КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ ТАДЖИКИСТАН

ПРЕЗИДЕНТ РЕСПУБЛИКИ ТАДЖИКИСТАН

УКАЗ

"О КОНЦЕПЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ ТАДЖИКИСТАН"

В целях формирования и развития государственной политики в области обеспечения информационной безопасности Республики Таджикистан постановляю:

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

2. Правительству Республики Таджикистан в трехмесячный срок:

- разработать и утвердить Программу обеспечения информационной безопасности Республики Таджикистан;

- принять необходимые меры по организационному и финансовому обеспечению реализации данной Концепции;

- привести свои решения в соответствии с настоящим Указом.

3. Контроль за ходом выполнения настоящего Указа возложить на Совет безопасности Республики Таджикистан.

Президент
Республики Таджикистан Э. Рахмонов

г.Душанбе 7 ноября 2003 года №1175

УТВЕРЖДЕНА

Указом Президента
Республики Таджикистан
от 7 ноября 2003 года №1175

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ ТАДЖИКИСТАН

Концепция информационной безопасности Республики Таджикистан представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Республики Таджикистан.
Настоящая Концепция служит основой для:

- формирования государственной политики в области обеспечения национальной информационной безопасности Республики Таджикистан;

- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения национальной информационной безопасности Республики Таджикистан;

- разработки целевых программ обеспечения информационной безопасности Республики Таджикистан.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ ТАДЖИКИСТАН

1.1. Национальные интересы Республики Таджикистан в информационной сфере и их обеспечение

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной структуры, осуществляющей сбор, формирование, распространение и использование информации, а также составляющей систему регулирования возникающих при этом общественных отношений. Информационная сфера является системообразующим фактором жизни общества.

Она активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности Республики Таджикистан, которая существенным образом зависит от обеспечения информационной безопасности.

Под информационной безопасностью Республики Таджикистан понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании демократического, правового, светского и унитарного государства, достижении и поддержании общественного согласия, в духовном обновлении Таджикистана.

Интересы государства в информационной сфере заключаются в создании условий для гармонического развития информационной инфраструктуры, которая направлена на реализацию конституционных прав и свобод человека и гражданина в области получения

информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности Республики Таджикистан, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Республики Таджикистан в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Под источниками угрозы информационной безопасности понимаются, в частности, стремление потенциальных противников к ущемлению интересов Республики Таджикистан в мировом информационном пространстве, вытеснении ее с внешнего и внутреннего рынков, обострение международной конкуренции за обладание информационно-техническими ресурсами.

Выделяются четыре основные составляющие национальных интересов Республики Таджикистан в информационной сфере.

Первая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления республики, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется:

- повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации общества, духовного возрождения народа Таджикистана;

- усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Республики Таджикистан;

- обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

- обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;

- укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных законодательством ограничений на доступ к конфиденциальной информации;

- гарантировать свободу массовой информации и запрет цензуры;

- не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

- обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен законодательством.

Вторая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя информационное обеспечение государственной политики, связанное с доведением до народа Таджикистана и международной общественности достоверной информации о государственной политике Республики Таджикистан, ее официальной позиции по социально значимым событиям Республики и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

- укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до граждан республики и иностранных граждан;

- интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.
Третья составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя применение современных информационных технологий, создание отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.
Для достижения этого требуется:

- развивать и совершенствовать инфраструктуру единого информационного пространства Республики Таджикистан;

- создать отечественную индустрию информационных услуг, аппаратных и программных средств защиты информации и методов контроля за их эффективностью и повышать эффективность использования государственных информационных ресурсов;

- обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов Республики Таджикистан в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории Республики Таджикистан.

В этих целях необходимо:

- повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем органов государственной власти и управления Республики Таджикистан, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооруженных сил и военной техники, систем управления войсками и оружием;

- обеспечить защиту сведений, составляющих государственную тайну;

- расширять международное сотрудничество Республики Таджикистан в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

1.2. Виды угроз информационной безопасности Республики Таджикистан
По своей общей направленности угрозы информационной безопасности Республики Таджикистан подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению Республики Таджикистан;

- угрозы созданию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории республики.
Такими угрозами могут являться:

- принятие органами государственной власти и управления нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

- создание монополий на формирование, получение и распространение информации в Республике Таджикистан, в том числе с использованием телекоммуникационных систем;

- нерациональное чрезмерное ограничение доступа к общественно необходимой информации;

- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

- неисполнение органами государственной власти и управления организациями и гражданами требований законодательства, регулирующего, отношения в информационной сфере;

- неправомерное ограничение доступа граждан к открытым информационным ресурсам органов государственной власти и управления Республики Таджикистан, к открытым архивным материалам, к другой открытой социально значимой информации;

- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

- вытеснение таджикских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни республики от зарубежных информационных структур;

- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в таджикском обществе;

- снижение духовного, нравственного и творческого потенциала населения Таджикистана, что существенно осложняет подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

- манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики
Республики Таджикистан могут являться:

- монополизация информационного рынка Таджикистана, его отдельных секторов отечественными и зарубежными информационными структурами;

- блокирование деятельности государственных средств массовой информации по информированию таджикской и зарубежной аудитории;

- низкая эффективность информационного обеспечения государственной политики Республики Таджикистан вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами созданию и развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции, а также обеспечению накопления, сохранности и эффективного использования зарубежных и отечественных информационных ресурсов могут являться:

- противодействие доступу Республики Таджикистан к новейшим информационным технологиям, а также создание условий для усиления технологической зависимости Таджикистана в области современных информационных
технологий;

- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи с отсутствием отечественных аналогов;

- отток за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, внедряемых, так и создаваемых на территории Республики Таджикистан, могут являться:

- противоправные сбор и использование информации;

- нарушения технологии обработки информации;

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

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

- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

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

- компрометация ключей и средств криптографической защиты информации;

- утечка информации по техническим каналам;

- внедрение электронных устройств для перехвата информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

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

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

- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии таджикской информационной инфраструктуры;

- несанкционированный доступ к информации, находящейся в банках и базах данных;

- нарушение законных ограничений на распространение информации.

1.3. Источники угроз национальной информационной безопасности Республики Таджикистан.

Источники угроз национальной информационной безопасности Республики Таджикистан подразделяются на внешние и внутренние. К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Республики Таджикистан в информационной сфере:

- стремление стран потенциальных противников к ущемлению интересов Таджикистана в мировом информационном пространстве, вытеснению его с внешних информационных рынков;

- обострение международной конкуренции за обладание информационными технологиями и ресурсами;

- деятельность международных террористических организаций;

- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных информационных технологий в развивающихся странах;

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

- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;

- недостаточная координация деятельности органов государственной власти Республики Таджикистан по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Республики Таджикистан;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

- неразвитость институтов гражданского общества и недостаточный государственной контроль за развитием информационного рынка Республики Таджикистан;

- недостаточное финансирование мероприятий по обеспечению информационной безопасности Республики Таджикистан;

- недостаточная экономическая мощь государства;

- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

- недостаточная активность органов государственной власти и управления в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

- отставание Республики Таджикистан от других стран мира по уровню информатизации органов государственной власти и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, экологии, сферы услуг и быта граждан.

1.4. Состояние информационной безопасности Республики Таджикистан и основные задачи по ее обеспечению.

За последние годы в Республике Таджикистан реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности. Начато и продолжается формирование и совершенствование базы правового обеспечения информационной безопасности. Приняты Законы Республики Таджикистан "О государственной тайне", "О печати и других СМИ", "О телевидении и радиовещании", "Об издательском деле", "О связи", "Об авторских и смежных правах", "Об информатизации", "Об архивном фонде и архивных учреждениях", "Об информации" и "О защите информации".

Осуществляются мероприятия по обеспечению информационной безопасности в органах государственной власти Республики Таджикистан, на предприятиях, в учреждениях и организациях независимо от форм собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Республики Таджикистан способствуют государственная система защиты информации, система защиты государственной тайны, система лицензирования деятельности в области защиты государственной тайны.

Вместе с тем анализ состояния информационной безопасности Республики Таджикистан показывает, что ее уровень не в полной мере соответствует потребностям общества и безопасности государства. Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Республики Таджикистан конкурентоспособных информационных агентств и средств массовой информации.
Недостаточная обеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.
Закрепленные в Конституции Республики Таджикистан права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки все еще не имеют в полной мере достаточного правового, организационного и технического обеспечения.
Неудовлетворительно организована защита собираемых органами государственной власти и управления Республики Таджикистан данных о физических лицах (персональных данных).

Нет четкости при проведении государственной политики в области формирования таджикского информационного обмена и интеграции информационного пространства Республики Таджикистан в мировое информационное пространство, что создает условия для вытеснения таджикских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

Недостаточна информационная поддержка, деятельности таджикских информационных агентств по продвижению их продукции на зарубежный информационный рынок.
Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

Отсутствие отечественных информационных технологий вынуждает органы государственной власти и управления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость Республики Таджикистан от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также широким применением открытых информационных систем возросли угрозы применения информационного оружия против информационной инфраструктуры Республики Таджикистан. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании.

Сложившееся положение дел в области обеспечения информационной безопасности Республики Таджикистан требует безотлагательного решения таких задач, как:

- разработка основных направлений государственной политики в области беспечения информационной безопасности Республики Таджикистан, а также мероприятий и механизмов, (например, создание соответствующего государственного органа, отвечающего непосредственно за обеспечение информационной безопасности Республики Таджикистан), связанных с реализацией этой политики;

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

- разработка целевых программ обеспечения информационной безопасности Республики Таджикистан;

- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Республики Таджикистан, а также сертификации этих систем и средств;

- совершенствование нормативной правовой базы обеспечения информационной безопасности Республики Таджикистан, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;

- установление ответственности должностных лиц, органов государственной власти и управления Республики Таджикистан, юридических лиц и граждан за соблюдение требований информационной безопасности;

- координация деятельности органов государственной власти, предприятий, учреждений и организаций независимо от форм собственности в области обеспечения информационной безопасности Республики Таджикистан;

- развитие научно-практических основ обеспечения информационной безопасности Республики Таджикистан с учетом современной геополитической ситуации, условий политического и социально-экономического развития Республики Таджикистан и реальности угроз применения "информационного оружия";

- разработка и создание механизмов формирования и реализации государственной информационной политики Республики Таджикистан;

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

- технологическое обеспечение Республики Таджикистан в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в сфере вооруженных сил;

- разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и, прежде всего, используемых в системах управления войсками, экономически важными производствами;

- развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

- создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения защиты информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;

- обеспечение условий для активного развития информационной инфраструктуры, участия Республики Таджикистан в процессах создание и использования глобальных информационных сетей и систем;

- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

II. МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ ТАДЖИКИСТАН

II.1. Общие методы обеспечения информационной безопасности Республики Таджикистан

Общие методы обеспечения информационной безопасности Республики Таджикистан разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Республики Таджикистан относятся разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Республики Таджикистан. Наиболее важными направлениями этой деятельности являются:

- внесение изменений и дополнений в законодательство Республики Таджикистан, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Республики Таджикистан;

- устранение внутренних противоречий в законодательстве Республики Таджикистан, а также в целях конкретизации правовых норм, устанавливается ответственность за правонарушения в области обеспечения информационной безопасности Республики Таджикистан;

- разработка и принятие нормативно-правовых актов Республики Таджикистан, устанавливающих ответственность юридических и

физических лиц за несанкционированный доступ к информации, её противоправные копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации;

- уточнение статуса иностранных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры Республики Таджикистан;

- законодательное закрепление приоритетов развития национальных сетей связи;

- определение статуса организации, предоставляющей услуги глобальных, информационно-телекоммуникационных сетей на территории Республики Таджикистан, и правовое регулирование деятельности этих организаций;

- создание правовой базы для формирования в Республике Таджикистан региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Республики Таджикистан является:

- создание и совершенствование системы обеспечения информационной безопасности Республики Таджикистан;

- усиление правоприменительной деятельности органов исполнительной власти, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развития защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при её хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;

- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

- контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Республики Таджикистан;

- формирование системы мониторинга показателей и характеристики информационной безопасности Республики Таджикистан в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности включают в себя:

- разработку программ обеспечения информационной безопасности Республики Таджикистан и определение порядка их финансирования;

- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

II.2. Особенности обеспечения информационной безопасности Республики Таджикистан в различных сферах общественной жизни.

Информационная безопасность Республики Таджикистан является одной из составляющих национальной безопасности Республики Таджикистан и оказывает влияние на защищенность национальных интересов Республики Таджикистан в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Республики Таджикистан и методы её обеспечения являются общими для этих сфер.

В каждой из них имеются свои особенности обеспечения информационной безопасности, связанные со спецификой объектов обеспечения безопасности, степенью их уязвимости в отношении угроз информационной безопасности Республики Таджикистан. В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Республики Таджикистан могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние информационной безопасности Республики Таджикистан.
В сфере экономики.

Обеспечение информационной безопасности Республики Таджикистан в сфере экономики играет ключевую роль в обеспечении национальной безопасности Республики Таджикистан.

Воздействию угроз информационной безопасности Республики Таджикистан в сфере экономики наиболее подвержены:

- система государственной статистики;

- кредитно-финансовая система;

- информационные и учетные автоматизированные системы подразделений органов государственной власти, обеспечивающих деятельность общества и государства в сфере экономики;

- системы бухгалтерского учета предприятий, учреждений и организаций не зависимо от формы собственности;

- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от форм собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем рынке товаров и услуг множества отечественных и зарубежных коммерческих структур-производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности Республике Таджикистан в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к экономической информации и для контроля за процессами её передачи и обработки со стороны иностранных спецслужб.

Отсутствие предприятий национальных отраслей промышленности, разрабатывающих и производящих средства информатизации, телекоммуникации, связи и защиты информации, приводит к широкому использованию соответствующих импортных средств, что создает угрозу возникновения технологической зависимости Республики Таджикистан от иностранных государств.

Серьезную угрозу для нормального функционирования экономики в целом представляют компьютерные преступления, связанные с проникновением криминальных элементов в компьютерные системы и сети банков и иных кредитных организаций. Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостоверность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и тому подобном, препятствует нормальному функционированию хозяйствующих субъектов. В то же время существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации наиболее опасны противоправное копирование информации и ее искажение вследствие преднамеренных или случайных нарушений технологии работы с информацией, несанкционированного доступа к ней. Это касается и органов государственной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Республики Таджикистан.

Основными мерами по обеспечению информационной безопасности Республики Таджикистан в сфере экономики являются:

- организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;

- разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

- разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация этих систем, а также разработка нормативной правовой базы, регламентирующей ее использование;

- совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

- совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

В сфере внутренней политики наиболее важными объектами обеспечения информационной безопасности Республики Таджикистан в сфере внутренней политики являются:

- конституционные права и свободы человека и гражданина:

- конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальная целостность Республики Таджикистан;

- открытые информационные ресурсы органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Республики Таджикистан:

- нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

- недостаточное правовое регулирование отношений в области прав
различных политических сил на использование средств массовой информации для пропаганды своих идей;

- распространение дезинформации о политике Республики Таджикистан, деятельности органов государственной власти, событиях, происходящих в стране и за рубежом;

- деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности Республики Таджикистан, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями в области обеспечения информационной безопасности Республики Таджикистан в сфере внутренней политики являются:

- создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

- активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике Таджикистана.

В сфере внешней политики.

К наиболее важным объектам обеспечения информационной безопасности Республики Таджикистан в сфере внешней политики относятся:

- информационные ресурсы органов государственной власти, реализующих внешнюю политику Республики Таджикистан, его представительств и организаций за рубежом, представительств Республики Таджикистан при международных организациях;

- информационные ресурсы представительств органов государственной власти, реализующих внешнюю политику Республики Таджикистан на территории Республики Таджикистан;

- информационные ресурсы таджикских предприятий, учреждений и организаций, реализующих внешнюю политику Республики Таджикистан;

- блокирование деятельности отечественных средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Республики Таджикистан, ее мнения по социально значимым событиям внутренней и международной жизни.

Из внешних угроз информационной безопасности Республики Таджикистан в сфере внешней политики наибольшую опасность представляют:

- информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики Республики Таджикистан;

- распространение за рубежом дезинформации о внешней политике Республики Таджикистан;

- нарушение прав таджикских граждан и юридических лиц в информационной сфере за рубежом;

- попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную инфраструктуру органов государственной власти, реализующих внешнюю политику Республики Таджикистан, таджикских представительств и организаций за рубежом, представительств Республики Таджикистан при международных организациях.

Из внутренних угроз информационной безопасности Республики Таджикистан в сфере внешней политики наибольшую опасность представляют:

- нарушение установленного порядка сбора, обработки, хранения и передачи информации в органах государственной власти, реализующих внешнюю политику Республики Таджикистан, и подведомственных им предприятий, учреждений и организаций;

- информационно-пропагандистская деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающая стратегию и тактику внешнеполитической деятельности Республики Таджикистан;

- недостаточная информированность населения о внешнеполитической деятельности Республики Таджикистан.

Основными мероприятиями по обеспечению информационной безопасности Республики Таджикистан в сфере внешней политики являются:

- разработка основных направлений государственной политики в области совершенствования информационного обеспечения внешнеполитического курса Республики Таджикистан; разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры органов государственной власти, реализующих внешнюю политику Республики Таджикистан, таджикских представительств и организаций за рубежом, представительств Республики Таджикистан при международных организациях;

- создание таджикским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике Республики Таджикистан;

- совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод граждан и юридических лиц Республики Таджикистан за рубежом;

- совершенствование информационного обеспечения субъектов Республики Таджикистан по вопросам внешнеполитической деятельности, которые
входят в их компетенцию.

В области науки и техники

Наиболее важными объектами обеспечения информационной безопасности Республики Таджикистан в области науки и техники являются:

- результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу Республики Таджикистан;

- открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;

- научно-технические кадры и система их подготовки.

К числу основных внешних угроз информационной безопасности Республики Таджикистан в области науки и техники следует отнести:

- стремление иностранных государств получить противоправный доступ к научно-техническим ресурсам Таджикистана для использования полученных таджикскими учеными результатов в собственных интересах;

- создание льготных условий на отечественном рынке для иностранной научно-технической продукции и стремление некоторых стран в то же время ограничить развитие научно-технического потенциала Таджикистана (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и тому подобное);

- политику некоторых стран, направленную на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств-участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных, наиболее перспективных научных коллективов;

- активизацию деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К числу основных внутренних угроз информационной безопасности Республики Таджикистан в области науки и техники следует отнести:

- сохраняющуюся сложную экономическую ситуацию, ведущую к резкому снижению финансирования научно-технической деятельности, временному падению престижа научно-технической сферы, утечке за рубеж идей и передовых разработок;

- неспособность предприятий национальных отраслей промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости Таджикистана от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при
создании и развитии в Таджикистане информационной структуры;

- серьезные проблемы в области патентной защиты результатов научно-технической деятельности отечественных ученых;

- сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности Республики Таджикистан в области науки и техники - это совершенствование законодательства Республики Таджикистан, регулирующего отношения в данной области, и механизмов его реализации. В этих целях государство должно способствовать созданию системы оценки возможного ущерба от реализации угроз наиболее важным объектам обеспечения информационной безопасности Республики Таджикистан в области науки и техники, включая общественные научные советы и организации независимой экспертизы, вырабатывающие рекомендации для органов государственной власти Республики Таджикистан по предотвращению противоправного или неэффективного использования интеллектуального потенциала Таджикистана.

В сфере духовной жизни.

Обеспечение информационной безопасности Республики Таджикистан в сфере духовной жизни имеет целью защиту конституционных прав и свобод человека и гражданина, связанных с развитием, формированием и поведением личности, свободой массового информирования, использования культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни, с сохранением культурного достояния народа Таджикистана, реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества, традиций патриотизма и гуманизма, здоровья граждан, культурного и научного потенциала Республики Таджикистан, обеспечения обороноспособности и безопасности государства.

**К числу основных объектов обеспечения информационной безопасности
Республики Таджикистан в сфере духовной жизни относятся:**

- достоинство личности, свобода совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, свобода мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду), а также свобода литературного, художественного, научного, технического и других видов творчества,преподавания;

- свобода массовой информации;

- неприкосновенность частной жизни, личная и семейная тайна;

- таджикский язык как фактор духовного единения и возрождения народа многонационального Таджикистана, и русский язык как язык межнационального общения и межгосударственного общения народов государств-участников Содружества Независимых Государств;

- языки, нравственные ценности и культурное наследие народностей и национальных меньшинств Республики Таджикистан;

- объекты интеллектуальной собственности.

Наибольшую опасность в сфере духовной жизни представляют следующие угрозы информационной безопасности Республики Таджикистан:

- деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных средств массовой информации в отечественном информационном пространстве;

- ухудшение состояния и постепенный упадок объектов таджикского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;

- возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

- использование зарубежными специальными службами средств массовой информации, действующих на территории Республики Таджикистан, для нанесения ущерба обороноспособности страны и безопасности государства, распространения дезинформации;

неспособность современного гражданского общества Таджикистана обеспечить формирование у подрастающего поколения и поддержание в обществе общественно необходимых нравственных ценностей, патриотизма и гражданской ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности Республики Таджикистан в сфере духовной жизни являются:

- развитие в Таджикистане основ гражданского общества;

- создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;

- выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей, отвечающих национальным интересам страны, воспитанием патриотизма и гражданской ответственности за ее судьбу; совершенствование законодательства Республики Таджикистан, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;

- государственная поддержка мероприятий по сохранению и возрождению культурного наследия народа и национальных меньшинств Республики Таджикистан;

- формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;

- разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности органов государственной власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

- разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки;

- сохранение культурных и исторических ценностей народа Таджикистана, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние;

- введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;

- противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

В общегосударственных информационных и телекоммуникационных системах
Основными объектами обеспечения информационной безопасности Республики Таджикистан в общегосударственных информационных и телекоммуникационных системах являются:

- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

- технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации;

- помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения

ограниченного доступа.

Основными угрозами информационной безопасности Республики Таджикистан в общегосударственных информационных и телекоммуникационных системах являются:

- деятельность специальных служб иностранных государств, преступных сообществ, организаций и групп, противозаконная деятельность отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем;

- вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;

- нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

- использование не сертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;

- привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Основными направлениями обеспечения информационной безопасности Республики Таджикистан в общегосударственных информационных и телекоммуникационных системах являются:

- предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

- исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

- предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

- предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

- обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;

- обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;

- выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах являются:

- лицензирование деятельности организаций в области защиты информации;

- аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;

- сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;

- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

- создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

В сфере обороны.

К объектам обеспечения нформационной безопасности Республики Таджикистан в сфере обороны относятся:

- информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Республики Таджикистан и родов войск, воинских частей и организаций, входящих в Вооруженные Силы Республики Таджикистан, научно-исследовательских и образовательных учреждений Министерства обороны Республики Таджикистан;

- информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

- программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

- информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности Республики Таджикистан в сфере обороны, являются:

- все виды разведывательной деятельности зарубежных государств;

- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;

- деятельность иностранных политических, экономических и военных структур, направленная против интересов Республики Таджикистан в сфере обороны.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны Республики Таджикистан, на предприятиях оборонного комплекса;

- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;

- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;

- возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил Республики Таджикистан и их боеготовность;

- нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;

- нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Перечисленные внутренние угрозу будут представлять особую опасность в условиях обострения военно-политической обстановки.

Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности Республики Таджикистан в сфере обороны являются:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;

- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;

- постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

- совершенствование структуры функциональных органов системы обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;

- совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;

- подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

В правоохранительной и судебной сферах

К наиболее важным объектам обеспечения информационной безопасности в правоохранительной и судебной сферах относятся:

- информационные ресурсы органов государственной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

- информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

- информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах, являются:

- разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Республики Таджикистан;

- деятельность иностранных государственных и частных коммерческих
структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

- недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

- отсутствие единой методологии сбора, обработки и хранения информации оперативно-розыскного, справочного, криминалистического и статистического характера;

- отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

- преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.
Наряду с широко используемыми общими методами и средствами защиты информации применяются также специфические методы и средства обеспечения информационной безопасности в правоохранительной и судебной сферах.

Главными из них являются:

- создание защищенной многоуровневой системы интегрированных банков данных оперативно-розыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;

- повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

В условиях чрезвычайных ситуаций.

Наиболее уязвимыми объектами обеспечения информационной безопасности Республики Таджикистан в условиях чрезвычайных ситуаций являются система принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций.

Особое значение для нормального функционирования указанных объектов имеет обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях. Сокрытие, задержка поступления, искажение и разрушение оперативной информации, несанкционированный доступ к ней отдельных лиц или групп лиц могут привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях:

- к приведению в движение больших масс людей, испытывающих психический стресс;

- к быстрому возникновению нераспространению среди них паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий направлениям обеспечения информационной безопасности относятся:

- разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;

- совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, об усло