современном информационном обществе информационной инфраструктуры и данных в информационных системах.

59. Политическая и социально-экономическая сферы, общественная и военная безопасность становятся все более уязвимыми перед преднамеренными или случайными технологическими воздействиями, формирующимися в том числе в условиях недостаточных глобальных механизмов согласованного и действенного предупреждения и сдерживания киберинцидентов в сети Интернет.

Повсеместное функционирование объектов промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности. Кибератаки на информационную инфраструктуру рассматриваются в мире как одна из наиболее значимых угроз безопасности.

Во многих национальных вооруженных силах создаются и развиваются кибервойска, а проведение кибероперации предусматривается в доктринальных и стратегических документах. Одновременно рассматривается возможность реагирования на кибератаки как на вооруженную агрессию, что в условиях практической невозможности точной идентификации их источников (инициаторов) может привести к бездоказательной и произвольной трактовке обоснованности встречных военных действий.

Неуклонно растет количество киберпреступлений. Информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными.

60. Однако ни в глобальном, ни в региональных масштабах пока не удается эффективно воспрепятствовать разработкам и распространению средств, заведомо предназначенных для уничтожения, блокирования, модификации, похищения информации в сетях и ресурсах или нейтрализации мер по ее защите. Выработка

правовых, процедурных, технических и организационных мер против кибервоздействий на информационные ресурсы отстает от формирования реальных и потенциальных угроз их осуществления.

## ГЛАВА 16
## ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

61. В качестве наиболее вероятных источников угроз кибербезопасности рассматриваются отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах, противоправная деятельность отдельных лиц и преступных групп, преднамеренные действия и ошибки персонала информационных систем, выражающиеся в нарушении установленных регламентов их эксплуатации и правил обработки информации, зависимость Беларуси от других стран – производителей программных и аппаратных средств при создании и развитии информационной инфраструктуры.

62. Перед Республикой Беларусь стоит стратегическая цель развития системы обеспечения кибербезопасности, базирующейся на передовых международных подходах управления рисками и предназначенной для реализации долгосрочных мер по их сокращению до приемлемого уровня.

63. Национальная система обеспечения кибербезопасности должна реализовывать весь возможный комплекс правовых, организационных и технических мер по обеспечению безопасности национальной информационной инфраструктуры, в том числе информационных систем, обеспечивать конфиденциальность, доступность и целостность информации, а также легко трансформироваться и адаптироваться в изменяющейся обстановке за счет постоянного анализа на предмет соответствия актуальным рискам кибербезопасности.

64. В первую очередь необходимо обеспечить киберустойчивость национального сегмента сети Интернет, критически важных объектов информатизации и государственных информационных систем, эффективное противодействие киберпреступлениям.

## ГЛАВА 17
## БЕЗОПАСНОСТЬ НАЦИОНАЛЬНОГО СЕГМЕНТА СЕТИ ИНТЕРНЕТ

65. Необходимым условием реализации прав граждан в информационной сфере, поддержания высокого уровня информационного обмена, оказания информационных услуг является устойчивое функционирование и управляемость национального сегмента сети Интернет. В Республике Беларусь кибербезопасность национального сегмента сети Интернет обеспечивается главным образом за счет отражения основного объема кибератак на информационные системы и сети передачи данных путем блокирования вредоносных коммуникаций между субъектами и объектами воздействий.

66. Государством поддерживается и стимулируется применение лучших практик обеспечения кибербезопасности. Наиболее перспективной задачей рассматривается создание единой государственной системы мониторинга национального сегмента сети Интернет с одновременным формированием облачной платформы предоставления комплексных сервисов информационной безопасности государственному сектору и бизнес-сообществу в интересах автоматизированного учета киберинцидентов и оперативного обмена информацией о них между уполномоченными государственными

органами, операторами электросвязи и командами быстрого реагирования на компьютерные инциденты (CERT/CSIRT). В перспективе также необходимо формирование экосистемы для создания и функционирования национального удостоверяющего центра, корневой сертификат которого будет являться доверенным для основных операционных систем и веб-браузеров.

67. Наряду с этим требуется организовать функционирование службы оценки репутации IP-адресов для предоставления в режиме реального времени поставщикам интернет-услуг сведений об адресах, используемых для кибератак.

68. Необходимо обеспечить достижение и сохранение баланса между надежной идентификацией пользователей, регистрацией их действий и созданием условий для безопасного сбора, обработки, предоставления, хранения и распространения персональных данных в национальном сегменте сети Интернет, а также формирование и развитие национальных рынков страхования киберрисков и услуг тестирования на проникновение.

## ГЛАВА 18
## КИБЕРУСТОЙЧИВОСТЬ КВОИ И ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

69. Обеспечение безопасности информационной инфраструктуры осуществляется путем выделения наиболее значимых объектов информатизации, отказ функционирования или нарушение работы которых может повлечь значительные негативные последствия для национальной безопасности в политической, экономической, социальной, информационной, экологической и иных сферах.

В целях достижения киберустойчивости КВОИ в Республике Беларусь реализуется особый комплекс правовых, организационных и технических мероприятий, основанный на выработке критериев отнесения объектов к такой категории и принятии в их отношении соответствующих целенаправленных и всесторонних защитных мер. Данный подход позволяет создавать индивидуальную модель безопасности каждого КВОИ с учетом систематизированных общих требований по безопасности, эффективно выявлять и оценивать риски, поддерживать высокую готовность к предупреждению и локализации последствий кибератак, а также проводить внешнюю оценку созданных систем безопасности.

70. Повышение эффективности обеспечения безопасности КВОИ необходимо осуществлять с помощью интегрирования в государственную систему мониторинга национального сегмента сети Интернет отраслевых систем мониторинга и контроля киберугроз. При обеспечении киберустойчивости КВОИ Беларусь заинтересована в использовании международных стандартов и лучших практик. Важное практическое значение имеют регулярные киберучения и соревнования с привлечением эксплуатирующего персонала, собственников, владельцев и внешних субъектов, задействованных в обеспечении кибербезопасности.

71. Государство заинтересовано в защите от рисков, вызовов и угроз государственных информационных систем. В этих целях определяются порядок их создания и эксплуатации, включения в информационные сети и правила обмена информацией, а также применяются специальные процедуры государственной регистрации.

В перспективе достижение необходимого уровня защиты сервисов электронного правительства и киберустойчивости государственных информационных систем должно

обеспечиваться главным образом за счет их безопасного проектирования и эксплуатации, а не принятия последующих защитных мер, а также через внедрение их обоснованной унификации при построении и модернизации этих систем.

72. Неотъемлемой частью обеспечения безопасности КВОИ и государственных информационных систем является использование регулярно обновляемого, подлинного лицензионного программного обеспечения, получаемого из доверенных источников.

## ГЛАВА 19
## ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ

73. В Республике Беларусь создана система предупреждения, выявления, пресечения и всестороннего расследования киберпреступлений. Обеспечивается соответствие норм Уголовного кодекса Республики Беларусь в данной области уровню общественного развития, мировым тенденциям правового регулирования и передовому зарубежному опыту.

В связи с появлением новых общественно опасных деяний в информационной сфере устанавливается уголовная и иная ответственность за их совершение. Обеспечивается постоянное совершенствование форм и методов предупреждения, выявления, пресечения и расследования киберпреступлений, повышается своевременность и качество оперативно-розыскной деятельности.

74. Беларусь заинтересована в сближении и унификации подходов противодействия киберпреступлениям на международном уровне, выработке общих стандартов в правоприменительной практике, международном обмене опытом и практическом взаимодействии. Осуществляются реализация регионального и международного сотрудничества в сфере кибербезопасности, отслеживание деятельности преступных групп и отдельных преступников, действующих в киберпространстве.

75. Важное значение в противодействии киберпреступлениям имеет повышение доверия между правоохранительными органами, организациями государственного и частного секторов, образовательными и научными учреждениями, объединение их усилий в предупреждении, выявлении, пресечении и расследовании киберпреступлений. Одной из эффективных мер предупреждения и профилактики киберпреступлений является снижение мотивации их совершения за счет устранения условий формирования противоправных схем.

76. Наряду с этим одним из приоритетных направлений деятельности уполномоченных государственных органов является профилактика киберпреступности, основанная на популяризации среди населения, прежде всего молодежи, нетерпимости к асоциальному поведению в информационном пространстве, проведении разъяснительной работы в СМИ и сети Интернет в целях формирования безопасной национальной информационной экосистемы. Для повышения правосознания и снижения уязвимости от кибератак проводится обучение граждан основам поведения в информационной сфере.

# РАЗДЕЛ VI
# ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

## ГЛАВА 20
## ОБУСЛОВЛЕННОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

77. Появление широких и доступных возможностей для сбора, хранения и обработки большого объема данных, создание технологий прямого доступа к информации обуславливают необходимость рассматривать ее как самостоятельный и ценный ресурс. Информационные ресурсы становятся приоритетным объектом преступлений и киберинцидентов, подвергаются похищению, модификации, уничтожению, блокированию и другим воздействиям.

78. Повышается значение технической защиты информации ограниченного распространения, в то время как средства похищения, незаконного блокирования и иного воздействия на информационные ресурсы универсально применяются в политических, военных, разведывательных, экономических, преступных и иных целях.

Множественные угрозы и риски незаконного и необоснованного вмешательства в частную жизнь граждан, похищение персональных данных, компрометация реквизитов доступа и избыточное профилирование сужают личное пространство человека и нарушают его приватность. Раскрытие личной информации стало неотъемлемым атрибутом корыстных преступлений и преступлений против личности.

Формируется нелегальный рынок баз и банков данных, спрос на которые обуславливает похищение информационных массивов, сопровождаемое нарушением авторских прав.

## ГЛАВА 21
## ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

79. Основными источниками угроз в области обеспечения безопасности информационных ресурсов в Республике Беларусь следует рассматривать деятельность отдельных лиц, преступных групп, недобросовестных отечественных и иностранных организаций, объединений или сообществ, направленную на получение неправомерного доступа к этим ресурсам в политических, военных, коммерческих, личных и иных целях, осуществляемого в обход установленного порядка или вопреки общепринятым нормам морали и нравственности, а также нарушение функционирования информационной инфраструктуры.

80. Основной целью государственной политики в области обеспечения безопасности информационных ресурсов является сохранение их доступности, целостности и конфиденциальности.

81. Система обеспечения безопасности информационных ресурсов основана на стратегическом принципе соблюдения баланса свободы информации и права на тайну, гарантиях государства на распространение или предоставление общедоступной информации. Государство обеспечивает расширение безопасного доступа к информационным ресурсам добросовестных пользователей, развитие сервисов качественного и удобного предоставления информации, совершенствование систем ее данных.

82. На этом этапе необходимо главным образом обеспечивать надежную и всесторонне обусловленную защиту информации ограниченного распространения, безопасность персональных данных и государственных информационных ресурсов.

## ГЛАВА 22
## ЗАЩИТА ГОСУДАРСТВЕННОЙ И СЛУЖЕБНОЙ ТАЙНЫ

83. Безопасность данных, отнесенных к государственной или служебной тайне, обеспечивается в соответствии с национальным законодательством о государственных секретах. Посредством правовых запретов ограничивается обращение информации, содержащей сведения, отнесенные к государственным секретам, получение лицами секретных сведений. Исключаются хранение и обработка сведений в общедоступных формах, в том числе в информационных системах, имеющих доступ в сеть Интернет и иные открытые компьютерные сети. Вводится ответственность за нарушение правовых запретов и предписаний в сфере государственных секретов.

84. Наряду с этим отнесение информации к государственным секретам является исключительным правом строго определяемого перечня государственных органов и организаций и осуществляется на основании оценки вреда (ущерба) от разглашения, похищения или утраты такой информации. Организационные, материальные и иные затраты на обеспечение защиты этой информации не могут превышать указанного вреда (ущерба), выводы о возможности и размере которого делаются на основе конкретных показателей (индикаторов) или принятых практик.

Государство исходя из презумпции свободного распространения информации, а также в целях повышения открытости социально-экономических и иных общественных отношений заинтересовано в последовательном уменьшении количества государственных органов и организаций, наделенных полномочиями засекречивания информации, и общего объема государственных секретов с одновременной гарантированно эффективной защитой охраняемых сведений. При этом не допускается расширение или ужесточение режимных мер, не обусловленное системными недостатками в сфере защиты государственных секретов, повлекшими вредные последствия.

85. Возникает необходимость адаптации института тайн к развитию информатизации. Наряду с организационно-правовыми мерами обеспечения безопасности информации возрастает роль ее защиты и техническими методами. В области технических и криптографических методов защиты государственных секретов максимально учитываются имеющиеся сведения о средствах, методах, технологиях получения несанкционированного доступа к защищаемым информационным ресурсам, результаты оперативно-розыскной и контрразведывательной деятельности, научных исследований и опытных разработок, а также всесторонние знания в области современных ИКТ и особенности обстановки в сфере национальной безопасности.

Государственные органы, наделенные полномочиями по определению порядка защиты государственных секретов от утечки по техническим каналам, обеспечивают его адекватность и соразмерность возможным рискам.

## ГЛАВА 23
## БЕЗОПАСНОСТЬ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

86. В соответствии с нормативными правовыми актами Республики Беларусь осуществляются формирование и защита служебной информации ограниченного распространения, а также защита информации, составляющей коммерческую, профессиональную, банковскую и иную охраняемую законом тайну, информации о частной жизни физического лица, персональных данных, иной информации, доступ к которой ограничен законодательными актами Республики Беларусь.

87. В условиях физической невозможности и нецелесообразности полностью отделить информационные системы и ресурсы, содержащие эти данные, от сети Интернет и иных сетей общедоступного пользования физическим и юридическим лицам

необходимо предпринимать необходимые правовые, организационно-распорядительные и технические меры, обеспечивающие минимизацию количества киберинцидентов и вреда от них в этих системах.

88. Государство в свою очередь должно совершенствовать требования к защите информации, в том числе продолжать развитие системы подтверждения соответствия средств технической и криптографической защиты информации, а также лицензирования деятельности в области технической защиты информации.

89. Достижение защищенности персональных данных обеспечивает взвешенная государственная политика по определению требований к всевозможным субъектам информационных отношений, осуществляющим сбор, обработку и хранение этих данных.

Внимание государства сосредотачивается на совершенствовании нормативной правовой базы в данной области. Государственное регулирование сбора, обработки, предоставления и распространения персональных данных осуществляется с учетом современного международного опыта, в том числе согласуется с положениями межгосударственных актов. Формируемые в Беларуси подходы к защите персональных данных базируются на принципе «безопасность по умолчанию».

90. Важной мерой по усилению контроля в этой сфере является функционирование в государстве уполномоченного субъекта (субъектов) по защите прав физических лиц при обработке их персональных данных.

## ГЛАВА 24
## ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ И ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ

91. Государство обеспечивает защиту информационных ресурсов, находящихся в распоряжении государственных органов и организаций, осуществляет правовое регулирование пользования, владения и распоряжения информационными ресурсами. В этих целях создается единая система учета и сохранности информационных ресурсов, а также применяются специальные процедуры государственной регистрации.

92. Государственными органами осуществляется защита общедоступной информации от противоправного уничтожения, модификации, блокирования правомерного доступа, необоснованного засекречивания, сокрытия, несвоевременного распространения или предоставления. Государство обеспечивает запрет цензуры, гарантирует оперативное доведение общедоступной информации установленными законодательством способами, расширяет возможности соответствующих сервисов, реализует концепцию «открытых данных». Государство заинтересовано в поддержании баланса между потребностью граждан в ознакомлении с общедоступной информацией, их права на отказ от получения такой информации, а также необходимостью ее защиты от противоправных посягательств.

# РАЗДЕЛ VII
# МЕХАНИЗМЫ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

## ГЛАВА 25
## ИСПОЛЬЗОВАНИЕ ПОЛОЖЕНИЙ КОНЦЕПЦИИ ПРИ ПОДГОТОВКЕ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ И ИНЫХ ДОКУМЕНТОВ

93. Положения Концепции используются при подготовке нормативных правовых актов, государственных программ, перспективных и текущих планов работы государственных органов, в реализации проектов вовлеченных общественных организаций и инициатив граждан, а также при оценке состояния национальной безопасности и уточнении индикаторов этого состояния.

94. Разработка и осуществление мер в области обеспечения и укрепления информационной безопасности, согласующихся с настоящей Концепцией, основываются на научном обеспечении, включая фундаментальные и прикладные исследования, и результатах практической деятельности.

95. В области правового обеспечения информационной безопасности Концепция служит основой для специальных актов законодательства, определяющих правовое положение субъектов обеспечения информационной безопасности, регулирующих деятельность государственных органов по ее обеспечению, формулирующих нормы и правила правомерного поведения в информационной сфере, необходимые регламенты, ограничения и запреты, закрепляющих другие нормы по обеспечению безопасности информационной сферы и защищенности соответствующих интересов личности, общества и государства.

## ГЛАВА 26
## ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

96. Эффективному решению задач в обеспечении информационной безопасности должно способствовать постоянное целенаправленное взаимодействие между государственным сектором и коммерческими организациями в форме государственно-частного партнерства с целью привлечения компетенций, кадров, технологий, капитала частных предприятий, повышения отдачи использования бюджетных средств и активов предприятий, совместной разработки и реализации инвестиционных и иных проектов в области информационной безопасности.

97. Государственно-частное партнерство в области обеспечения информационной безопасности рассматривается как юридически оформленное сотрудничество государственного органа и субъекта хозяйственной деятельности негосударственной формы собственности, основанное на объединении ресурсов и распределении рисков, реализуемое для обеспечения информационной безопасности с привлечением частных инвестиций и компетенций.

98. Одним из важнейших направлений реализации государственно-частного партнерства в сфере обеспечения информационной безопасности является поддержка отечественных производителей программного обеспечения информационных систем и систем информационной безопасности.

Наряду с преодолением зависимости Беларуси от других стран – производителей программных и аппаратных средств реализация инфраструктурных проектов и проектов, напрямую связанных с обеспечением информационной безопасности через механизм партнерства государства и отечественных частных компаний, должна способствовать формированию рыночного спроса на импортозамещающую национальную информационно-технологическую продукцию, повышению ее качества.

99. Государство заинтересовано во взаимодействии с IT-компаниями, интернет-провайдерами, операторами связи и внешними экспертами в обновлении и развитии механизмов выявления угроз информационной безопасности через IT-аудит, мониторинг

киберрисков, поиск уязвимостей и актуальных средств защиты, выработку правил поведения в сети Интернет.

100. Государственно-частное партнерство способствует подготовке квалифицированных кадров в области информационной безопасности, формированию актуальных программ подготовки соответствующих специалистов, внедрению новых образовательных и профессиональных стандартов в данной сфере, а также повышению общей компьютерной грамотности населения, включая обучение людей старшего и среднего возраста компьютерным навыкам, правилам пользования персональными данными, умению безопасной работы в сети Интернет.

101. В связи с трансформацией общественных отношений в информационной сфере государственно-частное партнерство становится наиболее эффективной моделью обеспечения информационной безопасности. В ней государство определяет цели, стратегические задачи и регулятивные подходы, а бизнес-сообщество предоставляет технологии, знания и ресурсы для решения поставленных задач. При этом государство стремится гарантировать технологическую нейтральность и защиту частных организаций (и их инвестиций) от возможных рисков.

## ГЛАВА 27
## УЧАСТИЕ РЕСПУБЛИКИ БЕЛАРУСЬ В ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

102. Целью обеспечения международной информационной безопасности является выявление, предупреждение и нейтрализация внешних рисков, вызовов и угроз информационной безопасности. Международное сотрудничество в сфере информационной безопасности на региональном, двустороннем, многостороннем и глобальном уровнях направлено на снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии в отношении Беларуси.

103. В рамках обеспечения международной информационной безопасности осуществляется активное, всестороннее, взаимовыгодное международное, в том числе межведомственное, сотрудничество.

Обеспечивается участие Республики Беларусь в международных организациях, профильных международных договорах, двусторонних отношениях с иными государствами, в других формах межгосударственного сотрудничества в целях формирования механизмов международного взаимодействия по противодействию угрозам международной информационной безопасности.

104. Главным средством для достижения целей обеспечения международной информационной безопасности являются поддержка и продвижение соответствующих инициатив, отвечающих национальным интересам Республики Беларусь в информационной сфере.

Беларусь поддерживает продвижение мер доверия в сфере международной информационной безопасности и выступает за ответственное поведение государств в информационной сфере, которое предусматривало бы в первую очередь предотвращение в ней конфликтов, а не их урегулирование. Государства должны воздерживаться от целенаправленных деструктивных информационных воздействий на другие страны, исключать использование своей территории для осуществления кибератак, а также противодействовать использованию скрытых вредоносных функций и программных

уязвимостей в программно-аппаратных средствах, добиваясь их безопасности для пользователей.

105. Республика Беларусь принимает участие в международном информационном обмене на основе международных договоров и соглашений, в рамках юрисдикции – обеспечивает его безопасность.