|  |  |
| --- | --- |
|  | Приложение  к распоряжению Правительства  Рязанской области  от 14.01.2021 № 4-р |

КОНЦЕПЦИЯ

защиты информации в исполнительных органах   
государственной власти Рязанской области на 2021-2025 годы

г. Рязань

2021 год

Введение

Концепция защиты информации в исполнительных органах государственной власти Рязанской области на 2021-2025 годы (далее - Концепция) представляет собой систему взглядов на содержание проблемы защиты информации, а также задачи, принципы, основные направления развития и совершенствования системы защиты информации в этих органах.

Правовую основу Концепции составляют: Конституция Российской Федерации, федеральные законы и иные нормативные правовые акты Российской Федерации в сфере защиты информации, а также международные договоры и соглашения, заключенные или признанные Российской Федерацией, определяющие права, обязанности и ответственность граждан, общества и государства в информационной сфере.

Настоящая Концепция детализирует Доктрину информационной безопасности Российской Федерации, утвержденную Указом Президента Российской Федерации от 5 декабря 2016 года № 646, и Стратегию национальной безопасности Российской Федерации, утвержденную Указом Президента Российской Федерации от 31 декабря 2015 года № 683, применительно к деятельности исполнительных органов государственной власти Рязанской области, а также направлена на реализацию в Рязанской области Указа Президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и национальной программы «Цифровая экономика Российской Федерации», утвержденной протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

I. Общие положения

Развитие информационных технологий и их широкое применение во всех сферах деятельности государства и общества способствовало не только значительному повышению их интенсивности и качества, но и возникновению угроз национальной безопасности в информационной сфере, связанных с расширением возможностей утечки информации и воздействия на нее в результате усилий спецслужб иностранных государств, деятельности преступных сообществ, недобросовестных конкурентов и отдельных злоумышленников. При этом, существенно расширился спектр угроз безопасности информации, связанных с:

- несанкционированным доступом к информации, обрабатываемой в информационных системах, построенных с использованием суперкомпьютерных технологий, грид-технологий, технологий виртуализации и облачных вычислений, путем использования вредоносного программного обеспечения, эксплуатирующего уязвимость данных технологий;

- удалением и модификацией информации путем использования новейшего вредоносного программного обеспечения (типа Stuxnet, Duqu, Flame), являющегося, по сути, информационным оружием;

- проведением компьютерных атак как на информационные системы в целом, так и на отдельные средства вычислительной техники (в том числе принтеры, коммуникаторы, коммутаторы), имеющие широкополосное подключение в информационно-телекоммуникационную сеть «Интернет», за счет использования вредоносного программного обеспечения;

- перехватом информации в беспроводных вычислительных сетях;

- использованием недекларированных возможностей (в том числе «программных закладок») программного и аппаратного обеспечения зарубежного производства;

- утечкой информации ограниченного доступа путем ее размещения в информационно-телекоммуникационной сети «Интернет»;

- перехватом информации с современных мобильных и стационарных устройств, использующих различные технологии обработки информации (удаленное управление и вычисление, распознавание речи, новые интерфейсы передачи данных) и отображения (LED, OLED-технологии, электронные чернила, трехмерное изображение);

- перехватом побочных электромагнитных излучений и наводок различных объектов (в том числе лазерных систем, суперкомпьютеров, видеосистем на основе жидких кристаллов) в широком диапазоне частот;

- утечкой акустической речевой информации по техническим каналам.

Реализация перечисленных угроз может привести к снижению эффективности деятельности государства во внутриполитической, экономической, международной и информационной областях, утрате передовых позиций в наиболее развитых отраслях науки и техники, значительным материальным потерям и другим негативным последствиям, существенно влияющим на состояние национальной безопасности России. Все это обусловливает необходимость принятия адекватных мер по обеспечению безопасности информации не только на федеральном уровне, но и на уровне субъектов Российской Федерации. Поэтому защита информации является неотъемлемой составной частью основной деятельности исполнительных органов государственной власти Рязанской области. Защита информации достигается проведением комплекса правовых, организационных, технических и методических мероприятий, направленных на предотвращение, а также на противодействие угрозам безопасности информации в зависимости от условий деятельности исполнительных органов государственной власти Рязанской области.

Проведение указанного комплекса мероприятий должно основываться на определении:

- возможных угроз безопасности информации на конкретных объектах информатизации с использованием сценариев развития событий;

- перечней объектов защиты информации с учетом их характеристик;

- адекватных возможным угрозам безопасности информации средств и способов защиты информации.

Необходимость повышения внимания к проблеме защиты информации в исполнительных органах государственной власти Рязанской области обусловлена:

- наличием на территории Рязанской области иностранных и совместных предприятий;

- прямой зависимостью результатов деятельности исполнительных органов государственной власти Рязанской области от достоверности используемой ими информации и своевременности ее получения, эффективности принятых мер по ее защите;

- приданием информации статуса объекта гражданских, публичных и иных отношений, формированием государственных информационных ресурсов, находящихся в ведении исполнительных органов государственной власти Рязанской области, необходимостью защиты этих ресурсов от противоправных действий;

- использованием исполнительными органами государственной власти Рязанской области региональных, межрегиональных и глобальных информационных систем, накапливающих и передающих большие объемы информации, уязвимой для несанкционированного доступа к ней, для несанкционированных и непреднамеренных воздействий на нее в этих системах;

- непредсказуемыми экономическими и социальными последствиями возникновения чрезвычайных ситуаций, связанных с нарушением безопасности информации;

- постоянным развитием рынка информационных технологий, используемых для обработки, передачи и хранения информации, и внедрением их в информационные системы исполнительных органов государственной власти Рязанской области;

- существенным расширением мобильного сектора сетей исполнительных органов государственной власти Рязанской области;

- возникновением принципиально новых технологий обработки информации (грид-технологий, суперкомпьютерных технологий, технологий облачных вычислений, виртуализации, конвергенции различных приложений на базе как локальных, корпоративных, так и глобальных компьютерных сетей и др.);

- существенным возрастанием производительности компьютерных систем, плотности хранения информации и пропускной способности каналов передачи данных;

- организацией широкополосного доступа из защищаемых информационных систем в информационно-телекоммуникационную сеть «Интернет»;

- ростом числа преступлений в сфере информационных технологий;

- повышением внимания государства к вопросам защиты персональных данных граждан Российской Федерации;

- размещением на территории Российской Федерации технических средств информационных систем, используемых в деятельности исполнительных органов государственной власти Рязанской области;

- использованием аппаратных, аппаратно-программных и программных средств, обеспечивающих сбор, хранение, обработку, передачу и защиту информации, несертифицированных по требованиям безопасности информации, не прошедших специальную проверку и специальные исследования.

Угрозы безопасности информации включают в себя внешние и внутренние факторы.

К внешним факторам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная на нанесение ущерба государственным интересам в информационной сфере;

- стремление ряда стран к доминированию и ущемлению национальных интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего 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 создания конкурентоспособных российских информационных технологий;

- разработка рядом государств концепций информационных войн, предусматривающих создание средств вредоносного воздействия на информационные сферы других стран мира, нарушение функционирования информационных систем и информационно-телекоммуникационных сетей.

К внутренним факторам относятся:

- глобализация информационно-телекоммуникационных сетей, внедрение телекоммуникационных и информационных технологий, реализуемых преимущественно на аппаратно-программных средствах зарубежного производства, что существенно обостряет проблему защиты информации;

- увеличение объемов хранимой и передаваемой информации, а также территориальная распределенность информационно-телекоммуникационных сетей;

- усложнение применяемых технологий и процессов функционирования информационно-телекоммуникационных сетей, что может привести к появлению ошибок и недекларированных возможностей в аппаратно-программных средствах;

- недостаточность правовой базы, регулирующей отношения в информационной сфере;

- дефицит квалифицированных кадров по защите информации;

- недостаточное финансирование мероприятий по защите информации;

- использование несертифицированных по требованиям безопасности информации отечественных и зарубежных информационных технологий, зарубежных средств аппаратного и программного обеспечения для информационных систем различного назначения, не прошедших специальную проверку и специальные исследования.

Основными способами реализации угроз безопасности информации в исполнительных органах государственной власти Рязанской области могут быть: информационные, аппаратно-программные, физические, радиоэлектронные, а также способы, связанные с нарушениями норм и требований.

К информационным способам реализации угроз безопасности информации относятся:

- противоправный сбор, распространение и использование информации;

- манипулирование информацией (сокрытие или искажение информации, навязывание ложной информации);

- незаконное уничтожение информации.

К аппаратно-программным способам реализации угроз безопасности информации относятся:

- внедрение вредоносных программ (компьютерных вирусов, сетевых червей, программных закладок и т.п.);

- несанкционированный доступ к информации с использованием возможностей межсетевого взаимодействия и уязвимости программного обеспечения с последующим ее копированием, уничтожением, модификацией, блокированием и т.п.;

- нарушение адресности и оперативности информационного обмена;

- нарушение технологии обработки данных и информационного обмена;

- использование или создание технических каналов утечки информации.

К физическим способам реализации угроз безопасности информации относятся:

- уничтожение, хищение или разрушение средств обработки, защиты информации, средств контроля эффективности защиты информации, связи, целенаправленное нарушение их работоспособности;

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

- хищение, целенаправленное нарушение работоспособности средств криптографической защиты информации, программных или аппаратных носителей информации, средств защиты информации от несанкционированного доступа.

К радиоэлектронным способам реализации угроз безопасности информации относятся:

- перехват информации в сетях передачи данных и линиях связи;

- внедрение электронных устройств перехвата информации в технические средства и помещения объектов информатизации;

- навязывание ложной информации по сетям передачи данных и линиям связи;

- радиоэлектронное подавление систем управления и сигналов, передаваемых по линиям связи.

К нарушениям норм и требований безопасности информации относятся:

- незаконная деятельность в области защиты информации;

- использование несертифицированных по требованиям безопасности информации средств защиты информации и средств контроля эффективности защиты информации, а также устаревших средств информатизации и информационных технологий;

- ошибки при разработке и реализации политики безопасности информации;

- ошибки при реализации организационных методов защиты информации;

- задержки разработки и принятия необходимых правовых и организационно-распорядительных документов в области защиты информации.

Результатами реализации угроз безопасности информации могут являться:

- нарушение конфиденциальности информации (разглашение, утрата, хищение, утечка, перехват и т.д.);

- нарушение целостности информации (искажение, уничтожение и т.д.);

- нарушение правил доступа к информации и работоспособности информационных систем (блокирование данных в информационных системах, разрушение элементов информационных систем, компрометация системы защиты информации и т.д.).

К основным объектам защиты информации в исполнительных органах государственной власти Рязанской области относятся:

- информация ограниченного доступа;

- общедоступная информация, неправомерное обращение с которой может нанести существенный ущерб ее обладателям и пользователям;

- объекты информатизации, в которых обрабатывается информация ограниченного доступа, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа;

- технические средства и системы, не обрабатывающие защищаемую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа;

- информация, обрабатываемая в критически важных объектах и системах информационной инфраструктуры;

- информация о критически важных объектах и системах информационной инфраструктуры и в первую очередь информация об их системах защиты информации;

- помещения, предназначенные для ведения переговоров, в ходе которых обсуждаются сведения ограниченного доступа.

К мероприятиям по обеспечению эффективной защиты информации относятся:

- развитие и совершенствование защиты информации в исполнительных органах государственной власти Рязанской области;

- координация деятельности исполнительных органов государственной власти Рязанской области в информационной сфере;

- разработка и реализация государственных программ Рязанской области, направленных на решение задач в сфере защиты информации;

- подготовка, профессиональная переподготовка и повышение квалификации специалистов по защите информации;

- разработка организационно-распорядительных документов в области защиты информации.

II. Цель и задачи защиты информации в исполнительных органах государственной власти Рязанской области

Основной целью защиты информации в исполнительных органах государственной власти Рязанской области является предотвращение или существенное снижение величины ущерба, наносимого информационной сфере из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию, а также создание условий, способствующих защите интересов общества в политической, экономической, научно-технической и других сферах деятельности.

Основными задачами защиты информации в исполнительных органах государственной власти Рязанской области являются:

- обеспечение конфиденциальности, целостности и доступности информационных систем Рязанской области;

- использование современных методов и средств защиты информации;

- защита государственной тайны;

- обеспечение конфиденциальности документированной информации ограниченного доступа в соответствии с законодательством Российской Федерации;

- организация контроля за состоянием защиты информации;

- предотвращение утечки информации, передаваемой по каналам связи;

- предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами обработки информации;

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

- выявление и предотвращение специальных воздействий, вызывающих уничтожение, искажение и блокирование информации или сбои в работе технических систем и средств;

- предотвращение утечки речевой информации из выделенных и защищаемых помещений;

- выявление внедренных на объекты и в технические средства иностранного производства электронных устройств перехвата информации (закладных устройств).

III. Основы организации защиты информации в исполнительных органах государственной власти Рязанской области

Содержание и порядок действий, направленных на обеспечение защиты информации, определяют организацию защиты информации в исполнительных органах государственной власти Рязанской области.

Организация защиты информации включает:

- формирование регионального правового и методического обеспечения деятельности в области защиты информации;

- формирование организационной структуры системы защиты информации и кадровое обеспечение ее деятельности;

- проведение анализа деятельности в части защиты информации, а также используемых объектов информатизации;

- категорирование объектов информатизации, а также классификацию автоматизированных систем по требованиям защищенности от несанкционированного доступа к информации;

- проведение анализа условий функционирования объектов информатизации, а также оценки угроз безопасности обрабатываемой в них информации;

- проведение организационно-технических мероприятий по защите информации;

- аттестацию объектов информатизации по требованиям безопасности информации;

- мониторинг и контроль состояния системы защиты информации;

- определение направлений развития и совершенствования системы защиты информации.

IV. Принципы функционирования системы защиты информации в исполнительных органах государственной власти Рязанской области и направления ее развития

Основными принципами функционирования системы защиты информации в исполнительных органах государственной власти Рязанской области являются следующие.

1. Принцип законности.

Развитие и совершенствование системы защиты информации исполнительных органов государственной власти Рязанской области осуществляется в соответствии с нормативными правовыми актами Российской Федерации в области технической защиты информации, в том числе с учетом международных договоров (соглашений) и методических документов ФСТЭК России, ФСБ России и других органов власти в пределах их компетенции.

2. Принцип разграничения полномочий.

Исполнительные органы государственной власти Рязанской области создают все условия для защиты информации на подведомственных им объектах информатизации в интересах реализации на них требуемого уровня защищенности информации.

3. Принцип своевременности реакции.

Использование процедур предварительного ограничения доступа к защищаемой информации (матриц доступа) позволяет осуществлять ее защиту и заранее установить ограничения на распространение этой информации с момента ее получения, разработки.

Заблаговременная разработка мер по технической защите информации, их непосредственная реализация обеспечивает адекватную реакцию на возникающие и прогнозируемые угрозы от деятельности технических разведок, преступных групп, злоумышленников, утечки информации по техническим каналам, специальных воздействий на нее, а также упреждающую нейтрализацию, быструю ликвидацию последствий угроз.

4. Принцип подконтрольности и подотчетности.

Исполнительные органы государственной власти Рязанской области в установленном порядке отчитываются за состояние защиты информации в подведомственных им организациях в соответствии с законодательством Российской Федерации, а федеральные органы исполнительной власти в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации осуществляют контроль за состоянием системы защиты информации в исполнительных органах государственной власти Рязанской области.

Централизованное предоставление сведений в федеральные органы исполнительной власти о состоянии защиты информации в Рязанской области осуществляется комиссией по информационной безопасности Рязанской области. Подготовку данной информации:

- составляющей государственную тайну, осуществляет управление по защите государственной тайны и мобилизационной работе аппарата Правительства Рязанской области;

- не составляющей государственную тайну, осуществляет министерство цифрового развития, информационных технологий и связи Рязанской области.

Исполнительные органы государственной власти Рязанской области отчитываются в комиссию по информационной безопасности Рязанской области о состоянии защиты информации в органе и подведомственных ему учреждениях.

5. Принцип соответствия.

Уровень развития системы защиты информации должен соответствовать задачам обеспечения информационной безопасности Российской Федерации и обеспечивать устойчивое развитие Рязанской области с учетом ее экономических возможностей. Средства и способы защиты информации применяются в соответствии с угрозами безопасности информации, определенными в утвержденных моделях угроз безопасности информации, и экономическими возможностями Рязанской области. Координационные и директивные методы управления системой защиты информации должны рационально сочетаться.

6. Принцип системности.

Защита информации в исполнительных органах государственной власти Рязанской области является составной частью обеспечения информационной безопасности Российской Федерации и организуется с учетом всех опасных для защищаемых объектов видов технических разведок, их возможностей и способов ведения, а также сочетания правовых, организационных, технических и специальных методов и средств защиты информации, преемственности и непрерывности мероприятий по защите информации. Принцип системности устанавливает единообразие создания и реализации механизма комплексной защиты информации в различных элементах информационной сферы исполнительных органов государственной власти Рязанской области.

Развитие существующей системы защиты информации будет осуществляться в следующих направлениях:

- постоянный анализ кадровой структуры исполнительных органов государственной власти Рязанской области в области защиты информации и ее совершенствование;

- организация подготовки, переподготовки и повышения квалификации кадров в исполнительных органах государственной власти Рязанской области в области защиты информации;

- централизованное решение задач в исполнительных органах государственной власти Рязанской области по защите сведений, не составляющих государственную тайну;

- развитие и совершенствование мероприятий по защите информации в целях нейтрализации новых угроз безопасности информации.

Система защиты информации в исполнительных органах государственной власти Рязанской области выполняет следующие функции:

- реализация мероприятий по защите информации как совокупность действий по применению мер, способов и средств защиты информации;

- управление (координация) защитой информации как совокупность целенаправленных действий, сил и средств защиты информации, необходимых для организации их согласованного функционирования.

Организационно структуру управления защитой информации в исполнительных органах государственной власти Рязанской области (приложение) формируют:

- комиссия по информационной безопасности Рязанской области;

- министерство цифрового развития, информационных технологий и связи Рязанской области;

- управление по защите государственной тайны и мобилизационной работе аппарата Правительства Рязанской области;

- специалисты, на которых возложены функции по защите информации, в том числе штатные специалисты по защите информации исполнительных органов государственной власти Рязанской области (при наличии);

- специалисты, на которых возложены функции по защите информации, в том числе штатные специалисты по защите информации (при наличии) или структурные подразделения по защите информации (при наличии) учреждений, подведомственных исполнительным органам государственной власти Рязанской области.

Исполнительные органы государственной власти Рязанской области реализуют государственную политику в области защиты информации во взаимодействии с аппаратом полномочного представителя Президента Российской Федерации в Центральном федеральном округе, Управлением ФСТЭК по Центральному федеральному округу, Управлением ФСБ России по Рязанской области, Управлением Роскомнадзора по Рязанской области, Центром специальной связи и информации ФСО России в Рязанской области по вопросам исполнения действующего законодательства в области защиты информации.

Методическая поддержка исполнительных органов государственной власти Рязанской области при защите информации, составляющей государственную тайну, осуществляет управление по защите государственной тайны и мобилизационной работе аппарата Правительства Рязанской области.

Координацию деятельности и методическую поддержку исполнительных органов государственной власти Рязанской области при защите информации, не составляющей государственную тайну, осуществляет министерство цифрового развития, информационных технологий и связи Рязанской области.

Ответственность за организацию и состояние защиты информации в исполнительных органах государственной власти Рязанской области и в их подведомственных учреждениях возлагается соответственно на руководителей этих органов и учреждений.

Мероприятия по защите информации в исполнительных органах государственной власти Рязанской области и их подведомственных учреждениях осуществляются:

- специалистами, на которых возложены функции по защите информации, в том числе штатными специалистами по защите информации исполнительных органов государственной власти Рязанской области (при наличии);

- специалистами, на которых возложены функции по защите информации, в том числе штатными специалистами по защите информации (при наличии) или структурными подразделениями по защите информации (при наличии) учреждений, подведомственных исполнительным органам государственной власти Рязанской области;

- государственным казенным учреждением Рязанской области «Центр информационных технологий Рязанской области», подведомственным министерству цифрового развития, информационных технологий и связи Рязанской области (по согласованию);

- организациями (в соответствии с заключенными контрактами и соглашениями), ведущими согласно имеющимся у них лицензиям деятельность в области защиты информации.

Иные функции, права и полномочия подразделений и коллегиальных органов, отвечающих за организацию и осуществление мероприятий по защите информации, определяются положениями об этих подразделениях и органах.

V. Этапы реализации Концепции защиты информации в исполнительных органах государственной власти   
Рязанской области на 2021-2025 годы

Основные положения Концепции реализуются путем:

- целенаправленной повседневной деятельности исполнительных органов государственной власти Рязанской области, их подведомственных учреждений;

- выполнения федеральных, межрегиональных и региональных научно-технических программ, научно-исследовательских и опытно-конструкторских работ в области защиты информации, государственных программ Рязанской области с учетом результатов выполнения общегосударственных программ в области защиты информации.

Результаты реализации Концепции рассматриваются на заседаниях комиссии по информационной безопасности Рязанской области.

Концепцию планируется реализовать до 2025 года в два этапа.

Первый этап (2021-2022 гг.) – развитие и совершенствование системы защиты информации в исполнительных органах государственной власти Рязанской области как неотъемлемой составной части государственной системы защиты информации.

В ходе первого этапа:

- совершенствуется подготовка, переподготовка и повышение квалификации специалистов в области защиты информации;

- разрабатываются правовые, методические, организационно-распорядительные и плановые документы в области защиты информации с учетом внедрения новых информационных технологий и новых угроз безопасности информации;

- выявляются проблемные вопросы в области защиты информации, вырабатываются предложения и планы по их реализации;

- формируется организационная структура обеспечения информационной безопасности Рязанской области;

- совместно со специализированными организациями проводится выбор оптимальных проектных решений, организационных и технических мероприятий в ходе создания и эксплуатации объектов исполнительных органов государственной власти Рязанской области, на которых предполагается обработка информации, содержащей сведения, составляющие государственную тайну;

- определяются и уточняются перечни информационных ресурсов, подлежащих защите, определяются структура и порядок деятельности соответствующих систем формирования, учета, хранения и предоставления информационных ресурсов;

- проводится анализ применяемых исполнительными органами государственной власти Рязанской области, их подведомственными учреждениями информационных систем и технологий связи для построения систем защиты информации и контроля;

- организуется мониторинг и оценка закупок отечественного и иностранного программного обеспечения исполнительными органами государственной власти Рязанской области, а также их подведомственными учреждениями;

- организуется мониторинг закупок серверного и телекоммуникационного оборудования иностранного производства исполнительными органами государственной власти Рязанской области, а также их подведомственными учреждениями;

- организуется контроль состояния защиты информации;

- в подведомственных исполнительным органам государственной власти Рязанской области учреждениях назначаются специалисты, на которых возложены функции по защите информации, в том числе штатные специалисты по защите информации или создаются структурные подразделения по защите информации, где такие сотрудники не назначены или имеется потребность в создании такого подразделения;

- формируется кадровая, организационная и программно-техническая основа для централизованного решения задач по защите сведений, не составляющих государственную тайну, в исполнительных органах государственной власти Рязанской области.

Второй этап (2023-2025 гг.) – совершенствование системы защиты информации в исполнительных органах государственной власти Рязанской области.

На втором этапе:

- совершенствуется правовое, методическое и техническое обеспечение контроля защищенности информации, обрабатываемой в государственных информационных системах;

- расширяется комплекс организационных и технических мероприятий по предотвращению возникновения каналов утечки информации;

- объекты информатизации оснащаются перспективной техникой защиты информации, обеспечивающей парирование угроз безопасности информации с учетом внедрения в информационные системы новых информационных технологий;

- увеличивается количество подготовленных специалистов по образовательным программам в области информационной безопасности с использованием в образовательном процессе отечественных высокотехнологичных комплексов и средств защиты информации.

Реализация Концепции позволит:

- усовершенствовать организационную структуру системы защиты информации, ее кадровое обеспечение;

- улучшить обеспеченность исполнительных органов государственной власти Рязанской области документами в области защиты информации;

- повысить оснащенность исполнительных органов государственной власти Рязанской области высокоэффективными программно-техническими средствами защиты информации;

- повысить эффективность функционирования системы защиты информации, не содержащей сведения, составляющие государственную тайну.

VI. Финансирование мероприятий по защите информации в исполнительных органах государственной власти Рязанской области

Финансирование расходов на проведение мероприятий по защите информации в исполнительных органах государственной власти Рязанской области осуществляется в пределах средств, предусмотренных в областном бюджете на реализацию соответствующими исполнительными органами государственной власти Рязанской области мероприятий государственной программы Рязанской области, целью которой является совершенствование цифровой экономики и деятельности органов государственной власти Рязанской области на основе использования современных информационно-коммуникационных технологий.