|  |  |
| --- | --- |
|  | УТВЕРЖДЕНО |
|  |  |
|  | Приказом №1-ОП от «21» июля 2014 года |
|  | директором ФОНДА «ТРИОНИКС» |
|  |  |
| **Образовательная программа** | |
| **дополнительная профессиональная программа** | |
| **(программа повышения квалификации)** | |
| **по специальности** | |
| **Информационная безопасность** | |
|  | |

1. **Наименование образовательной программы**

Наименование образовательной программы: дополнительная профессиональная программа (программа повышения квалификации и программа профессиональной переподготовки) по специальности **Информационная безопасность**.

1. **Общие положения**

Настоящая образовательная программа устанавливает правила организации и осуществления образовательной деятельности по дополнительным профессиональным программам, с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование, указанным в договоре об образовании, и является обязательной для всех участников отношений в сфере образования.

ФОНД «ТРИОНИКС» самостоятельно определяет содержание образования, выбирает учебно-методическое обеспечение, образовательные технологии, формы, средства, методы обучения, учебники, учебные пособия, материалы и иные средства обучения по реализуемым им образовательным программам, с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование, и указывает их в договоре об образовании.

1. **Условия обучения**
   1. **Платность услуг**

ФОНД «ТРИОНИКС» осуществляет обучение по настоящей образовательной программе на основе договора об образовании, заключаемого со слушателем и (или) с физическим или юридическим лицом, обязующимся оплатить обучение лица, зачисляемого на обучение.

* 1. **Лица, допускаемые к обучению по образовательной программе**

К обучению по настоящей образовательной программе допускаются только взрослые лица:

* имеющие среднее профессиональное и (или) высшее образование;
* или получающие среднее профессиональное и (или) высшее образование.

При освоении дополнительных профессиональных программ профессиональной переподготовки возможен зачет учебных предметов, курсов, дисциплин (модулей), освоенных в процессе предшествующего обучения по основным профессиональным образовательным программам и (или) дополнительным профессиональным программам, объем которого определяется индивидуально.

* 1. **Требования к знаниям, навыкам и умениям, необходимым для успешного освоения образовательной программы**

Для успешного усвоения дисциплины требований к обучающимся о владении знаниями, умениями и навыками, сформированными в процессе обучения по другим курсам/специальностям не предъявляется.

* 1. **Образовательные программы, в которых используются результаты настоящей образовательной программы**

Образовательные программы, в которых используются результаты настоящей образовательной программы:

* Документоведение;
* Менеджмент;
* Экономика и управление в организации;
* Автоматические системы управления;
* Государственное и муниципальное управление;
* Бизнес-информатика;
* Прикладная информатика;
* Управление и информатика в технических системах;
* Информационные системы;
* Организационно-технические системы;
* Деловое администрирование.
  1. **Цели, планируемые результаты и приобретаемые компетенции**
     1. **Цели**

Целью обучения по образовательной программе является достижение планируемых результатов по совершенствованию и (или) получению компетенции, необходимой для выполнения нового вида профессиональной деятельности, повышению профессионального уровня в рамках имеющейся квалификации, приобретению новой квалификации.

Цель обучения по образовательной программе указывается в договоре об образовании.

* + 1. **Профессии и квалификационные требования**

Обучение по образовательной программе осуществляется в соответствии с:

* Приказом Минздравсоцразвития РФ от 22.04.2009 №205 «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».

Конкретная профессия, должность или перечень квалификационных требований указывается в договоре об образовании.

* + 1. **Планируемые результаты**

Реализация программы **повышения квалификации** направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации

Реализация программы **профессиональной переподготовки** направлена на получение компетенции, необходимой для выполнения нового вида профессиональной деятельности, приобретение новой квалификации.

Образовательная программа разрабатывается на основании установленных квалификационных требований, профессиональных стандартов и требований соответствующих федеральных государственных образовательных стандартов среднего профессионального и (или) высшего образования к результатам освоения образовательных программ.

* + - 1. **Соответствие федеральным государственным образовательным стандартам**

Настоящая образовательная программа соответствует требованиям ФГОС:

* Приказ Минобрнауки РФ от 17.01.2011 №60 «Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки (специальности) 090303 Информационная безопасность автоматизированных систем (квалификация (степень) «специалист»)»;
* Приказ Минобрнауки РФ от 17.01.2011 №50 «Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки (специальности) 090302 Информационная безопасность телекоммуникационных систем (квалификация (степень) «специалист»)»;
* Приказ Минобрнауки РФ от 28.10.2009 №496 «Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «бакалавр»)»;
* Приказ Минобрнауки РФ от 28.10.2009 №497 «Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «магистр»)»;
* Приказ Минобрнауки РФ от 24.06.2010 №708 «Об утверждении и введении в действие федерального государственного образовательного стандарта среднего профессионального образования по специальности 090305 Информационная безопасность автоматизированных систем»;
* Приказ Минобрнауки РФ от 23.06.2010 №683 «Об утверждении и введении в действие федерального государственного образовательного стандарта среднего профессионального образования по специальности 090303 Информационная безопасность телекоммуникационных систем».
  + - 1. **Область профессиональной деятельности**

Область профессиональной деятельности по настоящей образовательной программе включает:

* сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением информационной безопасности автоматизированных систем в условиях существования угроз в информационной сфере;
* сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере;
* организация и проведение работ по обеспечению защиты автоматизированных систем в организациях различных структур и отраслевой направленности;
* организация и проведение работ по техническому обслуживанию и обеспечению информационной безопасности телекоммуникационных сетей и систем в организациях различных структур и отраслевой направленности.

Конкретная область профессиональной деятельности указывается в договоре об образовании.

* + - 1. **Объекты профессиональной деятельности**

Объектами профессиональной деятельности по настоящей образовательной программе являются:

* автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;
* информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и за действующие информационно-технологические ресурсы, подлежащие защите;
* технологии обеспечения информационной безопасности автоматизированных систем;
* системы управления информационной безопасностью автоматизированных систем;
* технологии обеспечения информационной безопасности автоматизированных систем;
* объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере;
* технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;
* фундаментальные проблемы информационной безопасности в условиях становления современного информационного общества;
* информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы;
* организационно-правовые механизмы обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующие создание и использование информационных ресурсов, средств защиты информации, проведение экспертизы, стандартизации, сертификации и контроля качества защиты информации и информационных ресурсов;
* технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта);
* методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности объектов информатизации;
* процессы управления информационной безопасностью защищаемых объектов, методы и средства оптимизации процессов управления;
* методы и средства обеспечения информационной безопасности автоматизированных систем;
* первичные трудовые коллективы;
* технические средства телекоммуникационных систем;
* средства обеспечения информационной безопасности телекоммуникационных систем;
* технические средства защиты информации.

Конкретный объект профессиональной деятельности может уточняться ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

* + - 1. **Виды профессиональной деятельности**

Обучающийся по настоящей образовательной программе готовится к следующим видам профессиональной деятельности:

* научно-исследовательская;
* проектно-конструкторская;
* контрольно-аналитическая;
* организационно-управленческая;
* эксплуатационная;
* проектно-технологическая;
* экспериментально-исследовательская;
* проектная;
* научно-педагогическая;
* эксплуатация подсистем безопасности автоматизированных систем;
* применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах;
* применение инженерно-технических средств обеспечения информационной безопасности;
* выполнение работ по одной или нескольким профессиям рабочих, должностям служащих;
* эксплуатация комплексных систем обеспечения информационной безопасности в автоматизированных системах;
* техническое обслуживание оборудования защищенных телекоммуникационных систем;
* применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем;
* участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем;
* участие в реализации комплексной информационной безопасности телекоммуникационных систем.

Конкретные виды профессиональной деятельности определяются ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

* + - 1. **Профессиональные задачи в соответствии с видами профессиональной деятельности**

Обучающийся по настоящей образовательной программе должен решать следующие профессиональные задачи в соответствии с видами профессиональной деятельности:

**научно-исследовательская деятельность:**

* сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем;
* подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;
* моделирование и исследование защищенных автоматизированных систем, анализ их уязвимостей и эффективности средств и способов защиты;
* анализ безопасности информационных технологий, реализуемых в автоматизированных системах;
* разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;
* анализ фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества;
* разработка планов и программ проведения научных исследований и технических разработок, подготовка отдельных заданий для исполнителей;
* выполнение научных исследований по выбранной теме;
* подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях.

**проектно-конструкторская деятельность:**

* сбор и анализ исходных данных для проектирования систем защиты информации;
* разработка политик информационной безопасности автоматизированных систем;
* разработка защищенных автоматизированных систем по профилю профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;
* выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
* разработка системы управления информационной безопасностью автоматизированных систем;

**контрольно-аналитическая:**

* контроль работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
* экспериментально-исследовательские работы при сертификации средств защиты автоматизированных систем;
* экспериментально-исследовательские работы при аттестации автоматизированных систем;
* инструментальный мониторинг защищенности автоматизированных систем;

**организационно-управленческая деятельность:**

* организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
* разработка предложений по совершенствованию и повышению эффективности принятых мер по обеспечению информационной безопасности автоматизированных систем;
* организация работ по выполнению требований защиты информации ограниченного доступа;
* методическое и организационное обеспечение информационной безопасности автоматизированных систем;
* организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
* контроль реализации политики информационной безопасности;

**эксплуатационная деятельность:**

* реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;
* администрирование подсистем информационной безопасности автоматизированных систем;
* мониторинг информационной безопасности автоматизированных систем;
* управление информационной безопасностью автоматизированных систем;
* обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций;
* установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
* участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
* администрирование подсистем информационной безопасности объекта;

**проектно-технологическая деятельность:**

* сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
* проведение проектных расчетов элементов систем обеспечения информационной безопасности;
* участие в разработке технологической и эксплуатационной документации;
* проведение предварительного технико-экономического обоснования проектных расчетов;

**экспериментально-исследовательская деятельность:**

* сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
* проведение экспериментов по заданной методике, обработка и анализ результатов;
* проведение вычислительных экспериментов с использованием стандартных программных средств;

**организационно-управленческая деятельность:**

* осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
* организация работы малых коллективов исполнителей с учетом требований защиты информации;
* совершенствование системы управления информационной безопасностью;
* изучение и обобщение опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны;
* контроль эффективности реализации политики информационной безопасности объекта;

**проектная деятельность:**

* системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев информационной безопасности, согласованных со стратегией развития информационных систем;
* концептуальное проектирование сложных систем, комплексов средств и технологий обеспечения информационной безопасности;
* обоснование выбора функциональной структуры, принципов организации технического, программного и информационного обеспечения систем, средств и технологий обеспечения информационной безопасности объектов защиты;
* разработка систем и технологий обеспечения информационной безопасности;
* адаптация к защищаемым объектам современных методов обеспечения информационной безопасности на основе отечественных и международных стандартов;

**научно-педагогическая деятельность:**

* выполнение педагогической работы в средних специальных и высших учебных заведениях в должностях преподавателя и ассистента под руководством ведущего преподавателя и профессора (доцента) по дисциплинам направления;
* разработка методических материалов, используемых студентами в учебном процессе;

**организационно-управленческая деятельность:**

* организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
* участие в работах по созданию, изготовлению, монтажу, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности;
* разработка проектов методических и нормативных документов, предложений и мероприятий по реализации разработанных проектов и программ, программ и методик испытаний;
* организация тестирования и отладки программно-аппаратных, криптографических и технических систем и средств обеспечения информационной безопасности;
* организация работы по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральная службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

**эксплуатация подсистем безопасности автоматизированных систем:**

* участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности;
* выполнять работы по администрированию подсистем безопасности автоматизированных систем;
* производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем;
* организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них;
* вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах;

**применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах:**

* применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах;
* участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности;
* участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах;
* участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
* решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов;
* применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

**применение инженерно-технических средств обеспечения информационной безопасности:**

* применять инженерно-технические средства обеспечения информационной безопасности;
* участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности;
* участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности;
* решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств;
* применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами;

**эксплуатация комплексных систем обеспечения информационной безопасности в автоматизированных системах:**

* участвовать в разработке организационной структуры комплексной системы обеспечения информационной безопасности;
* участвовать в оценке эффективности комплексной системы обеспечения информационной безопасности;
* участвовать в мониторинге эффективности комплексных систем обеспечения информационной безопасности;

**техническое обслуживание оборудования защищенных телекоммуникационных систем:**

* устанавливать, конфигурировать оборудование защищенных телекоммуникационных систем;
* эксплуатировать оборудование защищенных телекоммуникационных систем;
* осуществлять техническое обслуживание, диагностирование, устранение отказов, настройку и ремонт оборудования, проводить его аттестацию;
* осуществлять анализ качественных и количественных показателей функционирования оборудования;
* организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации телекоммуникационных систем и средств защиты информации в них;

**применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем:**

* осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем;
* обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению;
* формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем;
* вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей;

**участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем:**

* руководствоваться законодательными и нормативными документами в области обеспечения информационной безопасности телекоммуникационных систем, защиты государственной тайны и конфиденциальной информации;
* участвовать в подготовке и проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации;
* участвовать во внедрении разработанных технических решений и проектов во взаимодействии с другими специалистами, оказывать техническую помощь исполнителям при изготовлении, монтаже, настройке, испытаниях и эксплуатации технических средств;
* участвовать в организации работы малого коллектива исполнителей с учетом требований режима защиты информации и сохранения государственной тайны;

**участие в реализации комплексной информационной безопасности телекоммуникационных систем:**

* осуществлять сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике информационной безопасности телекоммуникационных систем;
* осуществлять проектные расчеты элементов систем обеспечения информационной безопасности;
* участвовать в работах по реализации политики комплексного обеспечения информационной безопасности телекоммуникационных систем;
* участвовать в мониторинге эффективности информационной безопасности телекоммуникационных систем.

По согласованию с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование, перечень общекультурных и профессиональных компетенций, качественное изменение которых осуществляется в результате обучения по настоящей образовательной программе, может дополняться общекультурными и профессиональными компетенциями, качественное изменение которых осуществляется в результате обучения ФОНДОМ «ТРИОНИКС» в рамках других образовательных программ.

Конкретные виды профессиональных задач в соответствии с видами профессиональной деятельности определяются ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

* + - 1. **Компетенции**

Обучающийся по настоящей образовательной программе должен обладать следующими общекультурными компетенциями:

* способностью действовать в соответствии с Конституцией Российской Федерации, исполнять свой гражданский и профессиональный долг, руководствуясь принципами законности и патриотизма;
* способностью осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе морально-нравственных и правовых норм, соблюдать принципы профессиональной этики;
* способностью анализировать социально значимые явления и процессы, в том числе политического и экономического характера, мировоззренческие и философские проблемы, применять основные положения и методы гуманитарных, социальных и экономических наук при решении социальных и профессиональных задач;
* способностью понимать движущие силы и закономерности исторического процесса, роль личности в истории, политической организации общества, способностью уважительно и бережно относиться к историческому наследию, толерантно воспринимать социальные и культурные различия;
* способностью понимать социальную значимость своей будущей профессии, цели и смысл государственной службы, обладать высокой мотивацией к профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;
* способностью к работе в коллективе, кооперации с коллегами, способностью в качестве руководителя подразделения, лидера группы сотрудников формировать цели команды, принимать организационно-управленческие решения в нестандартных ситуациях и нести за них ответственность, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности;
* способностью логически верно, аргументировано и ясно строить устную и письменную речь на русском языке, готовить и редактировать тексты профессионального назначения, публично представлять собственные и известные научные результаты, вести дискуссии;
* способностью к письменной и устной деловой коммуникации, к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков;
* способностью к логическому мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания;
* способностью самостоятельно применять методы и средства познания, обучения и самоконтроля для приобретения новых знаний и умений, в том числе в новых областях, непосредственно не связанных со сферой профессиональной деятельности, развития социальных и профессиональных компетенций, к изменению вида своей профессиональной деятельности;
* способностью к воспитательной и образовательной деятельности;
* способностью самостоятельно применять методы физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, достижения должного уровня физической подготовленности в целях обеспечения полноценной социальной и профессиональной деятельности;
* способностью уважительно и бережно относиться к историческому наследию и культурным традициям, толерантно воспринимать социальные и культурные различия;
* способностью понимать и анализировать политические события, мировоззренческие, экономические и социально значимые проблемы и процессы, применять основные положения и методы социальных, гуманитарных и экономических наук при решении социальных и профессиональных задач;
* способностью к кооперации с коллегами, работе в коллективе;
* способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность;
* способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной состязательной деятельности в условиях информационного противоборства;
* способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления;
* способностью логически верно, аргументировано и ясно строить устную и письменную речь, публично представлять собственные и известные научные результаты, вести дискуссии;
* способностью к чтению и переводу текстов по профессиональной тематике на одном из иностранных языков, владеть им на уровне не ниже разговорного;
* способностью к саморазвитию, самореализации, приобретению новых знаний, повышению своей квалификации и мастерства;
* способностью критически оценивать свои достоинства и недостатки, определять пути и выбрать средства развития достоинств и устранения недостатков;
* способностью к самостоятельному применению методов физического воспитания для повышения адаптационных резервов организма и укрепления здоровья, готовностью к достижению должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности;
* способностью совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности;
* способностью к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности;
* способностью свободно пользоваться русским и одним из иностранных языков как средством делового общения;
* способностью использовать на практике умения и навыки в организации научно-исследовательских и проектных работ, в управлении коллективом;
* способностью проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности;
* способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности;
* понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности;
* организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
* принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность;
* осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;
* использовать информационно-коммуникационные технологии в профессиональной деятельности;
* работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями;
* брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий;
* самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации;
* ориентироваться в условиях частой смены технологий в профессиональной деятельности;
* исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей);
* формулировать задачи логического характера и применять средства математической логики для их решения;
* владеть основными методами и средствами разработки программного обеспечения;
* производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах;
* понимать физическую сущность задач, возникающих в ходе профессиональной деятельности, и применять соответствующий физический аппарат для их решения;
* использовать вычислительную технику и прикладные программные пакеты для решения профессиональных задач;
* ориентироваться в элементной базе устройств телекоммуникационных систем и обеспечения их информационной безопасности.

Обучающийся по настоящей образовательной программе должен обладать следующими профессиональными компетенциями:

**общепрофессиональными:**

* способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения;
* способностью применять математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач;
* способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности;
* способностью понимать сущность и значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска и обработки больших объемов информации по профилю деятельности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации;
* способностью применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;
* способностью использовать нормативные правовые акты в своей профессиональной деятельности;
* способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;
* способностью к освоению новых образцов программных, технических средств и информационных технологий;
* способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности;
* способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах;
* способностью использовать нормативные правовые документы в своей профессиональной деятельности;
* способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;
* способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;
* способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов;
* способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;

**в научно-исследовательской деятельности:**

* способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности;
* способностью применять современные методы исследования с использованием компьютерных технологий;
* способностью разрабатывать и исследовать модели автоматизированных систем;
* способностью проводить анализ защищенности автоматизированных систем;
* способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;
* способностью проводить анализ рисков информационной безопасности автоматизированной системы;
* способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем;
* способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;
* способен анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;
* способен анализировать угрозы информационной безопасности объектов и разрабатывать методы противодействия им;
* способен осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методик и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок;
* способен проводить экспериментальные исследования защищенности объектов с применением современных математических методов, технических и программных средств обработки результатов эксперимента;
* способен оформлять научно-технические отчеты, обзоры, готовить публикации по результатам выполненных исследований, научные доклады;

**в проектно-конструкторской деятельности:**

* способностью проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем;
* способностью участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;
* способностью участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности;
* способностью разрабатывать политики информационной безопасности автоматизированных систем;
* способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;
* способностью участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы;

**в контрольно-аналитической деятельности:**

* способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
* способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем;
* способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации;
* способностью проводить инструментальный мониторинг защищенности автоматизированных систем;

**в организационно-управленческой деятельности:**

* способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;
* способностью разрабатывать оперативные планы работы первичных подразделений;
* способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;
* способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности;
* способностью разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности;
* способностью проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите;
* способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
* способностью формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы;
* способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
* способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью;
* способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
* способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации;
* способностью участвовать в работах по реализации политики информационной безопасности;
* способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности;
* способностью организовать работу малого коллектива исполнителей с учетом требований защиты информации;
* способностью организовать мероприятия по охране труда и технике безопасности в процессе эксплуатации и технического обслуживания средств защиты информации;
* способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю;
* способен организовать работу коллектива исполнителей, принимать управленческие решения в условиях спектра мнений, определять порядок выполнения работ;
* способен организовать работу по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России;
* способен разрабатывать проекты методических и нормативных документов, технической документации, а также предложения и мероприятия по реализации разработанных проектов и программ;
* способен организовать и выполнить работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности;

**в эксплуатационной деятельности:**

* способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
* способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы;
* способностью администрировать подсистему информационной безопасности автоматизированной системы;
* способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы;
* способностью управлять информационной безопасностью автоматизированной системы;
* способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций;
* способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия;
* способностью администрировать подсистемы информационной безопасности объекта;
* способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

**в профессионально-специализированной деятельности:**

* способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;
* способностью участвовать в разработке средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;
* способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов;
* способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов;
* способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов;
* способностью восстанавливать работоспособность средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов;
* способностью проводить анализ и исследовать модели защищенности открытых информационных систем;
* способностью участвовать в разработке компонентов открытых информационных систем;
* способностью обеспечить эффективное применение информационно-технологических ресурсов открытых информационных систем с учетом нормативных требований по защите информации;
* способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем;
* способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью открытой информационной системы;
* способностью проводить инструментальный мониторинг защищенности открытых информационных систем;
* способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью открытой информационной системы;
* способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем;
* способностью проводить анализ и исследовать модели автоматизированных банковских систем;
* способностью на практике применять стандарты, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;
* способностью на практике применять криптографические протоколы и стандарты при обеспечении информационной безопасности автоматизированных банковских систем;
* способностью проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем;
* способностью обеспечивать эффективное применение информационно-технологических ресурсов автоматизированных банковских систем с учетом нормативных требований по защите информации;
* способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем;
* способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью автоматизированных банковских систем;
* способностью проводить инструментальный мониторинг защищенности автоматизированных банковских систем;
* способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной банковской системы;
* способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы;
* способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления;
* способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления;
* способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях;
* способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления;
* способностью планировать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью защищенных автоматизированных систем управления и организаций;
* способностью применять современные технологии проектирования защищенных автоматизированных систем управления;
* способностью участвовать в разработке и оценке соответствия средств защиты информации подсистем обеспечения информационной безопасности защищенных автоматизированных систем управления нормативным требованиям по защите информации;
* способностью разрабатывать и исследовать модели информационно-технологических ресурсов в распределенных информационных системах;
* способностью разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах;
* способностью проводить анализ рисков информационной безопасности в распределенных информационных системах;
* способностью разрабатывать и руководить разработкой политики безопасности распределенных информационных систем;
* способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем;
* способностью проводить удаленное администрирование операционных систем в распределенных информационных системах;
* способностью проводить удаленное администрирование систем баз данных в распределенных информационных системах;
* способностью координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации;
* способностью применять криптографические протоколы для передачи и хранения данных в распределенных информационных системах;
* способностью использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты;
* способностью разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации;
* способностью применять инструментарий анализа безопасности программного обеспечения;
* способностью применять методы дизассемблирования программ и методы восстановления алгоритма программы по ее дезассемблированному коду;
* способностью принимать участие в проведении исследований и испытаний защищенных информационных систем;
* способностью участвовать в сертификационных испытаниях по существующим требованиям;
* способностью разрабатывать модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* способностью принимать участие в разработке, реализации и управлении процессами создания и эксплуатации автоматизированных систем в защищенном исполнении на всех стадиях и этапах их жизненного цикла;
* способностью рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* способностью применять современные технологии проектирования автоматизированных систем в защищенном исполнении;
* способностью применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла;
* способностью проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* способностью участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;
* способностью применять программные, программно-аппаратные и технические методы и средства защиты информации в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах транспорта;
* способностью разрабатывать предложения по совершенствованию мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах транспорта;
* способностью проводить оценку эффективности средств защиты информации, использующихся в автоматизированных, информационно-управляющих и информационно-логистических системах транспорта;
* способностью разрабатывать политику безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;
* способностью разрабатывать предложения по совершенствованию системы аудита и управления информационной безопасностью автоматизированных и информационно-управляющих систем транспорта;
* способностью осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта с учетом нормативных требований по защите информации;
* способностью осуществлять рациональный выбор элементной базы обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;
* способностью обеспечить эффективное применение средств защиты технологического электронного документооборота и технического документоведения на транспорте;
* способностью выявлять и прогнозировать угрозы информационной безопасности автоматизированных и информационно-управляющих систем транспорта, разрабатывать меры противодействия;
* способностью проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;
* способностью участвовать в разработке средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов;
* способностью применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов;
* способностью разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов;
* способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов;
* способностью восстанавливать работоспособность средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов;
* способностью проводить анализ и исследовать модели защищенности открытых информационных систем;
* способностью участвовать в разработке компонентов открытых информационных систем;
* способностью обеспечить эффективное применение информационно-технологических ресурсов открытых информационных систем с учетом нормативных требований по защите информации;
* способностью разрабатывать и реализовывать политики информационной безопасности открытых информационных систем;
* способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью открытой информационной системы;
* способностью проводить инструментальный мониторинг защищенности открытых информационных систем;
* способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью открытой информационной системы;
* способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем;
* способностью проводить анализ и исследовать модели автоматизированных банковских систем;
* способностью на практике применять стандарты, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;
* способностью на практике применять криптографические протоколы и стандарты при обеспечении информационной безопасности автоматизированных банковских систем;
* способностью проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем;
* способностью обеспечивать эффективное применение информационно-технологических ресурсов автоматизированных банковских систем с учетом нормативных требований по защите информации;
* способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем;
* способностью участвовать в проектировании и эксплуатации системы управления информационной безопасностью автоматизированных банковских систем;
* способностью проводить инструментальный мониторинг защищенности автоматизированных банковских систем;
* способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной банковской системы;
* способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы;
* способностью разрабатывать алгоритмы управления для защищенных автоматизированных систем управления на основе методов теории управления;
* способностью выбирать методы и разрабатывать алгоритмы принятия решений в защищенных автоматизированных системах управления;
* способностью выявлять режимы работы элементов защищенных автоматизированных систем управления и внешние воздействия на них, способствующие увеличению риска утечки информации в различных физических полях;
* способностью участвовать в разработке подсистем мониторинга информационной безопасности защищенных автоматизированных систем управления;
* способностью планировать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью защищенных автоматизированных систем управления и организаций;
* способностью применять современные технологии проектирования защищенных автоматизированных систем управления;
* способностью участвовать в разработке и оценке соответствия средств защиты информации подсистем обеспечения информационной безопасности защищенных автоматизированных систем управления нормативным требованиям по защите информации;
* способностью разрабатывать и исследовать модели информационно-технологических ресурсов в распределенных информационных системах;
* способностью разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах;
* способностью проводить анализ рисков информационной безопасности в распределенных информационных системах;
* способностью разрабатывать и руководить разработкой политики безопасности распределенных информационных систем;
* способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем;
* способностью проводить удаленное администрирование операционных систем в распределенных информационных системах;
* способностью проводить удаленное администрирование систем баз данных в распределенных информационных системах;
* способностью координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации;
* способностью применять криптографические протоколы для передачи и хранения данных в распределенных информационных системах;
* способностью использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты;
* способностью разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации;
* способностью применять инструментарий анализа безопасности программного обеспечения;
* способностью применять методы дизассемблирования программ и методы восстановления алгоритма программы по ее дезассемблированному коду;
* способностью принимать участие в проведении исследований и испытаний защищенных информационных систем;
* способностью участвовать в сертификационных испытаниях по существующим требованиям;
* способностью разрабатывать модели угроз и модели нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* способностью принимать участие в разработке, реализации и управлении процессами создания и эксплуатации автоматизированных систем в защищенном исполнении на всех стадиях и этапах их жизненного цикла;
* способностью рационально выбирать методы и средства для реализации процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* способностью применять современные технологии проектирования автоматизированных систем в защищенном исполнении;
* способностью применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла;
* способностью проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* способностью участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;
* способностью применять программные, программно-аппаратные и технические методы и средства защиты информации в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах транспорта;
* способностью разрабатывать предложения по совершенствованию мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах транспорта;
* способностью проводить оценку эффективности средств защиты информации, использующихся в автоматизированных, информационно-управляющих и информационно-логистических системах транспорта;
* способностью разрабатывать политику безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;
* способностью разрабатывать предложения по совершенствованию системы аудита и управления информационной безопасностью автоматизированных и информационно-управляющих систем транспорта;
* способностью осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта с учетом нормативных требований по защите информации;
* способностью осуществлять рациональный выбор элементной базы обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;
* способностью обеспечить эффективное применение средств защиты технологического электронного документооборота и технического документоведения на транспорте;
* способностью выявлять и прогнозировать угрозы информационной безопасности автоматизированных и информационно-управляющих систем транспорта, разрабатывать меры противодействия;

**в проектно-технологической деятельности:**

* способностью участвовать в разработке подсистемы управления информационной безопасностью;
* способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;
* способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности;
* способностью применять программные средства системного, прикладного и специального назначения;
* способностью использовать инструментальные средства и системы программирования для решения профессиональных задач;
* способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности;
* способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

**в экспериментально-исследовательской деятельности:**

* способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности;
* способностью применять методы анализа изучаемых явлений, процессов и проектных решений;
* способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;
* способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов;
* способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности;
* способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;

**в проектной деятельности:**

* способностью понимать и анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности, оценивать затраты и риски, формировать стратегию создания систем информационной безопасности в соответствии со стратегией развития организации;
* способностью проектировать сложные системы и комплексы управления информационной безопасностью с учетом особенностей объектов защиты;
* способностью произвести и детально обосновать выбор структуры, принципов организации, комплекса средств и технологий обеспечения информационной безопасности объектов защиты;
* способностью самостоятельно осваивать и адаптировать к защищаемым объектам современные методы обеспечения информационной безопасности, вновь вводимые отечественные и международные стандарты;
* способностью разработать программы и методики испытаний, организовать тестирование и отладку программно-аппаратных, криптографических и технических систем и средств обеспечения информационной безопасности;

**в научно-педагогической деятельности:**

* способен выполнять педагогическую работу в средних специальных и высших учебных заведениях в должностях преподавателя и ассистента под руководством ведущего преподавателя и профессора (доцента) по дисциплинам направления;
* способен разрабатывать методические материалы, используемые студентами в учебном процессе;

**эксплуатация подсистем безопасности автоматизированных систем:**

* участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности;
* выполнять работы по администрированию подсистем безопасности автоматизированных систем;
* производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем;
* организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них;
* вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах;

**применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах:**

* применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах;
* участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности;
* участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах;
* участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
* решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов;
* применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

**применение инженерно-технических средств обеспечения информационной безопасности:**

* применять инженерно-технические средства обеспечения информационной безопасности;
* участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности;
* участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности;
* решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств;
* применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами;

**эксплуатация комплексных систем обеспечения информационной безопасности в автоматизированных системах:**

* участвовать в разработке организационной структуры комплексной системы обеспечения информационной безопасности;
* участвовать в оценке эффективности комплексной системы обеспечения информационной безопасности;
* участвовать в мониторинге эффективности комплексных систем обеспечения информационной безопасности;

**техническое обслуживание оборудования защищенных телекоммуникационных систем:**

* устанавливать, конфигурировать оборудование защищенных телекоммуникационных систем;
* эксплуатировать оборудование защищенных телекоммуникационных систем;
* осуществлять техническое обслуживание, диагностирование, устранение отказов, настройку и ремонт оборудования, проводить его аттестацию;
* осуществлять анализ качественных и количественных показателей функционирования оборудования;
* организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации телекоммуникационных систем и средств защиты информации в них;

**применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем:**

* осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем;
* обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранению;
* формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем;
* вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей;

**участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем:**

* руководствоваться законодательными и нормативными документами в области обеспечения информационной безопасности телекоммуникационных систем, защиты государственной тайны и конфиденциальной информации;
* участвовать в подготовке и проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации;
* участвовать во внедрении разработанных технических решений и проектов во взаимодействии с другими специалистами, оказывать техническую помощь исполнителям при изготовлении, монтаже, настройке, испытаниях и эксплуатации технических средств;
* участвовать в организации работы малого коллектива исполнителей с учетом требований режима защиты информации и сохранения государственной тайны;

**участие в реализации комплексной информационной безопасности телекоммуникационных систем:**

* осуществлять сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике информационной безопасности телекоммуникационных систем;
* осуществлять проектные расчеты элементов систем обеспечения информационной безопасности;
* участвовать в работах по реализации политики комплексного обеспечения информационной безопасности телекоммуникационных систем;
* участвовать в мониторинге эффективности информационной безопасности телекоммуникационных систем.

Конкретные общекультурные и профессиональные компетенции, качественное изменение которых осуществляется в результате обучения, и их характеристика определяются ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

* + - 1. **Знания, умения и навыки**

По согласованию с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование, перечень знаний, умений и навыков, получаемых в результате обучения по настоящей образовательной программе, может дополняться знаниями, умениями и навыками, получаемыми в результате обучения ФОНДОМ «ТРИОНИКС» в рамках других образовательных программ.

Конкретные знания, умения и навыки определяются ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

В результате обучения по настоящей образовательной программе обучающийся должен:

* + - * 1. **Гуманитарный, социальный, экономический и общенаучный цикл**

**Должен знать:**

* взаимосвязь общения и деятельности;
* виды социальных взаимодействий;
* закономерности исторического процесса, основные этапы, события отечественной истории, место и роль России в истории человечества и в современном мире;
* источники, причины, виды и способы разрешения конфликтов;
* лексический (1200-1400 лексических единиц) и грамматический минимум, необходимый для чтения и перевода (со словарем) иностранных текстов профессиональной направленности;
* лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке;
* механизмы взаимопонимания в общении;
* научные основы, цели, принципы, методы и технологии управленческой деятельности;
* о роли физической культуры в общекультурном, профессиональном и социальном развитии человека;
* основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире;
* основные категории и понятия философии;
* основные понятия и методы в области управленческой деятельности;
* основные разделы и направления философии, методы и приемы философского анализа проблем;
* основные теории и методы макро- и микроэкономики;
* основные экономические категории и закономерности, методы анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микрои макро-) уровнях, основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений;
* основные экономические теории, категории и закономерности, методы анализа экономических явлений и процессов;
* основные этапы развития философской мысли, основную проблематику и структуру философского знания;
* основы здорового образа жизни;
* основы научной, философской и религиозной картин мира;
* основы права и законодательства России, основы конституционного строя Российской Федерации, характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации;
* основы философского учения о бытии;
* основы экономической и финансовой деятельности отрасли и ее структурных подразделений, методику оценки хозяйственной, деятельности (применительно к отрасли обеспечения информационной безопасности);
* основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации;
* характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности Российской Федерации;
* роли и ролевые ожидания в общении;
* роль философии в жизни человека и общества;
* роль философии в формировании ценностных ориентации в профессиональной деятельности;
* содержание и взаимосвязь основных принципов, законов, понятий и категорий гуманитарных, социальных и экономических наук;
* содержание и назначение важнейших правовых и законодательных актов мирового и регионального значения;
* сущность процесса познания;
* техники и приемы общения, правила слушания, ведения беседы, убеждения;
* цели, функции, виды и уровни общения;
* экономическое планирование и прогнозирование, методику оценки хозяйственной деятельности (применительно к отрасли обеспечения информационной безопасности);
* этические принципы общения;

**Должен уметь:**

* анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав;
* анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию;
* планировать и осуществлять свою деятельность с учетом результатов этого анализа;
* анализировать мировоззренческие, социально и личностно значимые философские проблемы;
* анализировать современные общественные процессы, опираясь на принципы историзма и научной объективности;
* анализировать экономические показатели деятельности подразделения;
* анализировать, оценивать и прогнозировать экономические эффекты и последствия реализуемой и планируемой деятельности;
* выявлять взаимосвязь отечественных, региональных, мировых социально-экономических, политических и культурных проблем;
* использовать в практической деятельности правовые знания, анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности;
* использовать приемы саморегуляции поведения в процессе межличностного общения;
* использовать принципы, законы и методы гуманитарных, социальных и экономических наук для решения профессиональных задач;
* использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей;
* общаться (устно и письменно) на иностранном языке на профессиональные и повседневные темы;
* ориентироваться в историческом прошлом и в современной экономической, политической и культурной ситуациях в России;
* ориентироваться в наиболее общих философских проблемах бытия, познания, ценностей, свободы и смысла жизни;
* оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения;
* переводить (со словарем) иностранные тексты профессиональной направленности;
* применять техники и приемы эффективного общения в профессиональной деятельности;
* работать в коллективе, принимать управленческие решения и оценивать их эффективность;
* самостоятельно совершенствовать устную и письменную речь, пополнять словарный запас;
* читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи.

**Должен владеть:**

* иностранным языком в объеме, необходимом для возможности получения информации по профессиональной тематике и навыками устной речи;
* иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке;
* навыками выбора, обоснования, реализации и контроля результатов управленческого решения;
* навыками критического восприятия информации;
* навыками обоснования, выбора, реализации и контроля результатов управленческого решения;
* навыками письменного аргументированного изложения собственной точки зрения;
* навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
* навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений;
* навыками публичной речи, аргументации, ведения дискуссии и полемики;
* основными методами научного познания;
* приемами экономического анализа и планирования, навыками реализации и контроля результатов управленческого решения по экономическим критериям.
  + - * 1. **Математический и естественнонаучный цикл**

**Должен знать:**

* базовые вопросы построения автоматизированных банковских систем;
* базовые вопросы построения открытых информационных систем;
* базовые системные программные продукты и пакеты прикладных программ;
* влияние способов кодирования на сложность структуры цифрового автомата, его быстродействие, устойчивость работы (исключение состязаний) и надежность работы;
* законы электромагнетизма;
* классификацию современных компьютерных систем;
* логические операции, законы и функции алгебры, логики;
* математические методы обработки экспериментальных данных;
* математические основы моделирования распределенных систем (графовая модель, сети Петри, логические модели, потоковые модели), модели программ;
* методы анализа и тестирования протоколов;
* методы восстановления алгоритма программы по ее дизассемблированному коду, а также методы построения графа передачи управления программы по исполняемому коду;
* методы и алгоритмы дизассемблирования программ;
* методы перечисления для основных дискретных структур;
* методы расчета и измерения параметров основных линий передачи сверхвысокочастотного диапазона;
* методы синтеза цифрового автомата с программируемой логикой;
* методы статистической радиотехники;
* общие принципы построения алгоритмов, основные алгоритмические конструкции;
* общий состав и структуру персональных компьютеров и вычислительных систем;
* общий состав и структуру персональных электронно-вычислительных машин (ЭВМ) и вычислительных систем;
* общую постановку задач математического программирования, динамического программирования, сетевого планирования, теории игр;
* основные дискретные структуры: конечные автоматы, грамматики, графы, комбинаторные структуры;
* основные задачи анализа алгоритмов;
* основные законы механики;
* основные законы термодинамики и молекулярной физики;
* основные законы электричества и магнетизма;
* основные криптографические протоколы и стандарты, используемые в автоматизированных банковских системах;
* основные криптографические протоколы и стандарты;
* основные математические методы исследования случайных процессов;
* основные машинные алгоритмы и характеристики их сложности для типовых задач, часто встречающихся и ставших «классическими» в области информатики и программирования;
* основные методы навязывания принятия ложного решения;
* основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи;
* основные методы принятия решений в условиях: неопределенности, неполноты сведений, навязывания ложной информации, дефицита времени и вычислительных ресурсов;
* основные методы разработки алгоритмов и программ, структуры данных, используемые для представления типовых информационных объектов;
* основные методы срыва процесса своевременного принятия решения;
* основные нормативные правовые акты в области метрологии;
* основные положения теории множеств;
* основные положения теории пределов функций, теории рядов;
* основные понятия и задачи векторной алгебры и аналитической геометрии;
* основные понятия и методы аналитической геометрии;
* основные понятия и методы дифференциального и интегрального исчисления;
* основные понятия и методы линейной алгебры и теории алгебраических систем;
* основные понятия и методы математического анализа;
* основные понятия и методы математической логики и теории алгоритмов, теории информации и кодирования;
* основные понятия и методы теории вероятностей и математической статистики;
* основные понятия и методы теории вероятностей, теории случайных процессов и математической статистики;
* основные понятия и методы теории функций комплексного переменного;
* основные понятия информатики;
* основные понятия теории автоматов;
* основные понятия теории игр;
* основные понятия теории информации и кодирования: энтропия, взаимная информация, источники сообщений, каналы связи, коды;
* основные понятия теории конфликтов;
* основные понятия теории надежности;
* основные понятия теории принятия решений;
* основные понятия теории сложности алгоритмов;
* основные понятия, законы и модели механики;
* основные понятия, законы и модели теории колебаний и волн, оптики, квантовой физики, физики твердого тела, статистической физики и термодинамики;
* основные понятия, законы и модели электричества и магнетизма;
* основные принципы математической логики;
* основные результаты о кодировании при наличии и отсутствии шума;
* основные свойства алгебраических структур;
* основные стандарты построения и взаимодействия открытых систем;
* основные стандарты, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;
* основные статистические пакеты прикладных программ;
* основные тенденции развития теории и техники антенн и сверхвысокочастотных устройств;
* основные тенденции развития теории и техники антенн и сверхвысокочастотных устройств;
* основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных;
* основные теоретико-числовые методы применительно к задачам защиты информации;
* основные типы статистических задач и математические методы их решения;
* основные функции, назначение и принципы работы распространенных операционных систем и сред;
* основы квантовой физики и физики твёрдого тела;
* основы комбинаторного анализа;
* основы линейной алгебры и аналитической геометрии;
* основы линейной алгебры над произвольными полями;
* основы обеспечения катастрофоустойчивости автоматизированных банковских систем;
* основы расчета единичных и комплексных показателей надежности автоматизированных систем и их компонентов;
* основы системного подхода к управлению;
* основы теории колебаний и волн, оптики;
* основы теории надежности;
* основы теории погрешностей измерений, методы обработки результатов измерений;
* основы теории формальной спецификации и верификации программного обеспечения;
* основы теории электрорадиоизмерений;
* основы физики колебаний и волн;
* особенности физических эффектов и явлений, используемых для обеспечения информационной безопасности;
* подходы к испытанию средств криптографической защиты и требования к встраиванию криптосистем в информационные системы;
* практические основы построения систем статического и динамического анализа программ;
* принципы построения и структуру автоматизированных средств измерений и контроля;
* принципы, методы измерений радиотехнических величин и структурные схемы радиоизмерительных приборов;
* свойства электронов в кристаллических проводниках и полупроводниках, принципы работы полупроводниковых и лазерных устройств;
* связь информативных признаков с параметрами побочных сигналов;
* современные средства отладки и эмуляции программного кода;
* состав, назначение функциональных компонентов и программного обеспечения персонального компьютера;
* состав, назначение функциональных компонентов и программного обеспечения персонального компьютера;
* спектрально-энергетические характеристики информативных сигналов в физических полях любой природы;
* способы защиты систем от исследования и отладки;
* способы нормирования и формы задания метрологических характеристик средств измерений;
* способы повышения надежности систем;
* способы расчета оценочных показателей надежности аппаратных и программных средств автоматизированных систем обработки информации и управления;
* стандартные типы данных;
* структуру представления конечных групп;
* типовые структуры и принципы организации компьютерных сетей;
* универсальные приемы исследования оптимизационных проблем при различной степени неопределенности условий;
* физические основы механики;
* физические основы образования технических каналов утечки информации;
* физические основы функционирования технических средств и систем обработки и передачи информации;
* физические явления возникновения побочных сигналов в различных физических полях;
* физические явления и эффекты, используемые при обеспечении информационной безопасности автоматизированных систем;
* формализации понятия алгоритма: машины Тьюринга, рекурсивные функции;
* формальные методы и подходы к верификации программного обеспечения;
* формы и способы представления данных в персональном компьютере;
* цели и методы сертификации;
* языки описания цифрового автомата с памятью и методы синтеза схем цифрового автомата произвольного назначения на элементах различного базиса и степени интеграции.

**Должен уметь:**

* анализировать и применять физические явления и эффекты для решения практических задач обеспечения информационной безопасности;
* анализировать приводимые представления конечных групп;
* выбирать и описывать тип системы управления при решении специализированных прикладных профессиональных задач;
* выбирать и оценивать различные структуры систем с точки зрения надежности;
* выбирать методы и модели принятия решений в защищенных автоматизированных системах управления;
* выполнять операции над матрицами и решать системы линейных уравнений;
* выполнять операции над множествами;
* вычислять теоретико-информационные характеристики источников сообщений и каналов связи;
* выявить атаку в информационных журналах системы, описать природу атаки, ее признаки и методы обнаружения, оценивать систему с точки зрения проведения возможных атак на систему;
* выявлять уязвимости различных методов и алгоритмов принятия решений для заданных условий эксплуатации защищенных автоматизированных систем управления
* дезассемблировать и отлаживать программу;
* дифференцировать функции комплексного переменного, строить конформные отображения простейших областей, вычислять комплексные интегралы, раскладывать функции в ряд Тейлора и ряд Лорана, а также вычислять вычеты функций;
* доказывать корректность составленного алгоритма и оценивать основные характеристики его сложности;
* использовать математические методы и модели для решения прикладных задач;
* использовать основные положения теории вероятностей и математической статистики в профессиональной деятельности;
* использовать основные положения теории вероятностей и математической статистики;
* использовать программные и аппаратные средства персонального компьютера;
* использовать современные программные средства для проектирования технологической документации;
* использовать средства операционных систем и сред для обеспечения работы вычислительной техники;
* использовать физические эффекты для обеспечения технической защиты информации;
* использовать языки программирования, разрабатывать логически правильные и эффективные программы;
* исследовать эффективность алгоритма и программы;
* обосновать выбор подходящего математического метода и привести алгоритм решения задачи;
* оперировать с числовыми многочленами, матрицами;
* определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач;
* определять необходимые устройства для измерения параметров информативных сигналов от технических средств обработки информации;
* определять оптимальные алгоритмы работы, оптимальную структуру и характеристики различных радиотехнических устройств;
* определять структуру оптимальных устройств обработки сигналов информационных радиотехнических систем и оценивать эффективность их работы;
* осваивать и использовать базовые системные программные продукты и пакеты прикладных программ;
* оценивать сложность алгоритмов и вычислений;
* получать стандартные формы представления цифрового автомата с памятью по их описанию на начальных языках;
* пользоваться пакетами прикладных программ для решения вероятностных и статистических задач;
* пользоваться расчетными формулами, таблицами, компьютерными программами при решении математических задач;
* пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет;
* применять измерительное оборудование для измерения параметров информативных сигналов в физических полях;
* применять методы дифференциального и интегрального исчисления;
* применять на практике методы физики при исследовании технических каналов утечки информации;
* применять на практике стандарты, относящиеся к обеспечению информационной безопасности банковской организации;
* применять на практике стандарты, относящиеся к открытым информационным системам;
* применять основные законы физики при решении прикладных задач;
* применять системы компьютерной математики для решения типовых задач;
* применять стандартные методы дискретной математики и теории автоматов для решения профессиональных задач;
* применять стандартные методы и модели к решению типовых вероятностных и статистических задач;
* применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач;
* применять стандартные методы и модели к решению типовых теоретико-вероятностных и статистических задач;
* применять теоретико-числовые методы для оценки криптографических свойств систем защиты информации;
* применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, очистки и дефрагментации диска);
* разрабатывать алгоритмы принятия решений для заданных условий эксплуатации защищенных автоматизированных систем управления;
* разрабатывать алгоритмы, используя общие схемы, методы и приемы построения алгоритмов, выбирая подходящие структуры данных для представления информационных объектов;
* разрабатывать модели нарушителя и угроз для информационных систем, выделять подсистемы и модули, содержащие критическую информацию;
* рассчитывать электрические токи и напряжения;
* реализовывать алгоритмы и используемые структуры данных средствами языков программирования высокого уровня;
* решать основные задачи векторной алгебры и аналитической геометрии;
* решать основные задачи линейной алгебры, системы линейных уравнений над полями;
* решать основные задачи на вычисление пределов функций, дифференцирование и интегрирование, на разложение функций в ряды;
* решать типовые задачи кодирования и декодирования;
* решать типовые прикладные физические задачи;
* самостоятельно строить вероятностные модели применительно к практическим задачам и производить статистическую оценку адекватности полученной модели и реальных задач;
* синтезировать логические схемы блоков операционного и управляющего автоматов с использованием методов синтеза цифрового автомата;
* создавать формальное описание протоколов с целью их дальнейшего анализа;
* строить и изучать математические модели конкретных явлений и процессов для решения расчетных и исследовательских задач;
* строить логические схемы и составлять алгоритмы;
* строить математические модели физических явлений и процессов;
* формализовать задачи анализа безопасности информационных систем, определять объем необходимых тестов и контрольных экспериментов, разрабатывать методики испытаний, применять существующие инструментальные средства статического и динамического анализа программного обеспечения, средства мониторинга и аудита безопасности;
* формировать множество альтернативных решений, ставить цель и выбрать оценочный критерий оптимальности, сформулировать ограничения на управляемые переменные, связанные со спецификой моделируемой системы.

**Должен владеть:**

* инструментальными и аппаратными средствами для проверки функционала испытуемых систем;
* методами и инструментальными средствами анализа безопасности программного обеспечения;
* методами и инструментарием эмуляции и виртуализации для проведения испытаний сложных систем;
* методами и средствами поиска уязвимостей, анализа и верификации протоколов;
* методами количественного анализа процессов обработки, поиска и передачи информации;
* методами комплексного анализа для вычисления определенных и несобственных интегралов и решения других задач алгебры и анализа;
* методами линейной алгебры;
* методами обработки результатов электрорадиоизмерений;
* методами проведения физического эксперимента при выявлении технических каналов утечки информации;
* методами проектирования систем по заданным требованиям надежности;
* методами проектирования систем, удовлетворяющих заданным требованиям надежности;
* методами теоретического исследования физических явлений и процессов;
* методикой анализа структуры автоматизированной банковской системы;
* методикой анализа структуры открытых информационных систем;
* навыками анализа и синтеза систем управления;
* навыками аналитического и численного решения задач математической статистики;
* навыками выбора и оптимизации вида базисных функций, соответствующих обрабатываемым сигналам и элементной базе;
* навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике;
* навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач;
* навыками использования стандартных теоретико-вероятностных и статистических методов при решении прикладных задач;
* навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией);
* навыками оценки вычислительной сложности реализации выбранных или разработанных алгоритмов принятия решений;
* навыками оценки технических характеристик информативных сигналов в различных физических полях;
* навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.);
* навыками пользования библиотеками прикладных программ для решения прикладных математических задач;
* навыками построения дискретных моделей при решении профессиональных задач;
* навыками построения и анализа моделей типичных операционных задач;
* навыками применения математического аппарата для решения прикладных теоретико-информационных задач;
* навыками проведения физического эксперимента и обработки его результатов;
* навыками работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов);
* навыками разработки алгоритмов защиты от принятия несвоевременных и ложных решений;
* навыками разработки алгоритмов и программ, структур данных, используемых для представления типовых информационных объектов;
* навыками реализации алгоритмов и используемых структур данных, средствами языков программирования высокого уровня;
* общими подходами к испытанию систем криптографической защиты (аутентификация, защита данных);
* основами построения математических моделей систем передачи информации;
* системным подходом при построении алгоритмов;
* современными методами обработки результатов экспериментов для оценки полноты и достоверности испытаний;
* современными средствами отладки и тестирования программы;
* современными средствами поиска уязвимостей;
* способами оценки сложности работы алгоритмов;
* типовыми средствами анализа сетевых протоколов.
  + - * 1. **Профессиональный цикл**

**Должен знать:**

* автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
* адресацию в сетях, организацию межсетевого воздействия;
* аппаратные средства вычислительной техники;
* архитектуру и общие принципы функционирования современных компьютеров;
* архитектуру и принципы работы современных сетей передачи данных;
* архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем;
* базовые понятия и классификацию систем управления базами данных;
* виды виртуальных сетей и их преимущества при конкретном применении;
* виды помех, методы их подавления;
* возможности технических средств перехвата информации;
* возможности, классификацию и область применения макрообработки;
* временные и спектральные характеристики модулированных сигналов и периодической последовательности импульсов;
* жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
* задачи и основные мероприятия гражданской обороны;
* законодательные и нормативные акты, регламентирующие трудовые правоотношения;
* интегрированные среды изучаемых языков программирования;
* информационного обслуживания, предоставляемые пользователям;
* источники и классификацию угроз информационной безопасности;
* источники угроз информационной безопасности и меры по их предотвращению;
* классификацию и структуру комплексных систем защиты информации в телекоммуникационных системах;
* классификацию, принципы построения, физические основы работы периферийных устройств;
* консольные и графические интерфейсы современных операционных систем;
* конструкцию и характеристики электрических и оптических кабелей связи;
* критерии оценки эффективности и надежности средств защиты операционных систем;
* логическую и физическую структуру баз данных;
* материально-технические, трудовые и финансовые ресурсы отрасли и организации, показатели их эффективного использования;
* меры пожарной безопасности и правила безопасного поведения при пожарах;
* место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;
* место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
* место информационной безопасности в системе национальной безопасности страны;
* методику разработки бизнес-плана;
* методологии и методы проектирования программного обеспечения;
* методы анализа и синтеза электронных схем;
* методы анализа электрических цепей;
* методы аттестации уровня защищенности автоматизированных систем;
* методы и приемы манипулирования данными;
* методы и процедуры выявления угроз и нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* методы и процедуры выявления угроз информационной безопасности на критически важных объектах;
* методы и средства анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* методы и средства для обеспечения информационной безопасности автоматизированных систем в защищенном исполнении на различных стадиях и этапах их жизненного цикла;
* методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
* методы концептуального проектирования технологий обеспечения информационной безопасности;
* методы организации и технологию ремонта оборудования защищенных телекоммуникационных систем;
* методы программирования и методы разработки эффективных алгоритмов решения прикладных задач;
* методы расчета эффективности защиты телекоммуникационных систем;
* методы тестирования и отладки программного обеспечения;
* методы электронного документооборота в автоматизированных банковских системах;
* методы, способы и средства обеспечения отказоустойчивости автоматизированных систем;
* методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
* механизмы и интерфейсы ввода-вывода информации и взаимодействия с периферийными устройствами, реализуемые современными операционными системами;
* механизмы и интерфейсы взаимодействия в современных операционных системах в рамках локальных и глобальных вычислительных сетей;
* механизмы и интерфейсы управления оперативной и виртуальной памятью в современных операционных системах;
* механизмы ценообразования на продукцию (услуги), формы оплаты труда в современных условиях;
* многозадачность в современных операционных системах, механизмы и интерфейсы управления параллельно выполняющимися задачами;
* модели баз данных;
* модели угроз информационной безопасности телекоммуникационных систем;
* модели шифров и математические методы их исследования;
* модемы, использующиеся в защищенных телекоммуникационных системах, принципы функционирования и подключения;
* назначение и принципы работы основных узлов современных технических средств информатизации;
* назначение, принципы работы и правила эксплуатации технических средств и систем, аппаратуры контроля, защиты и другого оборудования, используемого при проведении работ по защите информации;
* научные и организационные основы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий;
* номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;
* номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
* нормативную правовую базу, руководящие и методические документы, регламентирующие реализацию процессов создания автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла;
* нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты;
* о комплексном подходе к построению эшелонированной защиты для автоматизированных банковских систем;
* о комплексном подходе к построению эшелонированной защиты для открытых информационных систем;
* о политиках безопасности и мерах защиты в открытых информационных системах;
* область применения получаемых профессиональных знаний при исполнении обязанностей военной службы;
* общие положения экономической теории;
* общие принципы построения и использования современных языков программирования высокого уровня;
* опасные и вредные факторы системы «человек среда обитания», методы анализа антропогенных опасностей, научные и организационные основы защиты окружающей среды и ликвидации последствий, аварий, катастроф, стихийных бедствий;
* операционные системы персональных ЭВМ;
* определения и свойства основных алгебраических структур, используемых в криптографии;
* организационное обеспечение документирования управления персоналом и трудовой деятельности работников;
* организацию защиты информации от утечки по техническим каналам на объектах информатизации;
* организацию и порядок призыва граждан на военную службу и поступления на нее в добровольном порядке;
* организацию производственного и технологического процессов;
* организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
* организацию ремонтного обслуживания аппаратуры и средств защиты информации;
* основные виды вооружения, военной техники и специального снаряжения, состоящих на вооружении (оснащении) воинских подразделений, в которых имеются военно-учетные специальности, родственные настоящей специальности;
* основные виды потенциальных опасностей и их последствия в профессиональной деятельности и быту, принципы снижения вероятности их реализации;
* основные задачи и понятия криптографии;
* основные информационные технологии, используемые в автоматизированных системах;
* основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности;
* основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;
* основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах;
* основные критерии, методы и меры обеспечения доверия к информационной безопасности;
* основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);
* основные методы защиты информации в автоматизированных банковских системах;
* основные методы и средства реализации удаленных сетевых атак на открытые информационные системы;
* основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам;
* основные методы измерений параметров электрических цепей и сигналов;
* основные методы обеспечения безопасности пластиковых карт;
* основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;
* основные методы помехоустойчивого кодирования каналов связи;
* основные методы управления информационной безопасностью;
* основные модели данных, физическую организацию баз данных;
* основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;
* основные определения, законы, и методы расчёта электрических цепей;
* основные периферийные устройства и их работу;
* основные положения конструкторской, технологической и другой нормативной документации;
* основные положения системного подхода к технической защите информации;
* основные положения стандартов Единой системы конструкторской документации, Единой системы программной документации;
* основные положения теории управления;
* основные понятия и законы электродинамики и виброакустики;
* основные понятия и определения в области систем передачи информации;
* основные понятия и определения метрологии, стандартизации и сертификации;
* основные понятия компьютерных сетей и их аппаратные компоненты;
* основные понятия криптографии и типовые криптографические методы защиты информации;
* основные понятия теории баз данных, модели данных;
* основные понятия теории информации;
* основные приемы программирования;
* основные принципы и этапы проектирования баз данных;
* основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем;
* основные принципы синхронизации цифровых потоков;
* основные протоколы идентификации и аутентификации в телекоммуникационных системах;
* основные протоколы компьютерных сетей;
* основные свойства схем шифрования, электронной цифровой подписи и аутентификации при решении задач защиты технологического электронного документооборота и документоведения;
* основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;
* основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
* основные стандарты построения виртуальных сетей;
* основные структуры данных и способы их реализации на языке программирования;
* основные телекоммуникационные протоколы;
* основные термины и определения теории булевых функций;
* основные термины и определения теории множеств;
* основные технические каналы утечки защищаемой информации в автоматизированных и телекоммуникационных системах, физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности;
* основные технические методы и средства защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам, средств охраны и безопасности объектов;
* основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
* основные характеристики сигналов электросвязи, спектры и виды модуляции;
* основные характеристики физических полей различной природы;
* основы администрирования вычислительных сетей;
* основы военной службы и обороны государства;
* основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;
* основы маршрутизации в сетях передачи данных;
* основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
* основы построения систем менеджмента информационной безопасности на базе современных международных и национальных стандартов;
* основы схемотехники;
* основы теории электрических цепей;
* основы физической защиты объектов информатизации;
* особенности менеджмента в области обеспечения информационной безопасности
* особенности построения и составные элементы сетей передачи данных;
* особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
* особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;
* особенности распространения электромагнитных и акустических волн;
* периодичность поверок контрольно-измерительной аппаратуры;
* перспективы развития современных баз данных;
* подходы к интеграции виртуальных сетей с открытыми информационными системами;
* подходы к интеграции сетей в открытых информационных системах;
* показатели качества программного обеспечения;
* политику безопасности для виртуальных сетей;
* полный цикл мероприятий по комплексному обеспечению информационной безопасности автоматизированных систем;
* понятие и принципы управления персоналом в организациях различных форм собственности, основы организации работы малых коллективов;
* понятие и принципы управления персоналом на предприятиях различных форм собственности, основы организации работы малых коллективов;
* порядок и правила оказания первой помощи пострадавшим;
* порядок применения системного анализа при построении комплексных систем защиты информации;
* порядок проведения работ по технической защите информации объекта;
* последовательность и содержание этапов построения компьютерных сетей;
* последовательность и содержание этапов проектирования баз данных;
* построение запросов в системах управления базами данных;
* правила и нормы охраны труда, техники безопасности, промышленной санитарии и противопожарной защиты;
* правила применения, эксплуатации и обслуживания технических средств защиты информации;
* правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность);
* правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
* правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
* правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;
* принцип действия выпрямителей переменного тока;
* принцип модуляции;
* принципы аналого-цифрового преобразования, работы компандера, кодера и декодера;
* принципы защиты программного обеспечения защищенных автоматизированных систем управления от несанкционированного копирования с привязкой к магнитным носителям, регистрационным кодам и специальным аппаратным устройствам защиты (электронным ключам);
* принципы защиты электронных устройств от недопустимых режимов работы;
* принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организациях;
* принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности на предприятиях;
* принципы и методы организационной защиты информации;
* принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
* принципы кодирования и представления информации;
* принципы модуляции;
* принципы обеспечения устойчивости объектов экономики, прогнозирования развития событий и оценки последствий при техногенных чрезвычайных ситуациях и стихийных явлениях, в том числе в условиях противодействия терроризму как серьезной угрозе национальной безопасности России;
* принципы организации документирования разработки, процесса сопровождения программного обеспечения;
* принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;
* принципы организации информационных систем в соответствии с требованиями по защите информации;
* принципы организации технической эксплуатации защищенных телекоммуникационных систем;
* принципы передачи информации в системах электросвязи;
* принципы помехоустойчивого кодирования;
* принципы построения и технические средства локальных сетей;
* принципы построения и функционирования систем и сетей передачи информации;
* принципы построения и функционирования, архитектуру, примеры реализаций современных систем управления базами данных;
* принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;
* принципы построения и функционирования, примеры реализаций современных операционных систем;
* принципы построения информационных систем;
* принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;
* принципы построения многоканальных систем передачи;
* принципы построения распределенных систем и объектно-ориентированных систем управления базами данных, технологии автоматизированного проектирования баз данных и хранилищ данных, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;
* принципы построения сетей радиосвязи и их классификацию;
* принципы построения сетей радиосвязи с подвижными элементами и их классификация;
* принципы построения современных виртуальных локальных и частных сетей и направления их развития;
* принципы построения современных систем обеспечения информационной безопасности;
* принципы построения, основные характеристики типовых измерительных приборов и правила работы с ними;
* принципы построения, состав, структуру и функции современных операционных систем;
* принципы применения и построения систем управления ресурсами предприятия и технологий поддержки жизненного цикла, методы и средства обеспечения их информационной безопасности;
* принципы работы сетевых протоколов и технологий передачи данных в виртуальных сетях;
* принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах;
* принципы работы стабилизаторов напряжения и тока, импульсных источников питания;
* принципы работы типовых электронных устройств;
* принципы работы элементов и функциональных узлов электронной аппаратуры;
* принципы работы элементов современной радиоэлектронной аппаратуры и физические процессы, протекающие в них;
* принципы разработки алгоритмов программ;
* принципы расчета основных характеристик систем экранирования электромагнитных полей, акустической и виброакустической защиты;
* принципы статистического анализа;
* принципы факсимильной передачи сообщений;
* принципы формирования политики информационной безопасности в автоматизированных системах;
* принципы функционирования маршрутизаторов;
* программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях;
* разновидности проводных линий передачи;
* реляционную алгебру;
* свойства электромагнитных волн;
* сетевые модели, протоколы и их установку в операционных системах;
* сигналы электросвязи, принципы построения систем и средств связи;
* системы управления базами данных;
* современные системы проектирования программного и аппаратного обеспечения защищенных автоматизированных систем управления;
* современные средства и методы построения комплексных систем обеспечения информационной безопасности в автоматизированных системах;
* современные средства и способы обеспечения информационной безопасности
* современные средства разработки и анализа программного обеспечения на языках высокого уровня;
* современные технологии и методы программирования;
* современные технологии проектирования автоматизированных систем в защищенном исполнении;
* содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
* состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;
* состав и принципы работы автоматизированных систем, операционных систем и сред;
* спецификацию изделий, комплектующих, запасного имущества и ремонтных материалов, порядок их учета и хранения;
* специфику математического моделирования организационных задач в автоматизированных системах;
* способы защиты населения от оружия массового поражения;
* способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
* способы и средства охраны объектов;
* способы кодирования информации;
* способы коммутации в сетях связи;
* способы обеспечения информационной безопасности систем организационного управления;
* способы обработки исключительных ситуаций;
* способы описания поведения систем;
* способы описания сигналов и устройств цифровой обработки;
* средства защиты информации, используемые на критически важных объектах;
* средства защиты программного обеспечения защищенных автоматизированных систем управления;
* средства обеспечения безопасности данных;
* средства проектирования структур баз данных;
* структурные схемы и порядок взаимодействия компонентов современных технических средств информатизации;
* структуру систем документационного обеспечения;
* сущность и понятие информации, информационной безопасности и характеристику ее составляющих;
* сущность и понятие информационной безопасности, характеристику ее составляющих;
* сущность процесса модуляции;
* тактико-технические характеристики и возможности систем и средств технической разведки;
* терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем;
* технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
* технические каналы утечки информации;
* технические характеристики, показатели качества ЭВМ и систем, методы их оценки и пути совершенствования;
* типовые алгоритмы цифровой обработки и синтеза сигналов;
* типовые архитектуры и принципы построения современных защищенных информационных систем;
* типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;
* типовые модели управления доступом;
* типовые поточные и блочные шифры;
* типовые решения обеспечения информационной безопасности телекоммуникационных систем;
* типовые средства и методы ведения аудита и обнаружения вторжений;
* типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
* типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
* типовые схемотехнические решения основных узлов и блоков электронной аппаратуры;
* типовые услуги цифровых систем связи;
* типовые шифры с открытыми ключами;
* типы данных, базовые конструкции изучаемых языков программирования;
* требования к системам комплексной защиты информации;
* требования к шифрам и основные характеристики шифров;
* требования стандартов Единой системы конструкторской документации (ЕСКД) и Единой системы технологической документации (ЕСТД) к оформлению и составлению чертежей и схем;
* угрозы и атаки, характерные для распределенных информационных систем;
* уровня (объектно-ориентированное программирование);
* физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
* формы и методы инструктирования и обучения сотрудников;
* функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;
* функции, виды и психологию менеджмента;
* характеристики основных технических каналов утечки информации на критически важных объектах;
* частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;
* энтропия, взаимная информация, источники сообщений, модели каналов передачи информации, коды;
* эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы;
* эталонную модель взаимодействия открытых систем;
* язык программирования высокого.

**Должен уметь:**

* администрировать операционные системы, выполнять работы по устранению отказов и восстановлению работоспособности;
* администрировать операционные системы;
* администрировать подсистемы информационной безопасности автоматизированных систем;
* анализировать и оценивать степень риска проявления факторов опасности системы «человек среда обитания», осуществлять и контролировать выполнение требований по охране труда и технике безопасности в конкретной сфере деятельности;
* анализировать и оценивать угрозы информационной безопасности объекта;
* анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем;
* анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи;
* анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте, применять автоматизированные средства мониторинга, аудита и анализа защищенности данных систем;
* владеть способами бесконфликтного общения и саморегуляции в повседневной деятельности и экстремальных условиях военной службы;
* восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях;
* выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;
* выбирать, разрабатывать и внедрять практические меры по управлению информационной безопасностью на основе современных международных и национальных стандартов;
* выделять сущности и связи предметной области;
* выполнять запросы к базе данных;
* выполнять работы по устранению отказов и восстановлению работоспособности;
* выполнять регламенты техники безопасности;
* выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;
* выявлять и устранять уязвимости в основных компонентах открытых информационных систем;
* выявлять каналы утечки информации на объекте защиты;
* выявлять уязвимости защиты программного обеспечения защищенных автоматизированных систем управления и находить пути их устранения;
* выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем;
* диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
* защищать свои права в соответствии с трудовым законодательством;
* измерять основные параметры электрических цепей и электрорадиоэлементов;
* использовать встроенные механизмы защиты информации в системах управления базами данных;
* использовать динамически подключаемые библиотеки;
* использовать и оформлять техническую документацию в соответствии с действующими нормативными документами;
* использовать системы автоматизированного проектирования для подготовки технической документации;
* использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам;
* использовать средства индивидуальной и коллективной защиты от оружия массового поражения;
* использовать средства контроля работоспособности вычислительной техники;
* использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;
* использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
* использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов;
* использовать стандартные методы и средства проектирования цифровых узлов и устройств, в том числе для средств защиты информации;
* использовать технологии автоматизированного проектирования и структурный подход при проектировании информационных систем, определять ресурсы, необходимые для обеспечения безопасности информационной системы, использовать методы и средства определения технологической безопасности функционирования распределенной информационной системы;
* использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
* использовать шаблоны классов и средства макрообработки;
* использовать языки программирования высокого уровня;
* используя современные методы и средства, разрабатывать и оценивать модели и политики безопасности автоматизированных и информационно-управляющих систем на транспорте;
* используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для виртуальных сетей;
* используя современные методы и средства, разрабатывать и оценивать модели и политику безопасности для открытых информационных систем;
* исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений;
* классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
* классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
* классифицировать основные угрозы безопасности информации;
* контролировать соблюдение персоналом требований режима защиты информации;
* контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
* настраивать маршрутизацию в сетях передачи данных;
* настраивать, эксплуатировать и обслуживать локальные вычислительные сети;
* нормализовывать отношения при проектировании реляционной базы данных;
* обеспечивать безопасность систем управления ресурсами предприятия и технологий поддержки жизненного цикла;
* обеспечивать защиту электронного технологического документооборота на основе электронной цифровой подписи;
* обеспечивать работоспособность, обнаруживать и устранять неисправности подсистем безопасности автоматизированных систем согласно технической документации;
* обнаруживать и обезвреживать разрушающие программные воздействия с использованием программных средств;
* обнаруживать, прерывать и предотвращать удаленные сетевые атаки по их характерным признакам;
* обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности;
* оказывать первую помощь пострадавшим;
* описывать физические поля различной природы;
* определять и устранять основные угрозы информационной безопасности для открытых информационных систем;
* определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
* определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
* определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
* определять состав комплекса средств зашиты информации телекоммуникационных систем;
* организовывать безопасный доступ к информационным ресурсам информационно-телекоммуникационной системы;
* организовывать деловое общение с различными категориями работников;
* организовывать и конфигурировать компьютерные сети;
* организовывать и проводить мероприятия по защите работающих и населения от негативных воздействий чрезвычайных ситуаций;
* организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности;
* ориентироваться в перечне военно-учетных специальностей и самостоятельно определять среди них родственные полученной специальности;
* осуществлять администрирование открытых информационных систем;
* осуществлять выбор функциональной структуры системы обеспечения информационной безопасности;
* осуществлять диагностику компьютерных сетей;
* осуществлять комплектование, конфигурирование, настройку подсистем безопасности автоматизированных систем;
* осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
* осуществлять мониторинг и аудит сетевой безопасности;
* осуществлять настройку модемов, использующихся в защищенных телекоммуникационных системах;
* осуществлять настройку, регулировку и ремонт оборудования средств защиты;
* осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации;
* осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением современных информационных технологий;
* осуществлять техническую эксплуатацию линейных сооружений связи;
* осуществлять управление информационной безопасностью в открытых информационных системах;
* осуществлять установку, настройку и обслуживание технических средств защиты информации и средств охраны объектов;
* отображать предметную область на конкретную модель данных;
* оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
* оформлять техническую документацию в соответствии с действующей нормативной базой;
* оформлять эксплуатационную и ремонтную документацию;
* оценивать информационные риски в автоматизированных системах;
* оценивать точность проводимых измерений;
* оценивать эффективность и надежность защиты операционных систем;
* оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
* оценивать эффективность управленческих решений;
* планировать политику безопасности операционных систем;
* планировать разработку сложного программного обеспечения;
* пользоваться нормативными документами по защите информации;
* пользоваться нормативными документами по противодействию технической разведке;
* пользоваться основными видами современной вычислительной техники, периферийных и мобильных устройств и других технических средств информатизации;
* пользоваться стандартными средствами электрорадиоизмерений;
* пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
* пользоваться технической и справочной литературой;
* правильно эксплуатировать и устранять типичные выявленные дефекты технических средств информатизации;
* практически реализовывать различные варианты построения виртуальных сетей в соответствии со стандартами по оценке защищенных систем и давать оценку качества предлагаемых решений;
* практически решать задачи защиты программ и данных программно-аппаратными средствами и давать оценку качества предлагаемых решений;
* предпринимать профилактические меры для снижения уровня опасностей различного вида и их последствий в профессиональной деятельности и быту;
* применять знания о системах электрической связи для решения задач по созданию защищенных телекоммуникационных систем;
* применять инструментальные средства для исследования программного обеспечения защищенных автоматизированных систем управления в машинных кодах;
* применять математические методы исследования моделей шифров;
* применять методики оценки эффективности защиты телекоммуникационных систем;
* применять методы манипулирования данными;
* применять на практике методы анализа электрических цепей;
* применять нормативные документы по метрологии, стандартизации и сертификации на практике;
* применять нормативные правовые акты и нормативные методические документы в области защиты информации;
* применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
* применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами;
* применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами;
* применять основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий;
* применять основные положения системного и объектно-ориентированного проектирования и моделирования защищенных автоматизированных систем управления;
* применять основные правила и документы системы сертификации Российской Федерации;
* применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
* применять первичные средства пожаротушения;
* применять программно-аппаратные средства обеспечения информационной безопасности;
* применять профессиональные знания в ходе исполнения обязанностей военной службы на воинских должностях в соответствии с полученной специальностью;
* применять средства обеспечения безопасности данных;
* применять стандартные методы цифровой обработки сигналов;
* применять стандартные решения для защиты информации в виртуальных сетях и квалифицированно оценивать их качество;
* применять стандартные решения для защиты информации в открытых информационных системах и квалифицированно оценивать их качество;
* применять технические методы и средства защиты информации на выделенных объектах;
* применять технические средства защиты информации;
* применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;
* проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры;
* проводить анализ архитектуры и структуры ЭВМ и систем, оценивать эффективность архитектурно-технических решений, реализованных при построении ЭВМ и систем;
* проводить анализ достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* проводить анализ типовых устройств цифровой обработки сигналов;
* проводить анализ, выделять сущности и связи предметной области и отображать ее на конкретную модель данных;
* проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;
* проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач;
* проводить инструктаж сотрудников;
* проводить инструментальный мониторинг защищенности автоматизированных банковских систем;
* проводить комплексное тестирование и отладку программных систем;
* проводить мониторинг угроз безопасности компьютерных сетей;
* проводить синтез и анализ проектных решений по обеспечению информационной безопасности автоматизированных банковских систем;
* проводить сравнительный анализ технических и эксплуатационных характеристик средств обеспечения информационной безопасности телекоммуникационных систем;
* проводить типовые измерения;
* проводить типовые операции настройки средств защиты операционных систем;
* проектировать защищенные открытые информационные системы;
* проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;
* проектировать и кодировать алгоритмы с соблюдением требований к качественному стилю программирования;
* проектировать и реализовывать защиту программного обеспечения защищенных автоматизированных систем управления, исходя из поставленных целей защиты;
* проектировать и эксплуатировать системы управления информационной безопасностью автоматизированных банковских систем;
* проектировать структуру и архитектуру программного обеспечения с использованием современных методологий и средств автоматизации проектирования программного обеспечения;
* производить испытания, проверку и приемку оборудования защищенных телекоммуникационных систем;
* производить монтаж кабельных линий и оконечных кабельных устройств;
* производить монтаж компьютерных сетей;
* производить настройку программного обеспечения коммутационного оборудования защищенных телекоммуникационных систем;
* производить установку и настройку типовых программно-аппаратных средств защиты информации;
* производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы;
* работать в интегрированной среде программирования;
* работать с интегрированной средой разработки программного обеспечения;
* работать с протоколами разных уровней;
* работать с системами управления базами данных;
* работать с современной элементной базой электронной аппаратуры;
* разрабатывать и администрировать базы данных и интерфейсы прикладных программ к базам данных;
* разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем;
* разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем;
* разрабатывать методы и средства для проверки выполнения требований информационной безопасности и поиска уязвимостей;
* разрабатывать модели жизненного цикла защищенных автоматизированных систем управления с учетом требований по обеспечению информационной безопасности на основе современных международных и национальных стандартов;
* разрабатывать модели систем организационного управления;
* разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;
* разрабатывать модели угроз и нарушителей информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных банковских систем;
* разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;
* разрабатывать прикладные программы, осуществляющие взаимодействие с базами данных;
* разрабатывать проектные решения по автоматизированным системам в защищенном исполнении, их системам обеспечения информационной безопасности, реализовывать их, управлять процессами разработки и реализации этих проектных решений;
* разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации;
* разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;
* разрабатывать частные политики информационной безопасности автоматизированных систем;
* разрабатывать, реализовывать, оценивать и корректировать основные процессы управления информационной безопасностью;
* рассчитывать основные характеристики систем и средств экранирования электромагнитных полей;
* рассчитывать по принятой методике основные технико-экономические показатели деятельности организации;
* рассчитывать по принятой методике пропускную способность канала связи;
* рассчитывать простые электрические цепи;
* рассчитывать типовые электронные устройства;
* реализовывать и контролировать выполнение требований по охране труда и технике безопасности в профессиональной деятельности;
* реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;
* реализовывать политику безопасности баз данных;
* реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам защиты информации ограниченного доступа;
* реализовывать системы защиты информации в открытых информационных системах в соответствии со стандартами по оценке защищенных систем;
* реализовывать системы защиты информации в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах на транспорте в соответствии со стандартами по оценке защищенных систем;
* решать практические задачи информационной безопасности на основе инфраструктуры открытых ключей;
* решать типовые задачи кодирования и декодирования;
* решать частные технические задачи при аттестации объектов, помещений, технических средств;
* решать частные технические задачи, возникающих# при аттестации объектов, помещений, программ, алгоритмов;
* создавать объекты базы данных;
* сопрягать между собой различные телекоммуникационные устройства;
* составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;
* составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах;
* составлять, тестировать, отлаживать и оформлять программы на языках высокого уровня, включая объектно-ориентированные;
* строить запросы;
* строить модель нарушителя информационной безопасности для открытых информационных систем;
* устанавливать и настраивать параметры современных сетевых протоколов;
* устранять неисправности компьютерных сетей;
* участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
* участвовать в определении, формализации и оценке информационных рисков;
* участвовать в организации собеседований с персоналом;
* участвовать в рассмотрении технических заданий на проектирование, эскизных, технических и рабочих проектов подсистем обеспечения информационной безопасности телекоммуникационных систем;
* участвовать в рассмотрении технических заданий на проектирование, эскизных, технических и рабочих проектов подсистем обеспечения информационной безопасности;
* формализовать задачу контроля параметров безопасности информационными системами;
* формировать и эффективно применять комплекс мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем;
* формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;
* формировать требования по обеспечению информационной безопасности автоматизированных систем в защищенном исполнении;
* формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
* формулировать основные требования к методам и средствам технической защиты информации на критически важных объектах;
* читать чертежи и схемы;
* читать электрические принципиальные схемы;
* читать электрические принципиальные схемы типовых электронных устройств;
* эксплуатировать и обслуживать средства вычислительной техники;
* эксплуатировать комплексные системы обеспечения информационной безопасности в автоматизированных системах;
* эксплуатировать компоненты подсистем безопасности автоматизированных систем;
* эксплуатировать операционные системы;
* эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;
* эффективно использовать различные методы и средства защиты информации для компьютерных сетей;
* эффективно применять информационно-технологические ресурсы автоматизированных банковских систем с учетом требований информационной безопасности.

**Должен владеть:**

* администрирования подсистем безопасности автоматизированных информационных систем;
* выявления технических каналов утечки информации;
* диагностики составных частей защищенных телекоммуникационных систем;
* диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;
* использования основных методов и средств инженерно-технической защиты информации;
* криптографической терминологией;
* методами анализа и формализации информационных процессов объекта и связей между ними;
* методами и средствами выявления угроз безопасности автоматизированным системам;
* методами и средствами технической защиты информации;
* методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем;
* методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
* методами организации и управления деятельностью;
* методами организации и управления деятельностью служб защиты информации на предприятии;
* методами оценки информационных рисков;
* методами расчета и инструментального контроля показателей технической защиты информации;
* методами реализации и верификации моделей контроля и управления доступом;
* методами технической защиты информации;
* методами управления информационной безопасностью автоматизированных систем;
* методами формирования требований по защите информации;
* методами эксплуатации средств защиты информации;
* методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем;
* методиками оценки рисков информационной безопасности;
* методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;
* методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
* мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;
* навыками автоматизации и управления процессом проектирования защищенных автоматизированных систем управления;
* навыками анализа достаточности мер по обеспечению информационной безопасности процессов создания и эксплуатации автоматизированных систем в защищенном исполнении;
* навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем;
* навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности;
* навыками анализа основных узлов и устройств современных автоматизированных систем;
* навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации;
* навыками анализа угроз и навыками построения политик безопасности для открытых информационных систем и виртуальных сетей;
* навыками анализа угроз и навыками построения политик безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта;
* навыками анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте;
* навыками анализа угроз и уязвимостей информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов;
* навыками анализа угроз и формирования политик безопасности для автоматизированных банковских систем;
* навыками анализа угроз информационной безопасности и уязвимостей в автоматизированных банковских системах;
* навыками анализа угроз информационной безопасности и уязвимостей в открытых информационных системах;
* навыками безопасного использования технических средств в профессиональной деятельности;
* навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем;
* навыками выявления и уничтожения компьютерных вирусов;
* навыками использования измерительного оборудования при экспериментальном исследовании электронной аппаратуры;
* навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей;
* навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем;
* навыками использования типовых криптографических алгоритмов;
* навыками использования ЭВМ в анализе простейших шифров;
* навыками математического моделирования в криптографии;
* навыками организации и обеспечения режима секретности;
* навыками оценки быстродействия и оптимизации работы электронных схем на базе современной элементной базы;
* навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;
* навыками применения различных методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия;
* навыками применения средств анализа безопасности информационных систем;
* навыками проведения специальных исследований и инструментального контроля защищенности автоматизированных систем в защищенном исполнении;
* навыками проведения специальных исследований и инструментального контроля защищенности автоматизированных систем критически важных объектов;
* навыками программирования с использованием эффективных реализаций структур данных и алгоритмов;
* навыками проектирования программного обеспечения с использованием средств автоматизации;
* навыками работы с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении);
* навыками работы с нормативными правовыми актами;
* навыками работы с программными средствами схемотехнического моделирования;
* навыками работы с современными инструментальными средствами для исследования программного обеспечения защищенных автоматизированных систем управления;
* навыками работы с современными операционными системами, восстановления операционных систем после сбоев;
* навыками работы с технической документацией на компоненты автоматизированных систем на русском и иностранном языках;
* навыками работы с технической документацией на ЭВМ и вычислительные системы;
* навыками развертывания и обеспечения работы программных комплексов, обеспечивающих работу с цифровыми сертификатами;
* навыками разработки документации по метрологии, стандартизации и сертификации программных и аппаратных средств защиты;
* навыками разработки защиты программного обеспечения для защищенных автоматизированных систем управления;
* навыками разработки политики безопасности систем организационного управления;
* навыками разработки программной документации;
* навыками разработки систем мониторинга информационной безопасности защищенных автоматизированных систем управления;
* навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации;
* навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;
* навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;
* навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;
* навыками семантического моделирования данных, навыками проектирования информационных систем на базе корпоративных систем управления базами данных, методами снижения угроз безопасности информационных систем, вызванных ошибками на этапе проектирования, разработки и внедрения;
* навыками установки и настройки современных операционных систем с учетом требований по обеспечению информационной безопасности;
* навыками формирования и эффективного применения комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для обеспечения информационной безопасности автоматизированных банковских систем и банковских организаций;
* навыками формирования политик безопасности для критически важных объектов и автоматизированных систем критически важных объектов;
* навыками чтения принципиальных схем, построения временных диаграмм и восстановления алгоритма работы узла, устройства и системы по комплекту документации;
* навыками чтения электронных схем;
* навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
* обеспечения учета, обработки, хранения и передачи конфиденциальной информации;
* организационного и правового обеспечения информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации;
* применения инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем;
* применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами;
* применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем;
* применения программно-аппаратных средств обеспечения информационной безопасности;
* профессиональной терминологией в области информационной безопасности;
* профессиональной терминологией;
* работы в подразделениях защиты информации;
* работы с технической документацией;
* решения частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
* решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;
* системным подходом к организации информационных процессов (в том числе систем управления ресурсами предприятия и технологий поддержки жизненного цикла), анализу информационной безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта;
* служб защиты информации на предприятии;
* сравнительного анализа технических и эксплуатационных характеристик средств обеспечения информационной безопасности, используемых в составе комплексных систем
* средствами фиксации параметров безопасности информационных систем;
* терминологией и системным подходом построения защищенных автоматизированных банковских систем;
* терминологией и системным подходом построения защищенных автоматизированных систем критически важных объектов;
* терминологией и системным подходом построения защищенных открытых информационных систем и виртуальных сетей;
* терминологией и технологиями проектирования автоматизированных систем в защищенном исполнении;
* установки компонентов подсистем безопасности автоматизированных информационных систем;
* участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;
* участия в организации мероприятий внутреннего аудита информационной безопасности и мероприятия по подготовке к аудиту внешней стороной;
* эксплуатации компонентов подсистем безопасности автоматизированных систем, их диагностики, устранения отказов и восстановления работоспособности;
* эксплуатации оборудования защищенных телекоммуникационных систем;
* эксплуатации элементов (оборудования) обеспечения информационной безопасности телекоммуникационных систем.

Конкретные знания, умения и навыки определяются ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

* 1. **Документы о квалификации или об обучении**

Лицам, успешно освоившим соответствующую дополнительную профессиональную программу и прошедшим итоговую аттестацию, выдаются документы о квалификации: **удостоверение о повышении квалификации**.

Документ о квалификации подтверждает:

* повышение или присвоение квалификации по результатам дополнительного профессионального образования (подтверждается удостоверением о повышении квалификации);
* присвоение разряда или класса, категории по результатам профессионального обучения (подтверждается **свидетельством о профессии рабочего, должности служащего**, которые могут выдаваться по требованию прошедшего итоговую аттестацию одновременно с документом о квалификации).

Квалификация, указываемая в документе о квалификации, дает его обладателю право заниматься определенной профессиональной деятельностью и (или) выполнять конкретные трудовые функции, для которых в установленном законодательством Российской Федерации порядке определены обязательные требования к наличию квалификации по результатам дополнительного профессионального образования, если иное не установлено законодательством Российской Федерации.

Лицам, не прошедшим итоговой аттестации или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы и (или) отчисленным из ФОНДА «ТРИОНИКС», выдается **справка об обучении или о периоде обучения**.

Лицам, освоившим образовательные программы, по которым не предусмотрено проведение итоговой аттестации, выдаются документы об обучении – **свидетельство об обучении**.

Документ о квалификации выдается на бланке установленного образца.

При освоении дополнительной профессиональной программы параллельно с получением среднего профессионального образования и (или) высшего образования удостоверение о повышении квалификации и (или) диплом о профессиональной переподготовке выдается одновременно с получением соответствующего документа об образовании и о квалификации.

В случае если проведение итоговой аттестации по настоящей образовательной программе не предусмотрено, выдается **сертификат об обучении**, на бланке установленного образца.

Вид документа о квалификации или документа об обучении указывается в договоре об образовании.

* 1. **Срок обучения**

Минимально допустимый срок освоения программ **повышения квалификации** не может быть менее 16 часов. По программам менее 16 часов проводится **обучение**.

Срок обучения по образовательной программе определяется ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

* 1. **Методические материалы**

Обучающиеся, осваивающие настоящую образовательную программу, пользуются учебниками и учебными пособиями, приобретаемыми за свой счет или выдаваемыми в рамках заключенного договора об образовании. Им предоставляется право бесплатного пользования имеющимися в распоряжении ФОНДА «ТРИОНИКС» библиотечно-информационными ресурсами, учебной, производственной, научной базой ФОНДА «ТРИОНИКС» предназначенных для качественного освоения настоящей образовательной программы.

* 1. **Расчеты нормативных затрат оказания услуг по реализации образовательной программы**

Расчет нормативных затрат оказания услуг по реализации образовательной программы осуществляется с учетом Приказа Минфина РФ № 137н, Минэкономразвития РФ № 527 от 29.10.2010 «О методических рекомендациях по расчету нормативных затрат на оказание федеральными государственными учреждениями государственных услуг и нормативных затрат на содержание имущества федеральных государственных учреждений» и является внутренним документом ФОНДА «ТРИОНИКС».

1. **Учебный план**

При реализации дополнительных профессиональных программ ФОНДОМ «ТРИОНИКС» применяется форма организации образовательной деятельности, основанная на модульном принципе представления содержания образовательной программы и построения учебных планов, используются различные образовательные технологии, в том числе дистанционные образовательные технологии и электронное обучение.

Перечень, последовательность и трудоемкость учебных курсов и модулей, формы обучения и сроки освоения дополнительной профессиональной программы определяются ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

Перечень учебных циклов, курсов и модулей для формирования учебного плана по образовательной программе:

**Гуманитарный, социальный, экономический и общенаучный цикл**

* История;
* Философия;
* Экономика;
* Правоведение;
* Основы управленческой деятельности;
* Экономика и управление;
* Основы философии;
* Психология общения;
* Иностранный язык;
* Физическая культура.

**Математический и естественнонаучный цикл**

* Алгебра и геометрия;
* Математический анализ;
* Математическая логика и теория алгоритмов;
* Теория функций комплексного переменного;
* Антенно-фидерные устройства;
* Теория надежности;
* Открытые информационные системы;
* Криптографические протоколы и стандарты;
* Автоматизированные банковские системы;
* Катастрофоустойчивость автоматизированных банковских систем;
* Криптография в банковском деле;
* Основы теории управления;
* Физические основы защиты информации;
* Теория принятия решений в условиях информационных конфликтов;
* Исследование операций и теории игр;
* Теория графов и ее приложения;
* Верификация безопасности информационных систем;
* Анализ безопасности протоколов;
* Математический аппарат и средства анализа безопасности программного обеспечения;
* Метрология и электрорадиоизмерения;
* Основы теории надежности;
* Основы радиотехники;
* Теория автоматов;
* Структуры и алгоритмы обработки данных;
* Математика (математический анализ, алгебра, геометрия);
* Теория вероятностей и математическая статистика;
* Дискретная математика;
* Теория информации;
* Специальные разделы математики;
* Специальные разделы физики;
* Современная философия и методология науки;
* Деловой иностранный язык;
* Математическое моделирование технических объектов и систем управления;
* Теория игр и исследование операций;
* Теоретические основы управления;
* Математика;
* Информатика;
* Физика.

**Профессиональный цикл**

* Языки программирования;
* Технологии и методы программирования;
* Безопасность операционных систем;
* Безопасность сетей ЭВМ;
* Безопасность систем баз данных;
* Криптографические методы защиты информации;
* Организация ЭВМ и вычислительных систем;
* Техническая защита информации;
* Разработка и эксплуатация защищенных автоматизированных систем;
* Обеспечение информационной безопасности на критически важных объектах;
* Инженерно-техническая защита информации и технические средства охраны на критически важных объектах;
* Основы аттестации объектов информатизации критически важных объектов;
* Методы и средства противодействия террористической деятельности в системах управления критически важных объектов;
* Информационная безопасность открытых систем;
* Виртуальные частные сети;
* Аудит информационных технологий и систем обеспечения информационной безопасности;
* Защита информации в банковских системах;
* Защита электронного документооборота;
* Безопасность систем пластиковых карт;
* Нормативная база обеспечения информационной безопасности банковской организации;
* Защита программного обеспечения защищенных автоматизированных систем;
* Технологии проектирования защищенных автоматизированных систем;
* Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления;
* Обеспечение доверия к информационной безопасности защищенных автоматизированных систем управления;
* Информационная безопасность распределенных информационных систем;
* Методы проектирования защищенных распределенных информационных систем;
* Технология построения защищенных распределенных приложений;
* Мониторинг безопасности информационных систем;
* Анализ рисков информационной безопасности;
* Угрозы информационной безопасности автоматизированных систем;
* Создание автоматизированных систем в защищенном исполнении;
* Оценка информационной безопасности автоматизированных систем в защищенном исполнении;
* Информационная безопасность информационно-управляющих и информационно-логистических систем транспорта;
* Защита информации в распределенных информационных системах и центрах обработки данных;
* Информационная безопасность автоматизированных транспортных систем;
* Защита электронного технологического документооборота;
* Защищенные информационные системы;
* Технологии обеспечения информационной безопасности объектов;
* Управление информационной безопасностью;
* Экспертные системы комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем;
* Организационно-правовые механизмы обеспечения информационной безопасности;
* Методы и средства защиты информации в системах электронного документооборота;
* Теоретические основы компьютерной безопасности;
* Информационно-аналитические системы безопасности;
* Теория систем и системный анализ;
* Технические средства информатизации;
* Организационно-правовое обеспечение информационной безопасности;
* Сети и системы передачи информации;
* Операционные системы;
* Базы данных;
* Эксплуатация подсистем безопасности автоматизированных систем;
* Эксплуатация компьютерных сетей;
* Программно-аппаратные средства обеспечения информационной безопасности;
* Криптографические средства и методы защиты информации;
* Применение инженерно-технических средств обеспечения информационной безопасности;
* Эксплуатация комплексных систем обеспечения информационной безопасности в автоматизированных системах;
* Инженерная графика;
* Электротехника;
* Электроника и схемотехника;
* Электрорадиоизмерения и метрология;
* Основы цифровой обработки сигналов;
* Основы информационной безопасности;
* Физические основы защиты информации;
* Математические основы защиты информации;
* Вычислительная техника;
* Основы алгоритмизации и программирования;
* Экономика организации;
* Менеджмент;
* Безопасность жизнедеятельности;
* Приемо-передающие устройства, линейные сооружения связи и источники электропитания;
* Телекоммуникационные системы;
* Криптографическая защита информации;
* Инженерно-техническая защита информации;
* Программно-аппаратные средства защищенных телекоммуникационных систем;
* Организационное и правовое обеспечение информационной безопасности;
* Комплексное обеспечение информационной безопасности телекоммуникационных систем.

По согласованию с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование, Учебный план может дополняться предметами, дисциплинами и модулями, преподаваемыми ФОНДОМ «ТРИОНИКС» в рамках других образовательных программ.

1. **Рабочая программа учебных курсов и модулей**

Рабочая программа учебных курсов и модулей разрабатывается на основе Учебного плана и состоит из:

* определения перечня учебных курсов, модулей, тем и вопросов;
* определения объема дисциплины и видов учебной работы;
* определения учебно-методического обеспечения;
* определения материально-технического и информационного обеспечения;
* определения форм обучения, промежуточной и итоговой аттестации обучающихся и видов занятий и учебных работ;
* распределение по периодам обучения учебных курсов и модулей.
  1. **Перечень учебных курсов, модулей, тем и вопросов**

Перечень учебных курсов, модулей, тем, разделов, параграфов и вопросов определяются ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании и должны содержать:

* реферативное описание (изложение основных вопросов в заданной последовательности);
* наименование видов занятий по каждой теме;
* методические рекомендации по реализации учебной программы;
* список литературы (основной и рекомендуемой), а также других видов учебно-методических материалов и пособий, необходимых для изучения (конспектов лекций, видеолекций, лазерных дисков и др.).
  + 1. **Объем дисциплин и виды учебной работы**

Объем дисциплин и виды учебной работы по образовательной программе определяется ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

Виды занятий и учебных работ по образовательной программе:

* занятие/работа по социально-психологическому тестированию;
* занятие/работа по ознакомлению с новым материалом;
* занятие/работа по закреплению изученного;
* занятие/работа по обобщению и систематизации;
* занятие/работа по формированию умений и навыков;
* занятие/работа по контролю (проверки знаний, умений и навыков);
* комбинированное занятие/работа (включающие в себя элементы предыдущих типов).

Виды занятий и учебных работ по образовательной программе:

* **по охвату:** фронтальный, индивидуальный, групповой;
* **по времени:** нормированный (с указанием времени начала и конца урока), не нормированный;
* **по длительности:** в часах, в днях, до результата;
* **по месту проведения:** дистанционное, классное, полевое;
* **по территории проведения:** на территории заказчика, на территории образовательной организации, на территории третьих лиц;
* **по отрыву от работы:** с отрывом от работы, с частичным отрывом от работы, без отрыва от работы;
* **по учету учебных возможностей обучающихся:** с одинаковыми учебными возможностями, с различными учебными возможностями;
* **по участию преподавателя:** самостоятельная работа, очно, заочно;
* **по использованию обучающимися средств обучения:** с использованием специального оборудования, без использования специального оборудования.
  + 1. **Учебно-методическое обеспечение**

Обучающиеся, осваивающие настоящую образовательную программу, пользуются учебниками и учебными пособиями, приобретаемыми за свой счет самостоятельно или выдаваемыми в рамках заключенного договора об образовании. Перечень необходимых учебников и учебных пособий для самостоятельного приобретения указывается ФОНДОМ «ТРИОНИКС» в договоре об образовании.

Рекомендуемая литература для самостоятельного изучения определяется ФОНДОМ «ТРИОНИКС» самостоятельно и указывается в договоре об образовании.

* + 1. **Материально-техническое и информационное обеспечение**

Материально техническое и информационное обеспечение по образовательной программе определяется ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

* + 1. **Формы обучения, промежуточной и итоговой аттестации обучающихся и виды занятий и учебных работ**

Формы обучения, промежуточной и итоговой аттестации обучающихся и виды занятий и учебных работ определяются для каждого занятия настоящей образовательной программой и договором об образовании, и указываются в Рабочей программе учебных курсов и модулей.

Формы промежуточной аттестации по образовательной программе:

* **по участию преподавателя:** без преподавателя, очно, заочно;
* **по месту:** дистанционное, классное, полевое;
* **по охвату:** фронтальный, индивидуальный, групповой;
* **по времени:** нормированный (с указанием времени начала и конца урока), не нормированный;
* **по сложности в одном варианте:** с дифференциацией сложности, без дифференциации сложности;
* **по наличию вариантов ответов:** с заранее заданными вариантами ответов, без заранее заданных вариантов ответов;
* **по способу фиксации ответов:** письменное, устное, электронное, практическое, комбинированное;
* **по наличию формы ответа:** ответ по установленной форме, ответ без требований к форме;
* **по вариантам:** одновариантная, многовариантная, индивидуальная;
* **по цели промежуточного контроля:** проверка знаний, проверка теоретических навыков и умений, проверка практических навыков и умений;
* **по использованию обучающимися средств обучения:** с использованием специального оборудования, без использования специального оборудования;
* **по количеству выполняющих задание:** индивидуальная оценка, групповая оценка.

Формы итоговой аттестации по образовательной программе:

* **по учету результатов промежуточной аттестации:** с учетом, без учета;
* **по участию преподавателя:** без преподавателя, очно, заочно;
* **по месту:** дистанционное, классное, полевое;
* **по охвату:** фронтальный, индивидуальный, групповой;
* **по времени:** нормированный (с указанием времени начала и конца урока), не нормированный;
* **по сложности:** с дифференциацией сложности, без дифференциации сложности;
* **по наличию вариантов ответов:** с заранее заданными вариантами ответов, без заранее заданных вариантов ответов;
* **по способу фиксации ответов:** письменное, устное, электронное, практическое, комбинированное;
* **по наличию формы ответа:** ответ по установленной форме, ответ без требований к форме;
* **по вариантам:** одновариантная, многовариантная, индивидуальная;
* **по цели промежуточного контроля:** проверка знаний, проверка теоретических навыков и умений, проверка практических навыков и умений;
* **по использованию обучающимися средств обучения:** с использованием специального оборудования, без использования специального оборудования;
* **по количеству выполняющих задание:** индивидуальная оценка, групповая оценка.
  + 1. **Распределение по периодам обучения учебных курсов и модулей**

Распределение по периодам обучения учебных курсов и модулей осуществляется на основании договора об образовании и оформляется в виде Календарного учебного графика.

* 1. **Условия образовательной деятельности**

Условия образовательной деятельности по образовательной программе должны соответствовать лицензионным нормативам и действующему законодательству, быть направлены на соблюдение прав обучающихся.

Условия образовательной деятельности по образовательной программе конкретизируется ФОНДОМ «ТРИОНИКС» совместно с заинтересованными участниками образовательного процесса с учетом потребностей лица, по инициативе которого осуществляется дополнительное профессиональное образование и указывается в договоре об образовании.

При этом в договоре об образовании должно быть указано материально-техническое обеспечение, объем оборудования помещений в соответствии с государственными, местными нормами и требованиями, соблюдение государственных санитарно-эпидемиологических правил и нормативов и пожарных требований, в том числе необходимые для качественного оказания услуг по образовательной программе: приборы, оборудование, техника, программное обеспечение, средства защиты информации.

* 1. **Оценочные материалы**

Для аттестации обучающихся на соответствие их персональных достижений требованиям по достижению указанных в договоре об образовании целей, планируемых результатов и приобретаемых компетенций, ФОНДОМ «ТРИОНИКС» самостоятельно создаются типовые задания, контрольные работы, тесты, позволяющие оценить знания, умения и уровень приобретенных компетенций.

Формы проведения аттестации указываются в Рабочей программе.

По согласованию ФОНДОМ «ТРИОНИКС» с лицом, по инициативе которого осуществляется дополнительное профессиональное образование, возможно проведение совместной с таким лицом или иными лицами аттестации.

1. **Приложения**
   1. **Формы документов о квалификации или об обучении**
   2. **Учебно-методические материалы**
   3. **Оценочные материалы**