РЕПУБЛИКА МОЛДОВЕНЯСКЭ
НИСТРЯНЭ

ПРИДНІСТРОВСЬКА МОЛДАВСЬКА
РЕСПУБЛІКА

ПРИДНЕСТРОВСКАЯ МОЛДАВСКАЯ
РЕСПУБЛИКА

ПРЕЗИДЕНТ

УКАЗ

Об утверждении Доктрины информационной безопасности
Приднестровской Молдавской Республики
на 2020 – 2026 годы

В соответствии со статьей 65 Конституции Приднестровской Молдавской Республики, Указом Президента Приднестровской Молдавской Республики от 12 декабря 2018 года № 460 «Об утверждении Стратегии развития Приднестровской Молдавской Республики на 2019 – 2026 годы» (САЗ 18-50), в целях координации деятельности органов государственной власти, органов местного самоуправления Приднестровской Молдавской Республики в сфере обеспечения информационной безопасности, а также выработки мер по совершенствованию системы обеспечения информационной безопасности Приднестровской Молдавской Республики,
п о с т а н о в л я ю:

1. Утвердить Доктрину информационной безопасности Приднестровской Молдавской Республики на 2020 – 2026 годы согласно Приложению к настоящему Указу.

2. Органам государственной власти и управления Приднестровской Молдавской Республики в течение 60 (шестидесяти) дней со дня вступления в силу настоящего Указа:

а) разработать и направить на утверждение Президенту Приднестровской Молдавской Республики План мероприятий, направленный на реализацию Доктрины информационной безопасности Приднестровской Молдавской Республики на 2020 – 2026 годы;

б) привести свои нормативные правовые акты в соответствие с настоящим Указом;

в) ежегодно в срок до 15 декабря представлять в Администрацию Президента Приднестровской Молдавской Республики отчеты о выполнении планов мероприятий, направленных на реализацию Доктрины информационной безопасности Приднестровской Молдавской Республики на 2020 – 2026 годы.

3. Контроль за исполнением настоящего Указа возложить на Руководителя Администрации Президента Приднестровской Молдавской Республики.

4. Настоящий Указ вступает в силу со дня, следующего за днем официального опубликования.

ПРЕЗИДЕНТ В.КРАСНОСЕЛЬСКИЙ

г. Тирасполь
26 марта 2020 г.
№ 121

ПРИЛОЖЕНИЕ
к Указу Президента
Приднестровской Молдавской
Республики
от 26 марта 2020 года № 121

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИДНЕСТРОВСКОЙ МОЛДАВСКОЙ РЕСПУБЛИКИ НА 2020 – 2026 ГОДЫ

1. Общие положения

1. Настоящая Доктрина информационной безопасности Приднестровской Молдавской Республики на 2020 – 2026 годы (далее – Доктрина) представляет собой систему официальных взглядов на обеспечение информационной безопасности Приднестровской Молдавской Республики.

2. В настоящей Доктрине используются следующие основные понятия:

а) государственные интересы Приднестровской Молдавской Республики в информационной сфере (далее – государственные интересы в информационной сфере) – объективно значимые интересы государства, направленные на обеспечение государственной защиты интересов личности и общества в информационной сфере;

б) информационная безопасность Приднестровской Молдавской Республики (далее – информационная безопасность) – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

в) информационная инфраструктура Приднестровской Молдавской Республики (далее – информационная инфраструктура) – совокупность объектов информатизации, информационных систем, сайтов в глобальной сети Интернет и сетей электросвязи, расположенных на территории Приднестровской Молдавской Республики;

г) обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) сети электросвязи – технологические системы, обеспечивающие одну или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов сообщений, включая обмен информацией между электронными вычислительными машинами, телевизионное и радиовещание;

е) силы обеспечения информационной безопасности – органы государственной власти, органы местного самоуправления, государственные учреждения, а также должностные лица указанных органов и учреждений, уполномоченные на решение в соответствии с законодательством Приднестровской Молдавской Республики задач по обеспечению информационной безопасности;

ж) система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

з) средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

и) информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

к) угроза информационной безопасности Приднестровской Молдавской Республики (далее – информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба государственным интересам в информационной сфере.

3. Правовую основу настоящей Доктрины составляют Конституция Приднестровской Молдавской Республики, конституционные законы, законы, а также нормативные правовые акты Президента Приднестровской Молдавской Республики и Правительства Приднестровской Молдавской Республики.

4. Настоящая Доктрина разработана во исполнение Стратегии развития Приднестровской Молдавской Республики на 2019 – 2026 годы, утвержденной Указом Президента Приднестровской Молдавской Республики от 12 декабря 2018 года № 460 (САЗ 18-50).

5. Настоящая Доктрина является документом стратегического планирования в сфере обеспечения информационной безопасности Приднестровской Молдавской Республики.

6. Настоящая Доктрина служит основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также выработки мер по совершенствованию системы обеспечения информационной безопасности.

2. Государственные интересы в обеспечении информационной безопасности Приднестровской Молдавской Республики

7. Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой

информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Информационная структура, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Приднестровской Молдавской Республики, что подчеркивает её определяющую значимость для минимально необходимого уровня обеспечения государственной безопасности.

8. На основе государственных интересов в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики Приднестровской Молдавской Республики по обеспечению информационной безопасности.

9. Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических приоритетов Приднестровской Молдавской Республики.

10. Государственными интересами в информационной сфере являются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей народа Приднестровской Молдавской Республики;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры в мирное время, в чрезвычайных ситуациях, в период непосредственной угрозы агрессии и в военное время;

в) доведение до приднестровской и международной общественности достоверной информации о государственной политике Приднестровской Молдавской Республики и её официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения государственной безопасности Приднестровской Молдавской Республики;

г) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Приднестровской Молдавской Республики в информационной сфере.

11. Реализация государственных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также государственной безопасности Приднестровской Молдавской Республики.

3. Стратегические цели и задачи информационной безопасности Приднестровской Молдавской Республики

12. Стратегической целью обеспечения информационной безопасности в области:

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

б) государственной и общественной безопасности – являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Приднестровской Молдавской Республики, обеспечение основных прав и свобод человека и гражданина, а также защита информационной инфраструктуры;

в) экономики государства – является сведение к минимально возможному уровню влияния негативных факторов, обусловленных применением информационных технологий иностранных государств и негосударственных факторов, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности;

г) науки, технологий и образования – является инновационное и ускоренное развитие системы обеспечения информационной безопасности и отрасли информационных технологий, в том числе подготовка специалистов по направлению информационной безопасности;

д) стратегической стабильности и равноправного стратегического партнерства с зарубежными странами и международными организациями – является защита суверенитета Приднестровской Молдавской Республики в информационной сфере.

13. Сложившееся положение дел в области обеспечения информационной безопасности Приднестровской Молдавской Республики требует безотлагательного решения таких задач, как:

а) реализация основных направлений государственной политики в области обеспечения информационной безопасности Приднестровской

Молдавской Республики, а также разработка мероприятий и механизмов, направленных на реализацию данной политики с учетом современной геополитической ситуации, условий политического и социально-экономического развития республики;

б) развитие и совершенствование системы обеспечения информационной безопасности Приднестровской Молдавской Республики, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Приднестровской Молдавской Республики, а также системы противодействия этим угрозам;

в) разработка республиканских целевых программ обеспечения информационной безопасности Приднестровской Молдавской Республики;

г) совершенствование системы обеспечения информационной безопасности, а также разработка средств обеспечения информационной безопасности Приднестровской Молдавской Республики;

д) совершенствование нормативной правовой базы в целях обеспечения информационной безопасности Приднестровской Молдавской Республики;

е) совершенствование механизмов реализации прав граждан на получение информации и доступа к ней;

ж) координация деятельности органов государственной власти и управления, организаций независимо от формы собственности в области обеспечения информационной безопасности Приднестровской Молдавской Республики;

з) разработка механизмов реализации государственной информационной политики Приднестровской Молдавской Республики;

и) разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

к) разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, прежде всего используемых в системах управления войсками и оружием, охраны государственной границы, таможенной деятельности, экологически опасных и экономически важных производств;

л) развитие и совершенствование государственной системы защиты охраняемой законом информации и системы защиты государственной тайны;

м) создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях в период непосредственной угрозы агрессии и в военное время;

н) создание единой системы подготовки, переподготовки и повышения квалификации кадров в области информационной безопасности и информационных технологий;

о) оперативное реагирование на информационные вбросы, факты распространения провокационных и недостоверных сведений в социальных

сетях с последующим опубликованием опровержений, пояснений с обязательным комментарием компетентных в тех или иных областях уполномоченных специалистов, экспертов и их размещение на официальных страницах органов государственной власти и управления;

п) контроль защищенности информации, содержащейся в государственных информационных системах, путем:

1) выявления технических каналов утечки информации и способов несанкционированного доступа к ней;

2) контроля эффективности применяемых средств защиты информации;

р) проведения с сотрудниками органов государственной власти и управления лекций и семинаров, направленных на повышение уровня знаний о мерах информационной безопасности и их применении в рамках исполнения ими служебных и должностных обязанностей.

4. Угрозы и состояние информационной безопасности Приднестровской Молдавской Республики

14. Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы. При этом практика внедрения информационных технологий в отсутствие взаимосвязи с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

15. Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является усиление деятельности специальных служб иностранных государств, а также иных организаций или преступных элементов, осуществляющих техническую разведку, в целях получения доступа к защищаемой государством информации.

16. Расширяются масштабы использования специальными службами отдельных государств, а также иных организаций и преступных элементов средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в республике и приводящего к подрыву суверенитета и нарушению территориальной целостности Приднестровской Молдавской Республики.

В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

17. Различные террористические и экстремистские организации во всём мире широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников.

Такими организациями в противоправных целях активно создаются средства негативного воздействия на объекты информационной инфраструктуры.

18. Увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений постоянно совершенствуются.

19. По своей общей направленности угрозы информационной безопасности Приднестровской Молдавской Республики подразделяются на следующие виды:

а) угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному развитию общества республики;

б) угрозы информационному обеспечению государственной политики Приднестровской Молдавской Республики;

в) угрозы безопасности информационных систем и сетей электросвязи, как уже развернутых, так и создаваемых на территории Приднестровской Молдавской Республики.

20. Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному развитию общества Приднестровской Молдавской Республики могут являться:

а) противодействие, в том числе со стороны преступных сообществ, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

б) незаконное ограничение доступа к общественно необходимой информации;

в) неправомерное ограничение доступа граждан к открытым информационным ресурсам органов государственной власти, к открытым архивным материалам, к другой открытой социально значимой информации;

г) нарушение органами государственной власти, организациями и гражданами требований законодательства Приднестровской Молдавской Республики об информации, информационных технологиях и о защите информации;

д) дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы; нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

е) обесценивание духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в приднестровском обществе;

ж) манипулирование информацией (дезинформация, сокрытие или искажение информации);

з) распространение в информационной сфере искаженной, недостоверной и предвзятой информации, наносящей вред интересам Приднестровской Молдавской Республики.

21. Угрозами информационному обеспечению государственной политики Приднестровской Молдавской Республики могут являться:

а) блокирование деятельности государственных средств массовой информации по информированию приднестровской и зарубежной аудитории;

б) дефицит квалифицированных кадров, обеспечивающих информационную безопасность;

в) увеличение оттока за рубеж квалифицированных специалистов.

22. Угрозами безопасности информационных систем и сетей электросвязи, как уже развернутых, так и создаваемых на территории Приднестровской Молдавской Республики, являются угрозы, приводящие к нарушению целостности, доступности или конфиденциальности защищаемой государством информации. К ним относятся в том числе:

а) противоправные сбор и использование информации;

б) нарушение технологии обработки информации;

в) внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

г) разработка и распространение программ, нарушающих нормальное функционирование информационных систем и информационно-телекоммуникационных сетей, в том числе систем защиты информации;

д) уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, сетей электросвязи;

е) воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

ж) компрометация ключей и средств криптографической защиты информации;

з) утечка информации по техническим каналам;

и) внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти и управления, организаций независимо от формы собственности;

к) уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

л) перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

м) несанкционированный доступ к информации, находящейся в информационных системах;

н) нарушение законных ограничений на распространение информации.

23. Источники угроз информационной безопасности Приднестровской Молдавской Республики подразделяются на внешние и внутренние.

24. К внешним источникам угроз информационной безопасности Приднестровской Молдавской Республики относятся:

а) деятельность иностранных государственных, политических, экономических, религиозных, военных, разведывательных и информационных структур, препятствующая обеспечению информационной безопасности республики;

б) деятельность космических, воздушных, наземных технических и иных средств (видов) разведки иностранных государств;

в) разработка рядом иностранных государств концепций, предусматривающих создание средств опасного воздействия на информационные сферы других стран, нарушение нормального функционирования информационных систем и сетей электросвязи, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

25. К внутренним источникам угроз информационной безопасности Приднестровской Молдавской Республики относятся:

а) недостаточное финансирование мероприятий по обеспечению информационной безопасности Приднестровской Молдавской Республики;

б) тяжелое экономическое положение республики;

в) отсутствие технических средств защиты между специализированными абонентскими устройствами органов государственной власти и управления;

г) нарушение установленных требований, регламентирующих сбор, обработку, хранение и передачу информации;

д) сбои в работе технических средств и программном обеспечении.

26. В оборонной сфере наибольшую опасность с точки зрения информационной безопасности представляют:

а) все виды разведывательной деятельности иностранных государств;

б) информационно-техническое воздействие (методы радиоэлектронной борьбы, проникновение в компьютерные сети и иное) со стороны вероятных противников;

в) психологические операции вероятных противников, осуществляемые специальными методами и через деятельность средств массовой информации, сеть Интернет и мобильные приложения;

г) возможность нарушения установленных регламентов сбора, обработки, передачи и хранения информации в структурных подразделениях Министерства обороны Приднестровской Молдавской Республики;

д) объективная возможность преднамеренных действий и непреднамеренных ошибок персонала информационных систем специального назначения;

е) вероятность отказов в работе технических средств и сбоя программного обеспечения в информационных системах специального назначения.

27. В сфере государственной и общественной безопасности наибольшую опасность с точки зрения информационной безопасности представляют:

а) экстремистская деятельность, а также иная деятельность, направленная на подрыв суверенитета, политической и социальной стабильности, насильственное изменение конституционного строя, нарушение территориальной целостности Приднестровской Молдавской Республики;

б) чрезвычайные ситуации, вызванные информационно-техническим воздействием на информационную инфраструктуру;

в) утрата, разглашение, а также хищение сведений, составляющих государственную тайну, и иной информации ограниченного доступа;

г) разведывательная деятельность специальных служб иностранных государств, международных сообществ иных организаций и преступных элементов, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений, органов внутренних дел и государственной службы безопасности Приднестровской Молдавской Республики, а также деятельность, направленная на получение несанкционированного доступа к их информационным системам.

28. В сфере экономики наибольшую опасность с точки зрения информационной безопасности представляют хищения и преднамеренное искажение информации, возможность которых связана с преднамеренным или случайным нарушением технологии работы с информацией, несанкционированным доступом к ней, что обусловлено недостаточными мерами защиты информации. Такая же опасность существует в органах, занятых формированием и распространением информации о внешнеэкономической деятельности.

Серьезную опасность для нормального функционирования сферы экономики в целом представляют преступления в сфере компьютерной информации (подлоги, хищения и другое), связанные с проникновением преступных элементов в информационные системы и информационно-телекоммуникационные сети.

29. В области науки и техники специфика угроз информационной безопасности состоит в их многообразии, сложности идентификации, поскольку, как правило, они носят уникальный или индивидуальный характер. При классификации угроз в этой области необходимо уделять особое внимание изучению возможности осуществления промышленного шпионажа специальными службами иностранных государств иных организаций и преступных элементов. Реальный путь противодействия угрозам со стороны государства заключается в постоянном совершенствовании законодательства в этой области и механизмов его реализации. Многие мероприятия по предотвращению или нейтрализации угроз в этой области, особенно в части, касающейся научных кадров, лежат в сфере социальной и экономической политики государства.

30. В области стратегической стабильности и равноправного стратегического партнерства с иностранными государствами и международными организациями наибольшую опасность с точки зрения

информационной безопасности представляет подрыв суверенитета Приднестровской Молдавской Республики в информационной сфере.

31. Состояние информационной безопасности в области обороны республики в настоящее время характеризуется применением враждебно настроенными государствами и организациями информационных технологий в военно-политических целях, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Приднестровской Молдавской Республики.

32. Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объектах информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Приднестровской Молдавской Республики, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Приднестровской Молдавской Республики.

33. Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем защиты информации, циркулирующей в органах государственной власти, на которые возложено исполнение функций по обеспечению экономического развития республики.

34. Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, зачастую не имеют комплексной основы.

35. Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационной сфере.

5. Система обеспечения информационной безопасности Приднестровской Молдавской Республики

36. Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной ветвей власти в данной сфере с учетом предметов ведения органов государственной власти, а также органов местного самоуправления, определяемых законодательством Приднестровской Молдавской Республики в области обеспечения безопасности.

37. Состав системы обеспечения информационной безопасности определяется Президентом Приднестровской Молдавской Республики.

38. Организационную основу системы обеспечения информационной безопасности составляют органы государственной власти Приднестровской Молдавской Республики, центральный банк Приднестровской Молдавской Республики, органы местного самоуправления Приднестровской Молдавской Республики, принимающие, в соответствии с законодательством Приднестровской Молдавской Республики, участие в решении задач по обеспечению информационной безопасности.

39. Участниками системы обеспечения информационной безопасности являются: собственники объектов информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы электросвязи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей электросвязи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Приднестровской Молдавской Республики участвуют в решении задач по обеспечению информационной безопасности.

40. Деятельность органов государственной власти и управления Приднестровской Молдавской Республики по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанных на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие органов государственной власти и управления, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном доступе, обмене информацией и ограничениями, связанными с необходимостью обеспечения информационной безопасности Приднестровской Молдавской Республики;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Приднестровской Молдавской Республики, а также законодательства Приднестровской Молдавской Республики.

41. Задачами органов государственной власти Приднестровской Молдавской Республики в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-розыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

42. Задачами органов государственной власти и управления в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам;

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия органов государственной власти, органов местного самоуправления, государственных учреждений, организаций и граждан при решении задач по обеспечению информационной безопасности.

43. Компетенция органов государственной власти, органов местного самоуправления Приднестровской Молдавской Республики и государственных учреждений, входящих в состав системы обеспечения информационной безопасности Приднестровской Молдавской Республики, определяется законами, нормативными правовыми актами Президента и Правительства Приднестровской Молдавской Республики.

6. Основные направления обеспечения информационной безопасности Приднестровской Молдавской Республики

44. В соответствии с военной политикой Приднестровской Молдавской Республики основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) совершенствование системы обеспечения информационной безопасности Вооруженных сил Приднестровской Молдавской Республики, других войск, воинских формирований и органов;

б) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным силам Приднестровской Молдавской Республики в информационной сфере;

в) развитие защищенных, засекреченных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

г) совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы.

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

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Приднестровской Молдавской Республики;

б) пресечение деятельности, наносящей ущерб государственной безопасности Приднестровской Молдавской Республики, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, общественными или иными организациями или отдельными преступными элементами;

в) повышение защищенности информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий страны от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия органов государственной власти и управления, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности государственных

информационных систем и сети электросвязи, а также обеспечение безопасности информации, передаваемой, обрабатываемой и хранящейся в них;

д) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

е) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

ж) повышение эффективности информационного обеспечения реализации государственной политики Приднестровской Молдавской Республики.

46. Обеспечение информационной безопасности Приднестровской Молдавской Республики в сфере экономики играет ключевую роль в обеспечении государственной безопасности Приднестровской Молдавской Республики.

Основными направлениями обеспечения информационной безопасности в экономической сфере являются:

а) создание благоприятных условий для инновационного развития отрасли информационных технологий;

б) ликвидация зависимости от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания и развития отечественных разработок, а также производства продукции и оказания услуг на их основе.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением преступных элементов в компьютерные системы и сети банков и иных кредитных организаций.

Существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и её искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и органов государственной власти и управления, занятых формированием и распространением информации о внешнеэкономической деятельности Приднестровской Молдавской Республики.

47. Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются:

а) создание и внедрение информационных технологий и продуктов, имеющих определенную степень устойчивости к воздействию различного рода угроз;

б) проведение научных исследований и осуществление опытных разработок в целях создания перспективных информационных технологий и средств обеспечения информационной безопасности;

в) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

г) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

48. Основным направлением обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является защита суверенитета Приднестровской Молдавской Республики в информационной сфере посредством осуществления самостоятельной и независимой политики, направленной на реализацию государственных интересов в информационной сфере.