



АДМИНИСТРАЦИЯ СМОЛЕНСКОЙ ОБЛАСТИ

## ПОСТАНОВЛЕНИЕ

от 11.12.2014 № 948

Об утверждении Концепции  
защиты информации на территории  
Смоленской области на период 2014–  
2020 годов

На основании протокола выездного заседания Комиссии по информационной безопасности при полномочном представителе Президента Российской Федерации в Центральном федеральном округе от 31.07.2013 № А50-5746

Администрация Смоленской области п о с т а н о в л я е т:

1. Утвердить прилагаемую Концепцию защиты информации на территории Смоленской области на период 2014 – 2020 годов.
2. Признать утратившими силу:
  - постановление Администрации Смоленской области от 20.12.2004 № 366 «Об утверждении Концепции защиты информации в Смоленской области»;
  - постановление Администрации Смоленской области от 05.06.2008 № 324 «О внесении изменений в Концепцию защиты информации в Смоленской области»;
  - постановление Администрации Смоленской области от 06.04.2009 № 167 «О внесении изменений в постановление Администрации Смоленской области от 20.12.2004 № 336»;
  - постановление Администрации Смоленской области от 22.04.2010 № 193 «О внесении изменения в Концепцию защиты информации в Смоленской области».

Губернатор  
Смоленской области



УТВЕРЖДЕНА  
постановлением Администрации  
Смоленской области  
от 11.12.2014 № 898

**КОНЦЕПЦИЯ**  
**защиты информации на территории Смоленской области**  
**на период 2014 – 2020 годов**

**Введение**

Настоящая Концепция представляет собой систему взглядов на содержание проблемы защиты информации, а также цели, задачи, принципы и основные направления формирования и развития системы защиты информации на территории Смоленской области, которая является важной частью государственной системы защиты информации.

Настоящая Концепция предназначена для обеспечения согласованности действий органов государственной власти Смоленской области (далее – органы государственной власти) и органов местного самоуправления муниципальных образований Смоленской области (далее – органы местного самоуправления), организаций, предприятий и учреждений независимо от их организационно-правовых форм, форм собственности и видов деятельности, выполняющих работы по оборонной тематике и другие работы с использованием информации с ограниченным доступом и находящихся на территории Смоленской области (далее – организации), в работе по развитию и совершенствованию системы защиты информации.

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

Настоящая Концепция развивает Стратегию национальной безопасности Российской Федерации до 2020 года, утвержденную Указом Президента Российской Федерации от 01.07.2014 № 483, Доктрину информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 09.09.2000 № ПР-1895, Концепцию защиты информации в Центральном федеральном округе (на период 2013 – 2020 годов), одобренную протоколом заседания Комиссии по информационной безопасности при полномочном представителе Президента Российской Федерации в Центральном федеральном округе от 31.07.2013 № А50-5746, применительно к организации защиты информации на территории Смоленской области.

## 1. Термины и понятия, используемые в настоящей Концепции

Для целей настоящей Концепции используются следующие термины и понятия:

- информация – сведения (сообщения, данные) независимо от формы их представления;
- документированная информация (документ) – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;
- информация с ограниченным доступом – документированная информация, которая по условиям правового режима подразделяется на отнесенную к государственной тайне информацию и конфиденциальную информацию;
- государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- информационные ресурсы – отдельные документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);
- защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;
- защищаемая информация – информация, подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми обладателем информации;
- защищаемый объект информатизации (объект информатизации) – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров;
- безопасность информации – состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами;
- система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованных и функционирующих по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации;
- объект защиты – объект, имеющий охраняемые сведения, и (или) объект, на котором осуществляются работы с защищаемой информацией;

- техника защиты информации – средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации;
- средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации;
- средство контроля эффективности защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для контроля эффективности защиты информации;
- технический канал утечки информации (технический канал) – совокупность объекта защиты, физической среды и средства технической разведки, которыми добывается защищаемая информация;
- утечка информации по техническим каналам – неконтролируемое распространение защищаемой информации по техническим каналам в результате несанкционированного доступа к информации и получения защищаемой информации разведками;
- несанкционированный доступ к информации – получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

## 2. Общие положения

В последнее десятилетие бурное развитие средств вычислительной техники привело к созданию большого числа разного рода автоматизированных информационных и управляющих систем, к возникновению принципиально новых информационных технологий, в том числе и на территории Смоленской области.

С развитием информационных систем возникла и проблема обеспечения безопасности хранящейся и обрабатываемой в них информации. Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации может нанести серьезный ущерб многим субъектам, участвующим в процессах автоматизированного информационного взаимодействия.

В этот же период происходило становление организационной структуры системы защиты информации в Российской Федерации и ее субъектах, формировались основы нормативной правовой базы, накапливался опыт ее функционирования в новых политических и экономических условиях.

Развитие информационных технологий и их широкое применение во всех сферах деятельности государства и общества способствовали не только значительному повышению их интенсивности и качества, но и возникновению широкого спектра 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 кода, 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), имеющие широкополосное подключение в сеть общего пользования информационно-телекоммуникационной сети Интернет, за счет использования вредоносного программного обеспечения;

- перехватом информации в беспроводных вычислительных сетях;

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

- утечкой и опубликованием информации ограниченного доступа путем ее размещения в сети общего пользования 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 широком диапазоне частот;

- утечкой речевой информации по акустическому и вибрационному каналам.

Защита информации является неотъемлемой составной частью основной деятельности органов государственной власти, органов местного самоуправления и организаций, достигаемой путем проведения комплекса правовых, организационных, технических и методических мероприятий, направленных на предотвращение, нейтрализацию угроз безопасности информации в зависимости от условий деятельности и решаемых задач по обеспечению безопасности информации.

Проведение указанного комплекса мероприятий по защите информации должно основываться на определении:

- угроз безопасности информации на конкретных объектах информатизации;

- перечней объектов защиты и защищаемых сведений;

- средств и методов защиты информации.

Целями защиты информации на территории Смоленской области являются:

- предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации;

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;

- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с федеральным законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения;
- содействие экономическому, научно-техническому прогрессу Смоленской области, обеспечению ее безопасности и устойчивого развития.

Основными задачами защиты информации на территории Смоленской области являются:

- проведение единой государственной политики по защите информации;
- формирование и организация деятельности органов по защите информации;
- определение и учет информационных ресурсов, систем и средств формирования, передачи, хранения, обработки и распространения информации, подлежащей защите;
- исключение или существенное затруднение добывания информации средствами технической разведки путем предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию с целью ее уничтожения, искажения и блокирования;
- подготовка предложений по совершенствованию правового, нормативного, методического, научно-технического и организационного обеспечения защиты информации на объектах Смоленской области;
- анализ состояния и прогнозирование источников угроз безопасности информации;
- включение в областные государственные программы мероприятий по защите информационных ресурсов и средств информатизации;
- выявление ключевых проблем и определение приоритетных направлений развития системы защиты информации на территории Смоленской области;
- проведение практических мероприятий по созданию и развитию системы защиты информации на территории Смоленской области;
- методическое и информационное обеспечение работ по защите информации;
- контроль и анализ состояния защиты информации в органах государственной власти, органах местного самоуправления и организациях;
- совершенствование и развитие системы подготовки специалистов по защите информации.

Основными объектами обеспечения защиты информации на территории Смоленской области являются:

- информационные ресурсы, содержащие информацию ограниченного доступа;
- 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 переговоров, в ходе которых оглашаются сведения ограниченного доступа;

- иные чувствительные по отношению к непреднамеренным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы (в том числе открытая информация, подлежащая защите), представленные в виде документов и массивов информации, независимо от формы и вида их представления (возможный ущерб от несанкционированного использования или модификации этой открытой информации превышает стоимость затрат, связанных с мероприятиями по ее защите от этих угроз).

Совершенствование способов и средств технической разведки, повышение опасности угроз несанкционированного доступа к информации и специальных воздействий на нее в системах и средствах информатизации и связи, происходящие с течением времени изменения условий и приоритетов защиты объектов обуславливают необходимость развития системы защиты информации на территории Смоленской области. Планирование развития системы защиты информации на территории Смоленской области основывается на анализе ее состояния и выявлении ключевых проблем в развитии.

К основным проблемам, характеризующим современное состояние системы защиты информации на территории Смоленской области, относятся:

- нехватка специалистов в области защиты информации;
- слабая оснащённость подразделений по защите информации государственных и муниципальных органов, организаций средствами и аппаратурой контроля эффективности защиты информации, а также сертифицированными средствами защиты информации;

- слабое использование современных информационных технологий для обеспечения потребителей необходимыми документами, носящими открытый характер.

Существует ряд факторов, определяющих необходимость совершенствования системы защиты информации на территории Смоленской области. К этим факторам, в частности, относятся:

- приграничное расположение, наличие на территории Смоленской области совместных предприятий (в том числе с участием стран дальнего зарубежья);

- размещение на территории Смоленской области дипломатических и консульских учреждений, международных организаций и их представительств;

- реструктуризация систем управления хозяйственной деятельностью организаций, повышение их самостоятельности;

- возрастание зависимости результатов деятельности органов государственной власти, органов местного самоуправления, организаций от достоверности используемой ими информации, своевременности ее получения, эффективности принятых мер по ее защите;

- придание информации статуса объекта собственности, формирование государственных информационных ресурсов Смоленской области, информационных ресурсов организаций и граждан, необходимость защиты этих ресурсов от противоправных действий;

- использование в органах государственной власти, органах местного самоуправления, организациях межрегиональных и глобальных информационных систем, накапливающих и передающих большие объемы информации, потенциально уязвимых для несанкционированного доступа к информации, возрастание опасности несанкционированных и непреднамеренных воздействий на информацию в этих системах и, как следствие, непредсказуемые экономические и социальные последствия от возникновения критических ситуаций, связанных с нарушениями режимов безопасности информации в кредитно-финансовых учреждениях, системах управления экологически опасными производствами, транспортом, энергетикой;

- расширение спектра источников угроз безопасности информации, возникающих в отношении органов государственной власти, органов местного самоуправления, организаций;

- рост числа преступлений в сфере компьютерной информации;

- использование в органах государственной власти, органах местного самоуправления, организациях технических и программных средств, обеспечивающих сбор, хранение, обработку и передачу информации, не сертифицированных по требованиям безопасности информации;

- возрастание опасности информационных угроз, возникающих в непосредственной близости от защищаемых объектов Смоленской области или на них самих;

- неспособность отдельных организаций самостоятельно обеспечить эффективную защиту информации.

Перечисленные факторы выдвигают в число приоритетных задачу развития системы защиты информации, а устранение указанных проблем в области защиты информации является общей задачей реализации государственной политики в сфере построения региональной системы защиты информации.

### **3. Цель, задачи и основные направления защиты информации на территории Смоленской области**

Главной целью развития системы защиты информации на территории Смоленской области является формирование эффективных компонентов этой системы, соответствующих задачам обеспечения национальной безопасности Российской Федерации, безопасности и устойчивого развития Смоленской области, предотвращение и существенное снижение величины наносимого ущерба.

В этой связи на первый план выходит задача создания условий, обеспечивающих исключение или существенное затруднение добывания информации об объектах защиты средствами технической разведки путем предотвращения утечки, хищения, утраты, искажения, подделки информации ограниченного доступа по техническим каналам, несанкционированного доступа к ней и специальных воздействий на нее в различных сферах деятельности хозяйствующих субъектов на территории Смоленской области.



Основными задачами по развитию системы защиты информации на территории Смоленской области являются:

- формирование и совершенствование системы защиты информации, развитие ее научно-технического и кадрового потенциала;
- создание и совершенствование необходимых и достаточных правовых, организационных, экономических и научно-технических условий для обеспечения деятельности системы защиты информации;
- обеспечение эффективной технической защиты информации на объектах органов государственной власти, органов местного самоуправления, организаций;
- совершенствование системы контроля и управления системой защиты информации, приспособленной к изменяющимся условиям обстановки.

Основными принципами развития системы защиты информации на территории Смоленской области являются:

- соответствие уровня развития системы защиты информации задачам обеспечения национальной безопасности Российской Федерации, безопасности и устойчивого развития Смоленской области с учетом ее экономических возможностей;
- обеспечение на территории Смоленской области своевременной и адекватной реакции на возникающие и прогнозируемые угрозы ведения технической разведки, утечки информации по техническим каналам, несанкционированного доступа к информации и специальных воздействий на нее;
- использование коллегиальных методов руководства системой защиты информации и ее развития;
- программное планирование развития системы защиты информации.

Система защиты информации на территории Смоленской области организационно входит в систему защиты информации в Центральном федеральном округе (далее также – ЦФО) и образует три уровня:

- систему защиты информации на региональном уровне;
- систему защиты информации на муниципальном уровне;
- систему защиты информации на уровне организаций.

Организационную структуру системы защиты информации на региональном уровне образуют:

- Комиссия по информационной безопасности при Администрации Смоленской области;
- органы государственной власти, органы местного самоуправления, их коллегиальные органы, структурные подразделения по защите информации (штатные специалисты);
- учебные заведения, осуществляющие подготовку, профессиональную переподготовку и повышение квалификации специалистов в области защиты информации.

Организационную структуру системы защиты информации на муниципальном уровне образуют:

- комиссии по информационной безопасности в органах местного самоуправления;
- структурные подразделения по защите информации (штатные специалисты) органов местного самоуправления;

- организации, подведомственные органам местного самоуправления, выполняющие работы и оказывающие услуги в области защиты информации.

Организационную структуру системы защиты информации на уровне организаций образуют:

- организации, выполняющие работы по оборонной тематике и другие работы с использованием информации с ограниченным доступом;
- организации, проводящие работы с использованием информации с ограниченным доступом;
- организации-лицензиаты Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК);
- организации-лицензиаты Федеральной службы безопасности Российской Федерации.

Функциональное регулирование деятельности системы защиты информации на территории Смоленской области осуществляется на основании решений Комиссии при полномочном представителе Президента Российской Федерации в Центральном федеральном округе по информационной безопасности. Координацию и методическое руководство деятельностью в области защиты информации осуществляет Управление ФСТЭК России по Центральному федеральному округу.

Государственную политику в области защиты информации на территории Смоленской области реализуют:

- Губернатор Смоленской области – возглавляет систему защиты информации на территории Смоленской области;
- Комиссия по информационной безопасности при Администрации Смоленской области – координирует деятельность по защите информации государственных и муниципальных органов, организаций;
- Департамент Смоленской области по информационным технологиям – посредством взаимодействия с аппаратом полномочного представителя Президента Российской Федерации в ЦФО, Управлением ФСТЭК России по Центральному федеральному округу, Управлением Федеральной службы безопасности Российской Федерации по Смоленской области организует деятельность по защите информации в органах исполнительной власти и органах местного самоуправления через структурное подразделение по защите информации Департамента Смоленской области по информационным технологиям;
- органы государственной власти и органы местного самоуправления – обеспечивают исполнение нормативных правовых и распорядительных актов в области защиты информации;
- организации – осуществляют мероприятия по защите информации на подведомственных объектах защиты.

Функции, права и полномочия структурных подразделений (штатных специалистов) и коллегиальных органов, отвечающих за организацию и осуществление мероприятий по защите информации в органах государственной власти и органах местного самоуправления, организациях, определяются положениями об этих подразделениях и органах.

В органах государственной власти и органах местного самоуправления, организациях ответственность за организацию и состояние защиты информации возлагается на соответствующих руководителей.

Основными направлениями формирования и развития системы защиты информации на территории Смоленской области при решении задачи формирования и совершенствования организационной структуры системы защиты информации, развития ее научно-технического и кадрового потенциала являются:

- формирование в органах государственной власти, органах местного самоуправления, организациях структурных подразделений по защите информации (назначение штатных специалистов);

- создание и развитие системы подготовки и переподготовки специалистов в области защиты информации.

При решении задачи создания и совершенствования необходимых и достаточных правовых, организационных, экономических и научно-технических условий для обеспечения деятельности системы защиты информации осуществляются:

- совершенствование концептуальных и правовых основ деятельности системы защиты информации;

- организация и обеспечение работ по выявлению и оценке угроз безопасности информации, прогнозированию их развития, разработке типового перечня угроз безопасности информации для объектов защиты;

- разработка методических документов по защите информации, конкретизирующих и дополняющих документы федерального уровня;

- оснащение объектов информатизации органов государственной власти, органов местного самоуправления, организаций современными сертифицированными средствами защиты информации (в том числе средствами контроля эффективности защиты информации).

При решении задачи обеспечения эффективной технической защиты информации на объектах органов государственной власти, органов местного самоуправления, организаций осуществляются:

- разработка и внедрение типовых систем защиты информации;

- проведение мероприятий по защите информации при проведении региональных выставок, конференций, совещаний с участием представителей иностранных государств, при осуществлении международного информационного обмена, в том числе с использованием открытых информационных систем;

- использование сертифицированного общего и специального программного обеспечения, сертифицированных средств защиты информации.

При решении задачи совершенствования системы контроля и управления системой защиты информации, приспособленной к изменяющимся условиям обстановки, осуществляются:

- создание системы мониторинга и контроля состояния системы защиты информации в интересах информационного обеспечения принятия решений по защите информации;

- совершенствование взаимодействия органов государственной власти, органов местного самоуправления при организации и ведении защиты информации на территории Смоленской области;

- создание и развертывание информационно-аналитической системы защиты информации на территории Смоленской области в рамках информационно-аналитической системы государственной системы защиты информации.

Главными приоритетами в развитии системы защиты информации на территории Смоленской области являются:

- совершенствование концептуальных и правовых основ деятельности системы защиты информации;
- формирование структурных подразделений по защите информации (назначение штатных специалистов) в органах государственной власти, органах местного самоуправления, организациях, оснащение их средствами защиты информации, а также средствами контроля эффективности защиты информации;
- организация и обеспечение работ по выявлению и оценке угроз безопасности информации, прогнозированию их развития.

#### **4. Этапы формирования и развития системы защиты информации на территории Смоленской области**

Формирование и развитие системы защиты информации в соответствии с настоящей Концепцией предполагается осуществлять в три этапа.

Первый этап (2014 – 2015 гг.) – этап развития и совершенствования системы защиты информации на территории Смоленской области.

В ходе первого этапа:

- расширяется взаимодействие органов государственной власти, органов местного самоуправления, организаций, входящих в систему защиты информации в Смоленской области, при решении задач защиты информации;
- осуществляется разработка правовых, методических, организационно-распорядительных и плановых документов в области защиты информации с учетом внедрения новых информационных технологий;
- производится обеспечение органов государственной власти, органов местного самоуправления, организаций новыми правовыми, методическими, организационно-распорядительными и информационными документами в области защиты информации;
- производится оснащение государственных и муниципальных органов, организаций существующими средствами защиты информации и контроля эффективности защиты информации;
- определяются и уточняются перечни информационных ресурсов, подлежащих защите, определяются структура и порядок деятельности соответствующих систем формирования, учета, хранения и распространения информационных ресурсов;
- создаются структурные подразделения по защите информации (назначаются штатные специалисты) в органах государственной власти, органах местного самоуправления, организациях;
- организуется подготовка и переподготовка специалистов в области защиты информации;
- организуется контроль за состоянием защиты информации в органах государственной власти, органах местного самоуправления, организациях и создается информационно-аналитическая система обеспечения деятельности в области защиты информации;

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

Второй этап (2016 – 2018 гг.) – этап совершенствования координации деятельности органов государственной власти, органов местного самоуправления, организаций по решению задач защиты информации на территории Смоленской области.

† На втором этапе:

- проводится анализ деятельности органов государственной власти, органов местного самоуправления, организаций, а также применяемых ими систем управления и связи в интересах выявления сведений о новых угрозах безопасности информации, наиболее эффективных способах и средствах защиты, построении систем защиты и контроля;

- внедряется информационно-аналитическая система обеспечения деятельности в области защиты информации на территории Смоленской области;

- организуется подготовка, переподготовка и повышение квалификации специалистов в области защиты информации с учетом развития новых информационных технологий;

- совершенствуются организационные мероприятия, технические методы и техника защиты информации на объектах защиты;

- внедряется информационно-аналитическая система выявления, прогнозирования угроз безопасности информации и планирования мероприятий по защите информации;

- разрабатываются методические и технические основы мониторинга безопасности информации в основных ключевых системах информационной структуры на территории Смоленской области.

Третий этап (2019 – 2020 гг.) – этап развития автоматизации деятельности по защите информации в органах государственной власти, органах местного самоуправления, контроля защищенности информации.

На данном этапе также проводится совершенствование системы защиты информации на территории Смоленской области, на котором осуществляется ее интеграция в систему защиты информации в ЦФО и государственную систему защиты информации.

На третьем этапе:

- осуществляется дальнейшее совершенствование методического и технического обеспечения системы защиты информации;

- продолжается оснащение важнейших объектов системы защиты информации перспективными высокоэффективными средствами защиты информации, а также контроля состояния защиты информации;

- совершенствуется система технического контроля защиты информации на территории Смоленской области;

- продолжает осуществляться интеграция информационно-аналитической системы защиты информации Смоленской области в информационно-аналитическую систему государственной системы защиты информации;

- разрабатываются и внедряются системы автоматизированного мониторинга безопасности информации на наиболее важных ключевых системах информационной инфраструктуры Смоленской области;

- внедряются программные и программно-аппаратные средства автоматизации деятельности органов государственной власти, органов местного самоуправления, организаций по организации защиты информации в государственных информационных системах.

## **5. Ожидаемые результаты реализации настоящей Концепции**

Основные положения настоящей Концепции реализуются в результате целенаправленной повседневной деятельности органов государственной власти, органов местного самоуправления, организаций путем выполнения мероприятий по защите информации в рамках реализации федеральных и областных государственных программ.

Реализация настоящей Концепции позволит:

- усовершенствовать организационную структуру системы защиты информации на региональном уровне, ее кадровое обеспечение;
- улучшить обеспеченность органов государственной власти, органов местного самоуправления, организаций документами в области защиты информации;
- повысить оснащенность органов государственной власти, органов местного самоуправления, организаций высокоэффективной техникой защиты информации в условиях расширения спектра угроз безопасности информации в информационных системах, реализующих новые информационные технологии;
- повысить уровень координации деятельности органов государственной власти, органов местного самоуправления, организаций при решении задач защиты информации;
- повысить эффективность управления системой защиты информации за счет совершенствования информационного обеспечения и автоматизации деятельности по защите информации и контролю;
- повысить обоснованность, оперативность и качество управления системой защиты информации за счет создания на территории Смоленской области информационно-аналитической системы защиты информации Смоленской области и ее сопряжения с информационно-аналитической системой государственной системы защиты информации.

В результате планируется создать систему, соответствующую задачам обеспечения национальной безопасности Российской Федерации, безопасности и устойчивого развития Смоленской области с учетом ее экономических возможностей и адекватно реагирующую на угрозы безопасности информации в социально-экономической, административно-управленческой, правоохранительной и других сферах деятельности.

## **6. Финансирование мероприятий по защите информации**

Финансирование мероприятий по защите информации в органах государственной власти, органах местного самоуправления, организациях осуществляется за счет средств соответствующих бюджетов, а также средств внебюджетных источников.