Министерство культуры Российской Федерации
федеральное государственное бюджетное образовательное
учреждение высшего образования
«КРАСНОДАРСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ КУЛЬТУРЫ»

ПРИНЯТО

Решением Ученого совета
24 марта 2026 г.
(протокол № 4)

УТВЕРЖДАЮ

И.о.Ректора_____Н.В.Толмачева

24 марта 2026 г.

ПОЛИТИКА
защиты информации
ФГБОУ ВО «Краснодарский государственный институт культуры»

г. Краснодар
2026 г.

Раздел 1
Общие положения

1. Политика защиты информации в ФГБОУ ВО «Краснодарский государственный институт культуры» (далее – Политика) представляет собой официально принятую ФГБОУ ВО «Краснодарский государственный институт культуры» (далее – Институт) систему взглядов на цели, содержание и основные направления деятельности по обеспечению защиты информации, обрабатываемой в инфраструктуре Института, а также определяет требования и правила по защите информации.

2. Действие Политики распространяется на все структурные подразделения Института. Требования Политики обязательны для выполнения подрядными организациями, имеющими доступ к информационно-телекоммуникационной инфраструктуре Института, и закрепляется в соответствующих договорах (соглашениях).

3. Защите подлежит общедоступная информация, конфиденциальная информация, не содержащая сведений, составляющих государственную тайну (коммерческая тайна, для служебного пользования), персональные данные, обрабатываемые Институтом в границах контролируемых зон объектов информатизации в соответствии с требованиями:

федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных»;

постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказов ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

Национального стандарта Российской Федерации ГОСТ Р 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения», утверждённого приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 № 531-ст;

Национального стандарта Российской Федерации ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения», утверждённого приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 № 532-ст;

Национального стандарта Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», утверждённого приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 № 373-ст;

Государственного стандарта СССР ГОСТ 15971-90 «Системы обработки информации. Термины и определения», утверждённого постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 26.10.90 № 2698.

4. Координацию по вопросам защиты информации в Институте осуществляет отдел информационных технологий и печати (далее – отдел ИТиП).

Раздел 2
Термины и определения

5. В настоящей Политике используются следующие термины и определения:

аттестация объекта информатизации – комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации;

безопасность информации – состояние защищённости информации (данных), при котором обеспечены её (их) конфиденциальность, доступность и целостность;

доступность информации – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно;

защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

информация конфиденциального характера – информация, не содержащая сведения, составляющие государственную тайну, доступ к которой ограничен законодательством Российской Федерации;

информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

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

информационно-телекоммуникационная инфраструктура – это организационно-техническое объединение программных, вычислительных и телекоммуникационных средств и связей между ними, обеспечивающее предоставление информационных, вычислительных и сетевых сервисов;

коммерческая тайна – режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных

обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

конфиденциальность – состояние информации (ресурсов автоматизированной информационной системы), при котором доступ к ней (к ним) осуществляют только субъекты, имеющие на него право;

меры обеспечения информационной безопасности – совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности;

модель угроз – физическое, математическое, описательное представление свойств и характеристик угроз безопасности информации;

нарушитель безопасности информации – физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при её обработке техническими средствами в информационных системах;

несанкционированный доступ к информации – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

обработка информации – систематическое выполнение операций над данными, представляющими предназначенную для обработки информацию;

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных);

подрядная организация – организация, которой на основании договора или иного документа передаётся информация, предоставляется доступ к информационным системам оператора (обладателя информации) и (или) содержащейся в них информации для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а также для выполнения работ, оказания услуг по защите информации;

разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации;

санкционированный доступ к информации – доступ к информации, не нарушающий правила разграничения доступа;

служебная тайна – защищаемая по закону конфиденциальная информация, ставшая известной в Институте только на законных основаниях и

в силу исполнения сотрудниками Института служебных обязанностей, а также служебная информация о деятельности Института, доступ к которой ограничен федеральным законом или в силу служебной необходимости;

средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации;

угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

уязвимость – свойство информационной системы, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации;

целостность – состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

6. В настоящей Политике использованы следующие сокращения:

АТС – автоматическая телефонная станция;

ИБ – информационная безопасность;

ИР – информационный ресурс;

ИС– информационная система;

НСД – несанкционированный доступ;

ОС– операционная система;

ППО – прикладное программное обеспечение;

СОБИ – система обеспечения безопасности информации;

СУБД – система управления базой данных;

ФСБ России – Федеральная служба безопасности Российской Федерации;

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

Раздел 3
Цели и задачи защиты информации

7. Политика разработана для достижения следующих целей:

обеспечение конфиденциальности, целостности, доступности информации, обрабатываемой в структурных подразделениях Института;

защита ИР от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков такого воздействия;

обеспечение безопасного использования ИР Института, получение структурными подразделениями Института и гражданами полной и своевременной информации в условиях возможных внешних и внутренних угроз безопасности информации;

защита прав и свобод граждан, в том числе при обработке их персональных данных в ИС Института;

выполнение требований правовых и нормативных документов Российской Федерации, связанных с обеспечением ИБ.

8. Для достижения указанных целей необходимо выполнение следующих задач защиты информации:

исключение утечки информации ограниченного доступа и иной конфиденциальной информации;

предотвращение НСД к информационным системам и содержащейся в них информации, обнаружение фактов НСД и реагирование на них;

предотвращение несанкционированной модификации информации, обнаружение фактов несанкционированной модификации информации и реагирование на них;

предотвращение несанкционированной подмены информации, обнаружение фактов несанкционированной подмены информации и реагирование на них;

предотвращение несанкционированного удаления информации и программного обеспечения, обнаружение фактов несанкционированного удаления и реагирование на них;

исключение или существенное затруднение отказа в обслуживании авторизованным пользователям ИС;

недопущение использования ИС и содержащейся в них информации не по назначению;

исключение или существенное затруднение нарушения функционирования (работоспособности) ИС;

недопущение распространения с использованием ИС противоправной информации;

обеспечение возможности восстановления в установленные сроки доступа авторизованных пользователей к ИС и содержащейся в них информации, заблокированной вследствие реализации (возникновения) угроз безопасности информации;

обеспечение возможности восстановления в установленные сроки информации, модифицированной или уничтоженной вследствие реализации (возникновения) угроз безопасности информации.

Раздел 4
Принципы защиты информации

9. Основные принципы обеспечения защиты информации в органах Институте:

законность;

системность;

комплексность;

непрерывность;

своевременность;

преемственность и непрерывность совершенствования;

разумная достаточность;

персональная ответственность;
минимизация полномочий;
открытость алгоритмов и механизмов защиты;
специализация и профессионализм;
централизация управления;
гибкость управления и применения;
адекватность и экономическая обоснованность мер защиты информации;
обязательность контроля.

10. Принцип законности предполагает осуществление защитных мероприятий и разработку мер по защите информации Института в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности информации в Российской Федерации.

Пользователи и обслуживающий персонал ИС Института должны иметь представление об ответственности за правонарушения в области систем автоматизированной и неавтоматизированной обработки информации.

11. Принцип системности подхода к построению системы защиты информации предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации в Институте.

При создании системы защиты информации должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределённые системы и НСД к информации. Система защиты информации должна строиться с учётом не только всех известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

Все решения по обеспечению защиты информации в Институте необходимо согласовывать с отделом ИТиП.

12. Принцип комплексности использования методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

13. Принцип непрерывности состоит в том, что защита информации – не разовое мероприятие и не простая совокупность проведённых мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Института, начиная с самых ранних стадий (проектирование), а не только на этапе её эксплуатации.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т. п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты.

14. Принцип своевременности защиты предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации в Институте и реализацию мер обеспечения безопасности информации.

15. Принцип преемственности и совершенствования предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и их систем защиты с учётом достигнутого отечественного и зарубежного опыта в этой области.

16. Принцип разумной достаточности предполагает, что используемые меры и средства обеспечения безопасности информации не должны заметно ухудшать эргономические показатели работы с ИС, в которой эта информация циркулирует.

17. Принцип персональной ответственности предполагает возложение ответственности за обеспечение безопасности информации и системы её обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновных лиц был точно известен или сведён к минимуму.

18. Принцип минимизации полномочий предполагает, что пользователям должны предоставляться минимальные права доступа к информации в соответствии с производственной необходимостью, только в том случае и объёме, который необходим работнику для выполнения должностных обязанностей.

19. Принцип открытости алгоритмов и механизмов защиты предполагает, что безопасность информации не должна обеспечиваться только за счёт секретности структурной организации системы и алгоритмов функционирования её подсистем. Надежность защиты должна определяться устойчивостью самих механизмов и алгоритмов, а также защищенностью ключей, паролей и параметров настройки.

20. Принцип специализации и профессионализма предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ИС, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами, опыт которых подтверждён соответствующими сертификатами.

21. Принцип централизации управления предполагает, что организационные и программно-технические меры обеспечения защиты информации должны быть максимально централизованы и обеспечить функционирование системы безопасности по единым правовым, организационным, функциональным и методологическим принципам. Централизация управления средствами защиты информации должна обеспечивать максимальную информированность персонала, обоснованность, оперативность и минимальные затраты на координацию решений.

22. Принцип гибкости управления и применения предполагает, что система защиты информации должна перестраиваться с минимальными затратами времени и ресурсов при изменении требований к защите, а также обеспечивать защиту не только от известных угроз ИБ, но и от угроз, появление которых возможно в будущем.

23. Принцип адекватности и экономической обоснованности мер защиты информации предполагает, что применяемые меры защиты информации должны быть адекватно сопоставимы модели угроз информации, а также учитывать соотношение между величиной затрат на их реализацию и возможным ущербом от реализации угроз.

24. Принцип обязательности контроля предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и охватывать как несанкционированные, так и санкционированные действия пользователей.

Раздел 5
Объекты защиты

25. К объектам защиты информации в Институте относятся:

25.1. Защищаемая информация:

общедоступные сведения;

персональные данные;

для служебного пользования;

коммерческая тайна, полученная структурными подразделениями Института от третьих лиц в ходе деятельности.

25.2. Технические устройства, предназначенные для создания, обработки, хранения и передачи защищаемой информации:

автоматизированные рабочие места;

файловые серверы;

серверы баз данных;

web-серверы;

системы хранения данных;

системы резервного копирования;

сетевое и коммуникационное оборудование;

телефонные аппараты и офисные АТС;

линии и каналы связи;

другое оборудование, входящее в состав информационно-телекоммуникационной инфраструктуры Института (объектов информатизации).

25.3. Программное обеспечение:

ОС;

ППО обработки защищаемой информации, СУБД и ИР Института;

специальное программное обеспечение.

25.4. Носители защищаемой информации независимо от формы и вида её представления.

25.5. Средства защиты информации, в том числе средства криптографической защиты информации: носители ключевой, парольной и аутентифицирующей информации, системы и программно-аппаратные комплексы, предназначенные для защиты ИР Института.

25.6. Серверные помещения, рабочие кабинеты, места размещения активного сетевого и коммуникационного оборудования.

Раздел 6
Организация деятельности по защите информации

26. С целью достижения поставленных целей и задач должна быть создана СОБИ Института, посредством которой должны быть реализованы следующие мероприятия:

выявление и оценка угроз безопасности информации;

контроль конфигураций ИС;

управление уязвимостями;

управление обновлениями;

обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа;

обеспечение защиты информации при применении конечных устройств;

обеспечение защиты информации при применении мобильных устройств;

обеспечение защиты информации при удалённом доступе пользователей к ИС;

обеспечение защиты информации при беспроводном доступе пользователей к ИС;

обеспечение защиты информации при предоставлении пользователям доступа к ИС, предусматривающего чтение, выполнение, изменение, запись, удаление программ и (или) данных в ИС;

обеспечение мониторинга информационной безопасности;

обеспечение разработки безопасного программного обеспечения;

обеспечение физической защиты ИС;

обеспечение непрерывности функционирования ИС при возникновении нештатных ситуаций;

повышение уровня знаний и информированности пользователей по вопросам защиты информации;

обеспечение защиты информации при взаимодействии с подрядными организациями;

обеспечение защиты от компьютерных атак, направленных на отказ в обслуживании;

обеспечение защиты информации при использовании искусственного интеллекта;

реализация в ИС мер по их защите и защите содержащейся в них информации;

проведение контроля уровня защищённости информации, содержащейся в ИС;

обеспечение непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

27. Для реализации указанных в пункте 26 мероприятий отделом ИТиП в течение трёх месяцев со дня утверждения настоящей Политики разрабатываются (дорабатываются) и утверждаются документы по защите информации, содержащие в том числе:

требования к первичной идентификации лиц, обладающих правами доступа к ИС и (или) содержащейся в них информации и их использованию (далее – пользователи);

требования к применяемым моделям доступа пользователей;

перечень разрешённого и (или) запрещённого для использования программного обеспечения;

требования к типовым конфигурациям и настройкам программных, программно-аппаратных средств;

требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения доступа пользователей из информационных систем к информационно-телекоммуникационной сети Интернет;

требования к конфигурациям и настройкам программных, программно-аппаратных средств, предназначенных для обеспечения удалённого доступа пользователей к ИС и содержащейся в них информации, включая требования к обеспечению безопасной дистанционной работы;

ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими ИС;

требования к защите физических и виртуальных устройств информационных систем, имеющих постоянный доступ к сети Интернет (далее – конечные устройства);

требования к защите мобильных устройств, планшетных, переносных компьютеров, применяемых пользователями для доступа к ИС (за исключением

мобильных устройств, предназначенных для доступа к сайтам сети Интернет и иным публичным веб-ресурсам) (далее – мобильные устройства);

требования к непрерывности функционирования ИС;

требования к резервному копированию информации, программного обеспечения и его конфигураций;

требования к сбору, регистрации и анализу событий, связанных с возможным нарушением безопасности информации, нарушением функционирования ИС, реализацией угроз безопасности информации (далее – события безопасности);

требования к защите информации при подключении к ИС иных ИС, включая требования к каналам передачи данных при взаимодействии с такими ИС;

порядок создания, учёта, изменения и блокирования, контроля, удаления учётных записей;

порядок создания, учёта, изменения и блокирования, контроля, удаления привилегированных учётных записей;

порядок создания, изменения, блокирования, контроля, удаления аутентификационной информации и средств аутентификации;

порядок предоставления пользователям удалённого доступа к ИС и содержащейся в них информации;

порядок и условия предоставления работникам подрядных организаций доступа к ИС, содержащейся в них информации, и (или) передачи им информации, контроля за таким доступом, передачей в случае привлечения подрядных организаций;

порядок предоставления пользователям доступа из ИС в сеть Интернет и контроля её использования;

порядок повышения уровня знаний и информированности пользователей по вопросам защиты информации;

порядок выявления, оценки и устранения уязвимостей ИС (далее – управление уязвимостями);

порядок получения, оценки, тестирования и применения обновлений программных, программно-аппаратных средств (далее – управление обновлениями);

порядок обработки, хранения и обращения с информацией ограниченного доступа;

порядок обеспечения физической защиты ИС;

порядок разработки безопасного программного обеспечения в случае его самостоятельной разработки оператором (обладателем информации);

порядок вывода в контур промышленной эксплуатации сервисов, доступ к которым осуществляется с использованием сети Интернет, в случае наличия таких сервисов;

порядок мониторинга ИБ ИС;

порядок восстановления штатного функционирования ИС и тестирования процессов восстановления;

порядок контроля уровня защищённости информации, содержащейся в ИС.

28. Деятельность Института по защите информации организуется и координируется СОБИ Института. В функционировании СОБИ принимают участие:

ректор Института;

проректор, ответственный за организацию обработки персональных данных;

отдел ИТиП;

канцелярия, в части организации и выполнения требований по защите информации для служебного пользования;

отдел кадров, в части организации и выполнения требований по защите информации по персональным данным;

отдел комплексной безопасности;

сотрудники Института, отвечающие за эксплуатацию ИС и информационно-телекоммуникационных инфраструктур;

сотрудники Института по обеспечению защиты информации;

сотрудники Института.

29. Ректор Института определяет политику и основные направления обеспечения защиты информации в Институте в сооответствии с требованиями законодательства Российской Федерации, постановлений Правительства Российской Федерации, нормативных и методических документов ФСБ России, ФСТЭК России. Утверждает нормативные и правовые документы и требования, обязательные для выполнения структурными подразделениями и сотрудниками Института, имеющими доступ к информационно-телекоммуникационной инфраструктуре Института.

30. Проректор Института, ответственный за организацию обработки персональных данных:

- организует разработку документов и выполнение требований по защите информации в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

-организует разработку практических мер по реализации политики защиты информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации в Институте;

-утверждает планы проведения контрольных мероприятий по выполнению требований ИБ в Институте, представляет отчёты по результатам контрольных мероприятий ректору Института.

31. Отдел ИТиП, в состав которого входит специалист по защите информации, разрабатывает и отвечает за реализацию единой политики в сфере информатизации, ИБ, информационно-коммуникационных технологий и связи.

Отдел ИТиП осуществляет:

формирование и проведение единой политики в области создания, развития и эксплуатации ИС, обеспечения защиты информации в Институте;

разработку предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения создания, развития и эксплуатации ИС, защиты информации в Институте;

разработку и планирование мероприятий по защите информации;

координацию деятельности структурных подразделений Института при проведении работ по созданию, развитию и эксплуатации ИС с соблюдением требований ИБ;

организационно-техническую защиту информации, обрабатываемой средствами вычислительной техники и не относящейся к государственной тайне, иной охраняемой законом тайны, в том числе защиту информации, отнесённой к конфиденциальной, в информационных системах Института;

проведение оценки состояния защиты информации и на её основе совершенствование мероприятий и мер по защите информации;

планирование и представление установленным порядком финансовых затрат для реализации мероприятий по защите информации.

приоритетные направления создания/обновления ИР для работы, в целях повышения эффективности управления бюджетными расходами.

координацию и контроль выполнения организационно-технических мероприятий по вопросам защиты информации в Институте;

проведение классификации ИС обработки информации ограниченного доступа, не содержащей государственной тайны, персональных данных в соответствии с требованиями нормативных правовых документов;

совместно с канцелярией разработку организационных и программно-технических мероприятий по защите информации для служебного пользования, обрабатываемой в Институте, и контроль их исполнения;

развитие, функционирование и использование информационных систем (ресурсов), информационно-телекоммуникационной сети, информационно-коммуникационных технологий и связи, создает условия, обеспечивающие их устойчивое функционирование и комплексное развитие, организует доступ к содержащейся в них информации в установленном порядке и координирует работу по развитию, функционированию и использованию указанных ИС (ресурсов) и информационно-телекоммуникационной сети;

организацию обучения и тестирования работников Института в сфере информатизации, информационно-коммуникационных технологий и защиты информации;

контроль выполнения требований по защите информации в Институте.

32. Работники Института, отвечающие за эксплуатацию ИСи информационно-телекоммуникационных инфраструктур, обеспечивают выполнение требований по защите информации как на этапе их создания, так и

в ходе эксплуатации, в соответствии с руководящими документами по защите информации и эксплуатационной документацией.

33. Ответственные работники Института по обеспечению защиты информации организуют выполнение требований по защите информации в ИС, информационно-телекоммуникационных системах Института, обладателями (операторами) которых они являются, в соответствии с нормативными правовыми документами Российской Федерации, методическими рекомендациями и предписаниями ФСБ России, ФСТЭК России, нормативными актами Института.

34. Работники Института должны знать и выполнять требования по защите информации в рамках исполнения своих должностных обязанностей.

35. При взаимодействии структурных подразделений Института с подрядными организациями должны быть обеспечены мероприятия по защите информации:

в договорах должны быть установлены обязанности подрядных организаций по обеспечению защиты информации, к которой получен доступ, а также ответственность за невыполнение этой обязанности;

не допускать копирование подрядными организациями информации, к которой им предоставлен доступ, если такое копирование не предусмотрено в договорах или иных документах;

в ИС, отдельных программно-аппаратных средствах подрядных организаций, в которых осуществляется обработка и хранение полученной в результате предоставления доступа информации, должны быть приняты меры по защите информации;

не допускать разработку (развитие) и (или) тестирование программного обеспечения подрядными организациями непосредственно в контуре промышленной эксплуатации ИС.

Раздел 7
Ответственность за нарушение требований защиты информации

36. Нарушение требований по защите информации рассматривается как ненадлежащее исполнение должностных обязанностей. Лица, допустившие нарушение требований по защите информации, привлекаются к ответственности в соответствии с законодательством Российской Федерации.

Раздел 8
Механизм реализации Политики

37. Реализация настоящей Политики должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

федеральных законов в области защиты информации;

Указов Президента Российской Федерации;

постановлений Правительства Российской Федерации;

руководящих, организационно-распорядительных и методических документов ФСБ России, ФСТЭК России.

38. Для выполнения задач настоящей Политики необходимы:

функционирование СОБИ;

издание локальных нормативных актов Института, включающих в себя обязательные требования по выполнению положений политики ИБ;

аудит Института на предмет защищённости обрабатываемой информации;

разработка модели угроз Института и частных моделей угроз для отдельных информационных систем Института;

разработка технического проекта системы защиты информации Института;

разработка технического задания на создание системы защиты информации Института;

разработка организационно-распорядительных документов Института;

поставка, пусконаладка средств защиты информации в соответствии с техническим проектом системы защиты информации Института;

аттестация ИС Института по требованиям безопасности информации (типовых сегментов ИС).

Раздел 9
Ожидаемый эффект от реализации концепции

39. Применение настоящей Политики в Институте позволит:

оценить состояние безопасности информации, циркулирующей в ИС Института, выявить источники внутренних и внешних угроз ИБ, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

разработать распорядительные и нормативно-методические документы применительно к обеспечению ИБ в Институте;

провести организационно-режимные и технические мероприятия по обеспечению безопасности информации ограниченного доступа в Институте;

обеспечить необходимый уровень безопасности объектов защиты для создания и дальнейшего совершенствования единой, целостной и скоординированной СОБИ Института.