МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Северо-Восточный федеральный университет имени М.К. Аммосова»

Утверждаю:
Ректор
_____
«21» 02 2013г.

Номер внутривузовской регистрации
179-13-3.0

АННОТАЦИЯ

к основной профессиональной образовательной программе
среднего профессионального образования

по специальности
090305.51 Информационная безопасность автоматизированных систем

Квалификация
Техник по защите информации

Форма обучения
очная

г. Якутск, 2013

СОДЕРЖАНИЕ

1. Общие положения

1.1. Основная профессиональная образовательная программа (ОПОП) по направлению подготовки 090000 Информационная безопасность по специальности **090305 Информационная безопасность автоматизированных систем** представляет собой систему документов, разработанную с учетом требований рынка труда на основе Федерального государственного образовательного стандарта по направлению подготовки среднего профессионального образования (ФГОС СПО) и рекомендованной примерной образовательной программы.

ОПОП регламентирует цели, ожидаемые результаты, содержание, условия и технологии реализации образовательного процесса, оценку качества подготовки выпускника по данному направлению подготовки и включает в себя: учебный план, рабочие программы учебных курсов, предметов, дисциплин (модулей) и другие материалы, обеспечивающие качество подготовки обучающихся, а также программы учебной и производственной практики, календарный учебный график и методические материалы, обеспечивающие реализацию соответствующей образовательной технологии.

1.2. Нормативные документы для разработки ОПОП

Нормативную правовую базу разработки ОПОП составляют:

- Федеральные законы Российской Федерации: «Об образовании» (от 10 июля 1992 г. №3266-1) и «О высшем и послевузовском профессиональном образовании» (от 22 августа 1996 г. №125-ФЗ);
- Типовое положение об образовательном учреждении высшего профессионального образования (высшем учебном заведении), утвержденное постановлением Правительства Российской Федерации от 14 февраля 2008 г. №71 (далее – Типовое положение о вузе);
- Типовое положение об образовательном учреждении среднего профессионального образования (среднем специальном учебном заведении), утвержденное постановлением Правительства Российской Федерации от 18 июля 2008 г. N 543 (далее – Типовое положение о ССУЗе);
- Федеральный государственный образовательный стандарт по направлению подготовки **090000 Информационная безопасность** по специальности **090305 Информационная безопасность автоматизированных систем** среднего профессионального образования, утвержденный приказом Министерства образования и науки Российской Федерации №708 от 24.06.2010 г.
- Нормативно-методические документы Минобрнауки России;
- Примерная основная образовательная программа (ПрООП СПО) по направлению подготовки, утвержденная приказом Министерства образования и науки Российской Федерации от 24.06.2010 г. №708. (носит рекомендательный характер);
- Устав университета (2011 г.);

1.3. Общая характеристика ОПОП СПО

1.3.1. Цель (миссия) ОПОП

Миссия ОПОП по укрупненной группе направлений подготовки и специальностей 090000 Информационная безопасность по специальности СПО 090305 **Информационная безопасность автоматизированных систем** взращивание на основе консолидации научных и образовательных ресурсов университета конкурентоспособных специалистов в области информационной безопасности, защите информации, способных принять участие в реализации технологического прорыва в экономике и социокультурного развития населения Северо – Востока России.

Основные цели ОПОП СПО по специальности **090305 Информационная безопасность автоматизированных систем** направления подготовки **090000 Информационная безопасность**: развитие у студентов личностных качеств, формирование общекультурных и профессиональных компетенций, развитие навыков их реализации в практической деятельности в соответствии с требованиями ФГОС СПО по

специальности **090305 Информационная безопасность автоматизированных систем** направления подготовки **090000 Информационная безопасность**, утвержденного приказом Министерства образования и науки Российской Федерации №708 от 24.06.2010 г.

1.3.2. Срок освоения ОПОП

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности **090305 Информационная безопасность автоматизированных систем** направления подготовки 090000 Информационная безопасность предполагает освоение обучающимися основной профессиональной образовательной программы (ОПОП) базовой подготовки (**срок обучения** на базе среднего (полного) общего образования 2 г. 10 мес.) с присвоением **квалификации** на базовом уровне подготовки «Техник по защите информации».

ОПОП базовой подготовки по специальности **090305 Информационная безопасность автоматизированных систем** направления подготовки **090000 Информационная безопасность** разработана на основе ФГОС по данной специальности СПО и является инструментом внедрения ФГОС в образовательную практику.

1.3.3. Трудоемкость ОПОП

Максимальная учебная нагрузка обучающихся: 4536 ч., в т.ч. обязательная – 3024 ч., самостоятельная работа – 1512 ч.

На учебную и производственную практику отводится – 900 ч., в т.ч. на учебную – 504 ч., на производственную – 396 ч.

На промежуточную аттестацию отводится – 5 нед.

На преддипломную практику отводится – 4 нед., подготовку выпускной квалификационной работы – 4 нед., защиту выпускной квалификационной работы – 2 нед.

На консультации отводится 300 часов.

1.4. Требования к абитуриенту

Абитуриент должен иметь документ государственного образца о среднем (полном) общем образовании или начальном профессиональном образовании.

2. Характеристика профессиональной деятельности выпускника ОПОП

2.1. Область профессиональной деятельности выпускника: организация и проведение работ по обеспечению защиты автоматизированных систем в организациях различных структур и отраслевой направленности.

Выпускник по данной специальности направления подготовки **090000 Информационная безопасность** может развернуть виды деятельности: 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).

Может занимать должности: техник по защите информации, компьютерным системам, техник – программист, системный администратор и другие. Предполагаемые места трудоустройства: различные предприятия, научно – исследовательские институты, органы управления и исполнительной власти, банки, финансовые и страховые компании и другие организации различных форм собственности.

2.2. Объекты профессиональной деятельности выпускника

Объектами профессиональной деятельности выпускника по специальности 090305 Информационная безопасность автоматизированных систем направления подготовки 090000 Информационная безопасность являются:

- автоматизированные системы;
- методы и средства обеспечения информационной безопасности автоматизированных систем;

- первичные трудовые коллективы.

2.3. Виды профессиональной деятельности выпускника

Техник по защите информации готовится к следующим видам деятельности:

2.3.1. Эксплуатация подсистем безопасности автоматизированных систем

2.3.2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

2.3.3. Применение инженерно-технических средств обеспечения информационной безопасности

2.3.4. Выполнение работ по рабочей профессии: 16199 Оператор электронно - вычислительных машин

2.3.5. Сетевые технологии

2.3.6. Участие в интеграции программных модулей

2.4. Задачи профессиональной деятельности выпускника

Задачи профессиональной деятельности выпускника по видам профессиональной деятельности сформулированы для каждого вида профессиональной деятельности на основе Федерального государственного образовательного стандарта по направлению подготовки 090000 Информационная безопасность по специальности 090305 Информационная безопасность автоматизированных систем среднего профессионального образования, утвержденного приказом Министерства образования и науки Российской Федерации №708 от 24.06.2010 г. и дополнены с учетом традиций учебного заведения и потребностями партнеров - работодателей.

С целью овладения указанными видами профессиональной деятельности и соответствующими профессиональными компетенциями в результате изучения профессиональных модулей обучающийся должен:

2.4.1. Эксплуатация подсистем безопасности автоматизированных систем

иметь практический опыт:

эксплуатации компонентов подсистем безопасности автоматизированных систем, их диагностики, устранения отказов и восстановления работоспособности; администрирования подсистем безопасности автоматизированных информационных систем; установки компонентов подсистем безопасности автоматизированных информационных систем;

уметь:

эксплуатировать компоненты подсистем безопасности автоматизированных систем; обеспечивать работоспособность, обнаруживать и устранять неисправности подсистем безопасности автоматизированных систем согласно технической документации; осуществлять комплектование, конфигурирование, настройку подсистем безопасности автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы; использовать и оформлять техническую документацию в соответствии с действующими нормативными документами; выполнять регламенты техники безопасности; организовывать и конфигурировать компьютерные сети; работать с протоколами разных уровней; устанавливать и настраивать параметры современных сетевых протоколов; производить монтаж компьютерных сетей; осуществлять диагностику компьютерных сетей; устранять неисправности компьютерных сетей;

знать:

состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ; основные приемы программирования; модели баз данных; классификацию, принципы построения, физические основы работы периферийных устройств: основные методы организации

и проведения технического обслуживания вычислительной техники и других технических средств информатизации; правила и нормы охраны труда, техники безопасности, промышленной санитарии и противопожарной защиты; основные понятия компьютерных сетей и их аппаратные компоненты; сетевые модели, протоколы и их установку в операционных системах; адресацию в сетях, организацию межсетевого воздействия.

2.4.2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

иметь практический опыт:

применения программно-аппаратных средств обеспечения информационной безопасности; диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности; мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности; обеспечения учета, обработки, хранения и передачи конфиденциальной информации; решения частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов; применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами;

уметь:

применять программно-аппаратные средства обеспечения информационной безопасности; диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности; оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности; участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; решать частные технические задачи, возникающих при аттестации объектов, помещений, программ, алгоритмов; использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись; применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

знать:

методы и формы применения программно-аппаратных средств обеспечения информационной безопасности; особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом: типовые средства, методы и протоколы идентификации, аутентификации и авторизации; типовые средства и методы ведения аудита и обнаружения вторжений; типовые средства и методы обеспечения; информационной безопасности в локальных и глобальных вычислительных сетях; основные понятия криптографии и типовые криптографические методы защиты информации.

2.4.3. Применение инженерно-технических средств обеспечения информационной безопасности

иметь практический опыт:

выявления технических каналов утечки информации; использования основных методов и средств инженерно-технической защиты информации; диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности; участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности; решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;

уметь:

применять технические средства защиты информации; использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам; применять нормативные правовые акты; нормативные методические документы по обеспечению информационной безопасности техническими средствами;

знать:

физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации; основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам; номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

2.4.4. Выполнение работ по рабочей профессии: 16199 Оператор электронно - вычислительных машин

иметь практический опыт:

1.1.1.1. ввода цифровой и аналоговой информации в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования;

1.1.1.2. конвертирования медиа файлов в различные форматы, экспорта и импорта файлов в различные программы-редакторы;

1.1.1.3. обработки аудио-, визуального и мультимедийного контента с помощью специализированных программ-редакторов;

1.1.1.4. создания и воспроизведения видео роликов, презентаций, слайд-шоу, медиа-файлов и другой игровой продукции из исходных аудио;

уметь:

1.3.2.1. подключать и настраивать параметры функционирования персонального компьютера, периферийного и мультимедийного оборудования;

1.3.2.2. настраивать основные компоненты графического интерфейса операционной системы и специализированных программ редакторов;

1.3.2.3. управлять файлами данных на локальных, съемных запоминающихся устройствах, а также на дисках локальной компьютерной сети и в Интернете;

1.3.2.4. вводить цифровую и аналоговую информацию в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования;

1.3.2.5. создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;

1.3.2.6. Конвертировать файлы с цифровой информацией в различные форматы;

1.3.2.7. производить сканирование прозрачных и непрозразных оригиналов;

1.3.2.8. производить съемку и передачу цифровых изображений с фото- и видеокамеры на персональный компьютер;

1.3.2.9. обрабатывать аудио, визуальный контент и медиа-файлы средствами звуковых, графических и видео-редакторов;

1.3.2.10. создавать видео-ролики, презентации, слайд шоу, медиа-файлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов;

1.3.2.11. воспроизводить аудио, визуальный контент и медиа-файлы средствами персонального компьютера и мультимедийного оборудования;

1.3.2.12. производить распечатку, копирование и тиражирование документов на принтер и другие периферийные устройства вывода;

1.3.2.13. использовать мультимедиа-проектор для демонстрации содержимого экранных форм с персонального компьютера;

1.3.2.14. вести отчетную и техническую документацию;

знать:

1.3.3.1. принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;

1.3.3.2. виды и параметры форматов аудио-, графических- и видео-и мультимедийных файлов и методы их конвертирования;

1.3.3.3. назначение, возможности, правила эксплуатации мультимедийного оборудования;

1.3.3.4. основные типы интерфейсов для подключения мультимедийного оборудования;

1.3.3.5. основные приемы обработки цифровой информации;

1.3.3.6. назначение, разновидности и функциональные возможности программ обработки звука;

1.3.3.7. назначение, разновидности и функциональные возможности программ графических изображений;

1.3.3.8. назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента.

2.4.5. Сетевые технологии

иметь практический опыт:

- по настройке сервера и рабочих станций для безопасной передачи информации;
- установки Web - сервера;
- организации доступа к локальным и глобальным сетям;
- сопровождению и контролю использования почтового сервера, SQL - сервера и др.;
- расчета стоимости лицензионного программного обеспечения сетевой инфраструктуры;
- сбора данных для анализа использования и функционирования программно-технических средств компьютерных сетей;

уметь:

- администрировать локальные вычислительные сети;
- принимать меры по устранению возможных сбоев;
- устанавливать информационную систему;
- создавать и конфигурировать учетные записи отдельных пользователей и пользовательских групп;
- регистрировать подключение к домену, вести отчетную документацию;
- рассчитывать стоимость лицензионного программного обеспечения сетевой инфраструктуры;
- устанавливать и конфигурировать антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга,
- обеспечивать защиту при подключении к Интернет средствами операционной системы;
- разрабатывать и тестировать программы с применением программных средсвт, используемых в современных инфокоммуникационных технологиях
- использовать специальную литературу в изучаемой предметной области

знать:

- основные принципы администрирования компьютерных сетей, основные задачи обслуживания;
- типы серверов; технологию «клиент-сервер»; способы установки и управления сервером; утилиты, функции, удаленное управление сервером;
- технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в Web;

- мониторинг и настройку производительности;
- технологию ведения отчетной документации;
- классификацию программного обеспечения сетевых технологий, и область его применения;
- лицензирование программного обеспечения;
- оценку стоимости программного обеспечения в зависимости от способа и места его использования
- основные технологии программирования в программных средствах, используемых в современных инфокоммуникационных технологиях

2.4.6. Участие в интеграции программных модулей

иметь практический опыт:

участия в выработке требований к программному обеспечению; участия в проектировании программного обеспечения с использованием специализированных программных пакетов;

уметь:

владеть основными методологиями процессов разработки программного обеспечения; использовать методы для получения кода с заданной функциональностью и степенью качества;

знать:

модели процесса разработки программного обеспечения; основные принципы процесса разработки программного обеспечения; основные подходы к интегрированию программных модулей; основные методы и средства эффективной разработки; основы верификации и аттестации программного обеспечения; концепции и реализации программных процессов; принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного обеспечения; методы организации работы в коллективах разработчиков программного обеспечения; основные положения метрологии программных продуктов, принципы построения, проектирования и использования средств для измерений характеристик и параметров программ, программных систем и комплексов; стандарты качества программного обеспечения; методы и средства разработки программной документации

3. Компетенции выпускника ОПОП

В результате освоения данной ОПОП выпускник должен обладать следующими компетенциями:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

ОК 11. Формулировать задачи логического характера и применять средства математической логики для их решения.

ОК 12. Владеть основными методами и средствами разработки программного обеспечения.

ОК 13. Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

5.2. Техник по защите информации должен обладать **профессиональными компетенциями,** соответствующими основным видам профессиональной деятельности:

5.2.1. Эксплуатация подсистем безопасности автоматизированных систем

ПК 1.1. 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.

ПК 1.2. Выполнять работы по администрированию подсистем безопасности автоматизированных систем.

ПК 1.3. Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.

ПК 1.4. Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.

ПК 1.5. Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.

5.2.2. **Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах**

ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.

ПК 2.2. 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.

ПК 2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

ПК 2.5. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.

ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

5.2.3. **Применение инженерно-технических средств обеспечения информационной безопасности**

ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.

ПК 3.2. 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.

ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.

ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

5.2.4. Выполнение работ по рабочей профессии: 16199 Оператор электронно - вычислительных машин

ПК 6.1. Выполнять ввод цифровой и аналоговой информации в персональный компьютер с различных носителей;

ПК 6.2. Конвертировать файлы с цифровой информацией в различные форматы;

ПК 6.3. Обрабатывать аудио и визуальный контент средствами звуковых, графических и видео-редакторов;

ПК 6.4. Создавать видео-ролики, презентации, слайд-шоу, медиа-файлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов;

ПК 6.5. Воспроизводить аудио, визуальный контент и медиа-файлы средствами персонального компьютера и мультимедийного оборудования.

5.2.5. Сетевые технологии

ПК 4.1. Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.

ПК 4.2. Выполнять интеграцию модулей в программную систему.

ПК 4.3. Выполнять отладку программного продукта с использованием специализированных программных средств.

ПК 4.4. Осуществлять разработку тестовых наборов и тестовых сценариев.

ПК 4.5. Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.

ПК 4.6. Разрабатывать технологическую документацию.

ПК 6.2. Выполнять требования нормативно-технической документации.

5.2.6. Участие в интеграции программных модулей

ПК 4.1. Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.

ПК 4.2. Выполнять интеграцию модулей в программную систему.

ПК 4.3. Выполнять отладку программного продукта с использованием специализированных программных средств.

ПК 4.4. Осуществлять разработку тестовых наборов и тестовых сценариев.

ПК 4.5. Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.

ПК 4.6. Разрабатывать технологическую документацию.

ПК 6.2. Выполнять требования нормативно-технической документации.

4. Документы, регламентирующие содержание и организацию образовательного процесса при реализации ОПОП

4.1. Календарный учебный график

Календарный учебный график см. в Приложении 3

4.2. Учебный план

Учебный план см. в Приложении 1

4.3. Рабочие программы учебных дисциплин (модулей) (Аннотации см. в Приложении 2).

ЕН Математический и общий естественнонаучный цикл

ЕН.1 Математика

ЕН.2 Информатика

ЕН.3 Физика

П Профессиональный цикл

ОП Общепрофессиональные дисциплины

ОП.1 Основы информационной безопасности

ОП.2 Технические средства информатизации

ОП.3 Организационно - правовое обеспечение информационной безопасности

ОП.4 Сети и системы передачи информации

ОП.5 Основы алгоритмизации и программирования

ОП.6 Электроника и схемотехника

ОП.7 Операционные системы

ОП.8 Базы данных

ОП.9 Экономика организации

ОП.10 Менеджмент

ОП.11 Методы и средства защиты информации

ОП.12 Электротехника

ОП.13 Компьютерная графика

ОП.14 Метрология, стандартизация и сертификация

ОП.15 Безопасность жизнедеятельности

ПМ Профессиональные модули

ПМ.1 Эксплуатация подсистем безопасности автоматизированных систем

МДК.1.1 Эксплуатация подсистем безопасности автоматизированных систем

МДК.1.2 Эксплуатация компьютерных сетей

ПМ.2 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

МДК.2.1 Программно аппаратные средства обеспечения информационной безопасности

МДК.2.2 Криптографические средства и методы защиты информации

ПМ.3 Применение инженерно-технических средств обеспечения информационной безопасности

МДК.3.1 Применение инженерно-технических средств обеспечения информационной безопасности

ПМ.4 Выполнение работ по рабочей профессии: 16199 Оператор электронно - вычислительных машин

МДК.4.1 Технология создания и обработки мультимедийной информации

ПМ.5 Сетевые технологии

МДК.5.1 Web-программирование

ПМ.6 Участие в интеграции программных модулей

МДК.6.1 Технология разработки программного обеспечения

МДК.6.2 Инструментальные средства разработки программного продукта

4.4. Программы учебной и производственной практик.

4.4.1. Программы учебных практик.

Аннотация программы практики.

Направление подготовки	***090000 Информационная безопасность***
Специальность:	**090305 Информационная безопасность автоматизированных систем**
Профиль подготовки	
Квалификация (степень) выпускника	***Техник по защите информации***
Цикл, раздел учебного плана	Учебная и производственная практика
Семестр(ы) изучения	*II-VI*
Количество зачетных единиц (кредитов)	*468*
Форма промежуточной аттестации (зачет/экзамен)	*зачет*
Количество часов всего, из них:	*14 недель,*
I курс	*4 недели*
II курс	*9 недель*
III курс	*1 неделя*

1. Целями учебной практики по направлению подготовки 090000 Информационная безопасность по специальности 090305 Информационная безопасность автоматизированных систем являются формирование и развитие профессиональных компетенций и профессиональных знаний в сфере избранной специальности, закрепление полученных теоретических знаний и овладение необходимыми методами по новым видам деятельности, использование результатов практики для подготовки выпускной квалификационной работы.

3. **Компетенции студента, формируемые в результате прохождения учебной практики:**

Общие компетенции, включающие в себя способность:

- ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
- ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
- ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
- ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

– ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

Профессиональные компетенции, соответствующие основным видам профессиональной деятельности:

ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем

ПК 1.1. 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.

ПК 1.2. Выполнять работы по администрированию подсистем безопасности автоматизированных систем.

ПК 1.3. Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.

ПК 1.4. Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.

ПК 1.5. Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.

ПМ 2. **Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах**

ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.

ПК 2.2. 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.

ПК 2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

ПК 2.5. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.

ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

ПМ 3. Применение инженерно-технических средств обеспечения информационной безопасности

ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.

ПК 3.2. 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.

ПК 3.3. Участвовать в мониторинге эффективности применяемых безопасности.

ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

ПМ 4. Выполнение работ по рабочей профессии: 16199 Оператор электронно-

вычислительных машин

ПК 4.1. Выполнять ввод цифровой и аналоговой информации в персональный компьютер с различных носителей;

ПК 4.2. Конвертировать файлы с цифровой информацией в различные форматы;

ПК 4.3. Обрабатывать аудио и визуальный контент средствами звуковых, графических и видео-редакторов;

ПК 4.4. Создавать видео-ролики, презентации, слайд-шоу, медиа-файлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов;

ПК 4.5. Воспроизводить аудио, визуальный контент и медиа-файлы средствами персонального компьютера и мультимедийного оборудования.

ПМ 5. Сетевые технологии

ПК 4.1. Участвовать в разработке организационной структуры комплексной системы обеспечения информационной безопасности.

ПК 4.2. Участвовать в оценке эффективности комплексной системы обеспечения информационной безопасности.

ПК 4.3. Участвовать в мониторинге эффективности комплексных систем обеспечения информационной безопасности.

ПМ 6. Участие в интеграции программных модулей

ПК 4.1. Участвовать в разработке организационной структуры комплексной системы обеспечения информационной безопасности.

ПК 4.2. Участвовать в оценке эффективности комплексной системы обеспечения информационной безопасности.

ПК 4.3. Участвовать в мониторинге эффективности комплексных систем обеспечения информационной безопасности.

В результате прохождения учебной практики обучающийся должен демонстрировать следующие результаты образования:

1)Знать

ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.2. Эксплуатация компьютерных сетей

- состав и принципы работы автоматизированных систем, операционных систем и сред;
- принципы разработки алгоритмов программ; основные приемы программирования; модели баз данных;
- классификацию, принципы построения, физические основы работы периферийных устройств: основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;
- правила и нормы охраны труда, техники безопасности, промышленной санитарии и противопожарной защиты;

ПМ 2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

МДК 2.1. Программно-аппаратные средства обеспечения информационной безопасности

МДК 2.2. Криптографические средства и методы защиты информации

- методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
- особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;

- типовые модели управления доступом: типовые средства, методы и протоколы идентификации, аутентификации и авторизации;

- типовые средства и методы ведения аудита и обнаружения вторжений; типовые средства и методы обеспечения **информационной безопасности в локальных и глобальных вычислительных сетях;**

- основные понятия криптографии и типовые криптографические методы защиты информации.

ПМ.3. Применение инженерно-технических средств обеспечения информационной безопасности

МДК 3.1. Применение инженерно-технических средств обеспечения информационной безопасности

- физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

- номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;

- основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам;

- номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

ПМ 4. Выполнение работ по рабочей профессии: 16199 Оператор электронно-вычислительных машин

МДК 4.1. Технология создания и обработки мультимедийной информации

- принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;
- виды и параметры форматов аудио-, графических- и видео-и мультимедийных файлов и методы их конвертирования;
- назначение, возможности, правила эксплуатации мультимедийного оборудования;
- основные типы интерфейсов для подключения мультимедийного оборудования;
- основные приемы обработки цифровой информации;
- назначение, разновидности и функциональные возможности программ обработки звука;
- назначение, разновидности и функциональные возможности программ графических изображений;
- назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента.

ПМ.5.СЕТЕВЫЕ ТЕХНОЛОГИИ

МДК.5.1. Web-программирование

- основные направления администрирования компьютерных сетей;
- типы серверов, технологию «клиент-сервер»; способы установки и управления сервером; утилиты, функции, удаленное управление сервером;
- технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в Web;
- использование кластеров;
- взаимодействие различных операционных систем; автоматизацию задач обслуживания;
- мониторинг и настройку производительности;
- технологию ведения отчетной документации;
- классификацию программного обеспечения сетевых технологий, и область его применения;

- лицензирование программного обеспечения;
- оценку стоимости программного обеспечения в зависимости от способа и места его использования
- основные технологии программирования в программных средствах, используемых в современных инфокоммуникационных технологиях

ПМ.6. Участие в интеграции программных модулей

МДК 6.1. Технология разработки программного обеспечения

МДК 6.2. Инструментальные средства разработки программного продукта

- модели процесса разработки программного обеспечения;
- основные принципы процесса разработки программного обеспечения;
- основные подходы к интегрированию программных модулей;
- основные методы и средства эффективной разработки;
- основы верификации и аттестации программного обеспечения;
- концепции и реализации программных процессов;
- принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного обеспечения;
- методы организации работы в коллективах разработчиков программного обеспечения;
- основные положения метрологии программных продуктов, принципы построения, проектирования и использования средств для измерений характеристик и параметров программ, программных систем и комплексов
- стандарты качества программного обеспечения
- методы и средства разработки программной документации

2) Уметь

ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.2. Эксплуатация компьютерных сетей

- эксплуатировать компоненты подсистем безопасности автоматизированных систем;

- обеспечивать работоспособность, обнаруживать и устранять неисправности подсистем безопасности автоматизированных систем согласно технической документации;

- осуществлять комплектование, конфигурирование, настройку подсистем безопасности автоматизированных систем;

- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы; использовать и оформлять техническую документацию в соответствии с действующими нормативными документами;

- выполнять регламенты техники безопасности; организовывать и конфигурировать компьютерные сети; работать с протоколами разных уровней; устанавливать и настраивать параметры современных сетевых протоколов;

- производить монтаж компьютерных сетей; осуществлять диагностику компьютерных сетей; устранять неисправности компьютерных сетей;

ПМ 2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

МДК 2.1. Программно-аппаратные средства обеспечения информационной безопасности

МДК 2.2. Криптографические средства и методы защиты информации

- применять программно-аппаратные средства обеспечения информационной безопасности;

- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;
- оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;
- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;
- решать частные технические задачи, возникающих при аттестации объектов, помещений, программ, алгоритмов;
- использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

ПМ.3. Применение инженерно-технических средств обеспечения информационной безопасности

МДК 3.1. Применение инженерно-технических средств обеспечения информационной безопасности

- применять технические средства защиты информации;
- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
- использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам;
- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами.

ПМ.4. Выполнение работ по рабочей профессии: 161999 Оператор электронно-вычислительных машин

МДК.4.1. Технология создания и обработки мультимедийной информации

- подключать и настраивать параметры функционирования персонального компьютера, периферийного и мультимедийного оборудования;
- настраивать основные компоненты графического интерфейса операционной системы и специализированных программ редакторов;
- управлять файлами данных на локальных, съемных запоминающихся устройствах, а также на дисках локальной компьютерной сети и в Интернете;
- вводить цифровую и аналоговую информацию в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования;
- создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;
- Конвертировать файлы с цифровой информацией в различные форматы;
- производить сканирование прозрачных и непрозразных оригиналов;
- производить съемку и передачу цифровых изображений с фото- и видеокамеры на персональный компьютер;
- обрабатывать аудио, визуальный контент и медиа-файлы средствами звуковых, графических и видео-редакторов;
- создавать видео-ролики, презентации, слайд шоу, медиа-файлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов;
- воспроизводить аудио, визуальный контент и медиа-файлы средствами персонального компьютера и мультимедийного оборудования;
- производить распечатку, копирование и тиражирование документов на принтер и другие периферийные устройства вывода;
- использовать мультимедиа-проектор для демонстрации содержимого экранных форм с персонального компьютера;
- вести отчетную и техническую документацию;

ПМ.5. СЕТЕВЫЕ ТЕХНОЛОГИИ

МДК.5.2. Web-программирование

- администрировать локальные вычислительные сети;
- принимать меры по устранению возможных сбоев;
- устанавливать информационную систему;
- создавать и конфигурировать учетные записи отдельных пользователей и пользовательских групп;
- регистрировать подключение к домену, вести отчетную документацию;
- рассчитывать стоимость лицензионного программного обеспечения сетевой инфраструктуры;
- устанавливать и конфигурировать антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга,
- обеспечивать защиту при подключении к Интернет средствами операционной системы;
- разрабатывать и тестировать программы с применением программных средств, используемых в современных инфокоммуникационных технологиях
- использовать специальную литературу в изучаемой предметной области

ПМ.6. Участие в интеграции программных модулей

МДК.6.1. Технология разработки программного обеспечения

МДК.6.2. Инструментальные средства разработки программного продукта

- участия в выработке требований к программному обеспечению;
- участия в проектировании программного обеспечения с использованием специализированных программных пакетов;

3) Владеть

ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.2. Эксплуатация компьютерных сетей

- эксплуатации компонентов подсистем безопасности автоматизированных систем, их диагностики, устранения отказов и восстановления работоспособности;
- администрирования подсистем безопасности автоматизированных информационных систем;
- установки компонентов подсистем безопасности автоматизированных информационных систем

ПМ 2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

МДК 2.1. Программно-аппаратные средства обеспечения информационной безопасности

МДК 2.2. Криптографические средства и методы защиты информации

- применения программно-аппаратных средств обеспечения информационной безопасности;
- диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;
- мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;
- обеспечения учета, обработки, хранения и передачи конфиденциальной информации;
- решения частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
- применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами;

ПМ.3. Применение инженерно-технических средств обеспечения информационной безопасности

МДК 3.1. Применение инженерно-технических средств обеспечения информационной безопасности

- выявления технических каналов утечки информации;
- использования основных методов и средств инженерно-технической защиты информации;
- диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;
- участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;
- решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;

ПМ.4. Выполнение работ по рабочей профессии: 161999 Оператор электронно-вычислительных машин

МДК.4.1. Технология создания и обработки мультимедийной информации

- принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;
- виды и параметры форматов аудио-, графических- и видео-и мультимедийных файлов и методы их конвертирования;
- назначение, возможности, правила эксплуатации мультимедийного оборудования;
- основные типы интерфейсов для подключения мультимедийного оборудования;
- основные приемы обработки цифровой информации;
- назначение, разновидности и функциональные возможности программ обработки звука;
- назначение, разновидности и функциональные возможности программ графических изображений;
- назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента.

ПМ.5. Сетевые технологии

МДК. 5.1. Web-программирование

- по настройке сервера и рабочих станций для безопасной передачи информации;
- установки Web - сервера;
- организации доступа к локальным и глобальным сетям;
- сопровождению и контролю использования почтового сервера, SQL - сервера и др.;
- расчета стоимости лицензионного программного обеспечения сетевой инфраструктуры;
- сбора данных для анализа использования и функционирования программно-технических средств компьютерных сетей;

ПМ.6. Участие в интеграции программных модулей

МДК.6.1. Технология разработки программного обеспечения

МДК.6.2. Инструментальные средства разработки программного продукта

- участия в выработке требований к программному обеспечению;

участия в проектировании программного обеспечения с использованием специализированных программных пакетов.

3. Краткое содержание учебной практики

Разделы (этапы) практики
Подготовительный этап, включающий установочную конференцию (инструктаж по

технике безопасности)
ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем
МДК 1.1. Эксплуатация подсистем безопасности автоматизированных систем МДК 1.2. Эксплуатация компьютерных сетей
Учебная практика Виды работ • эксплуатирование компонентов подсистем безопасности автоматизированных систем; • обеспечение работоспособности, обнаружение и устранение неисправности подсистем безопасности автоматизированных систем согласно технической документации; • комплектование, конфигурирование, настройка подсистем безопасности автоматизированн**ых систем;** • установка, адаптация и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы;
ПМ 2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах МДК 2.1. Программно-аппаратные средства обеспечения информационной безопасности МДК 2.2. Криптографические средства и методы защиты информации
Виды работ: • **применение программно-аппаратных средств обеспечения информационной безопасности;** • диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности; • оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности; • участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; • решать частные технические задачи, возникающих при аттестации объектов, помещений, программ, алгоритмов; • использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись; • применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами;
ПМ.3. Применение инженерно-технических средств обеспечения информационной безопасности МДК 3.1. Применение инженерно-технических средств обеспечения информационной безопасности
Виды работ: • применять технические средства защиты информации; • использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; • использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам;
ПМ.4. Выполнение работ по рабочей профессии: 161999 Оператор электронно-вычислительных машин МДК.4.1. Технология создания и обработки мультимедийной информации
Учебная практика Виды работ • Методы обработки фотографий • Технологии создания и обработки мультимедийной информации
ПМ.5. Сетевые технологии МДК. 5.1. Web-программирование

Учебная практика Виды работ ♠ Установка и настройка стека TCP/IP. ♠ Установка сетевого программного обеспечения общего назначения ♠ Программное обеспечение поиска неисправностей в сетях, анализа и моделирования сетей ♠ Внедрение удаленного доступа ♠ Установка и настройка Windows Server 2008 ♠ Протокола RADIUS ♠ Сервер сетевых политик (Network Policy Server – NPS) ♠ Разработка статического сайта ♠ Разработка динамического сайта
ПМ.6. Участие в интеграции программных модулей МДК.6.1. Технология разработки программного обеспечения МДК.6.2. Инструментальные средства разработки программного продукта
Учебная практика Виды работ: ♠ Разработка технологической документации; ♠ Разработка программного продукта с использованием ООП Разработка программного продукта с использованием ООП; ♠ Автоматизированное тестирование; ♠ Работа с CASE-средством; ♠ Организация работ при коллективной разработке программных продуктов Организация работ при коллективной разработке программных продуктов;

4.4.2. Программа производственной практики.

Аннотация программы практики.

Направление подготовки	***090000 Информационная безопасность***
Специальность:	**090305 Информационная безопасность автоматизированных систем**
Профиль подготовки	
Квалификация (степень) выпускника	***Техник по защите информации***
Цикл, раздел учебного плана	Производственная и производственная практика
Семестр(ы) изучения	*III*
Количество зачетных единиц (кредитов)	*396*
Форма промежуточной аттестации (зачет/экзамен)	*зачет*
Количество часов всего, из них:	*4 недели*
III курс	*4 недели*

1. Целями производственной практики по направлению подготовки 090000 Информационная безопасность по специальности 090305 Информационная безопасность автоматизированных систем являются формирование и развитие профессиональных компетенций и профессиональных знаний в сфере избранной специальности, закрепление полученных теоретических знаний и овладение необходимыми методами по новым видам деятельности, использование результатов практики для подготовки выпускной квалификационной работы.

4. **Компетенции студента, формируемые в результате прохождения производственной практики:**

Общие компетенции, включающие в себя способность:

- ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
- ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
- ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
- ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
- ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

Профессиональные компетенции, соответствующие основным видам профессиональной деятельности:

ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем

ПК 1.1. 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.

ПК 1.2. Выполнять работы по администрированию подсистем безопасности автоматизированных систем.

ПК 1.3. Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.

ПК 1.4. Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.

ПК 1.5. Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.

ПМ 2. **Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах**

ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.

ПК 2.2. 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.

ПК 2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

ПК 2.5. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.

ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

ПМ 3. Применение инженерно-технических средств обеспечения информационной безопасности

ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.

ПК 3.2. 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.

ПК 3.3. Участвовать в мониторинге эффективности применяемых безопасности.

ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

ПМ 4. Выполнение работ по рабочей профессии: 16199 Оператор электронно-вычислительных машин

ПК 4.1. Выполнять ввод цифровой и аналоговой информации в персональный компьютер с различных носителей;

ПК 4.2. Конвертировать файлы с цифровой информацией в различные форматы;

ПК 4.3. Обрабатывать аудио и визуальный контент средствами звуковых, графических и видео-редакторов;

ПК 4.4. Создавать видео-ролики, презентации, слайд-шоу, медиа-файлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов;

ПК 4.5. Воспроизводить аудио, визуальный контент и медиа-файлы средствами персонального компьютера и мультимедийного оборудования.

ПМ 5. Сетевые технологии

ПК 4.1. Участвовать в разработке организационной структуры комплексной системы обеспечения информационной безопасности.

ПК 4.2. Участвовать в оценке эффективности комплексной системы обеспечения информационной безопасности.

ПК 4.3. Участвовать в мониторинге эффективности комплексных систем обеспечения информационной безопасности.

ПМ 6. Участие в интеграции программных модулей

ПК 4.1. Участвовать в разработке организационной структуры комплексной системы обеспечения информационной безопасности.

ПК 4.2. Участвовать в оценке эффективности комплексной системы обеспечения информационной безопасности.

ПК 4.3. Участвовать в мониторинге эффективности комплексных систем обеспечения информационной безопасности.

В результате прохождения производственной практики обучающийся должен демонстрировать следующие результаты образования:

1)Знать

ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.2. Эксплуатация компьютерных сетей

- состав и принципы работы автоматизированных систем, операционных систем и сред;
- принципы разработки алгоритмов программ; основные приемы программирования; модели баз данных;
- классификацию, принципы построения, физические основы работы периферийных устройств: основные методы организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;
- правила и нормы охраны труда, техники безопасности, промышленной санитарии и противопожарной защиты;

ПМ 2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

МДК 2.1. Программно-аппаратные средства обеспечения информационной безопасности

МДК 2.2. Криптографические средства и методы защиты информации

- методы и формы применения программно-аппаратных средств обеспечения информационной безопасности;
- особенности применения программно-аппаратных средств обеспечения информационной безопасности в операционных системах, компьютерных сетях, базах данных;
- типовые модели управления доступом: типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- типовые средства и методы ведения аудита и обнаружения вторжений; типовые средства и методы обеспечения информационной безопасности в локальных и глобальных вычислительных сетях;
- основные понятия криптографии и типовые криптографические методы защиты информации.

ПМ.3. Применение инженерно-технических средств обеспечения информационной безопасности

МДК 3.1. Применение инженерно-технических средств обеспечения информационной безопасности

- физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации;
- основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съёма и утечки по техническим каналам;
- номенклатуру применяемых средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

ПМ 4. Выполнение работ по рабочей профессии: 16199 Оператор электронно-вычислительных машин

МДК 4.1. Технология создания и обработки мультимедийной информации

- принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;
- виды и параметры форматов аудио-, графических- и видео-и мультимедийных файлов и методы их конвертирования;
- назначение, возможности, правила эксплуатации мультимедийного оборудования;
- основные типы интерфейсов для подключения мультимедийного оборудования;

- основные приемы обработки цифровой информации;
- назначение, разновидности и функциональные возможности программ обработки звука;
- назначение, разновидности и функциональные возможности программ графических изображений;
- назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента.

ПМ.5.СЕТЕВЫЕ ТЕХНОЛОГИИ

МДК.5.1. Web-программирование

- основные направления администрирования компьютерных сетей;
- типы серверов, технологию «клиент-сервер»; способы установки и управления сервером; утилиты, функции, удаленное управление сервером;
- технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в Web;
- использование кластеров;
- взаимодействие различных операционных систем; автоматизацию задач обслуживания;
- мониторинг и настройку производительности;
- технологию ведения отчетной документации;
- классификацию программного обеспечения сетевых технологий, и область его применения;
- лицензирование программного обеспечения;
- оценку стоимости программного обеспечения в зависимости от способа и места его использования
- основные технологии программирования в программных средствах, используемых в современных инфокоммуникационных технологиях.

ПМ.6. Участие в интеграции программных модулей

МДК 6.1. Технология разработки программного обеспечения

МДК 6.2. Инструментальные средства разработки программного продукта

- модели процесса разработки программного обеспечения;
- основные принципы процесса разработки программного обеспечения;
- основные подходы к интегрированию программных модулей;
- основные методы и средства эффективной разработки;
- основы верификации и аттестации программного обеспечения;
- концепции и реализации программных процессов;
- принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного обеспечения;
- методы организации работы в коллективах разработчиков программного обеспечения;
- основные положения метрологии программных продуктов, принципы построения, проектирования и использования средств для измерений характеристик и параметров программ, программных систем и комплексов
- стандарты качества программного обеспечения
- методы и средства разработки программной документации

2) Уметь

ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.2. Эксплуатация компьютерных сетей

- эксплуатировать компоненты подсистем безопасности автоматизированных систем;

- обеспечивать работоспособность, обнаруживать и устранять неисправности подсистем безопасности автоматизированных систем согласно технической документации;

- осуществлять комплектование, конфигурирование, настройку подсистем безопасности автоматизированных систем;

- производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы; использовать и оформлять техническую документацию в соответствии с действующими нормативными документами;

- выполнять регламенты техники безопасности; организовывать и конфигурировать компьютерные сети; работать с протоколами разных уровней; устанавливать и настраивать параметры современных сетевых протоколов;

- производить монтаж компьютерных сетей; осуществлять диагностику компьютерных сетей; устранять неисправности компьютерных сетей;

ПМ 2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

МДК 2.1. Программно-аппаратные средства обеспечения информационной безопасности

МДК 2.2. Криптографические средства и методы защиты информации

- применять программно-аппаратные средства обеспечения информационной безопасности;

- диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности;

- оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;

- участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;

- решать частные технические задачи, возникающих при аттестации объектов, помещений, программ, алгоритмов;

- использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;

- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами;

ПМ.3. Применение инженерно-технических средств обеспечения информационной безопасности

МДК 3.1. Применение инженерно-технических средств обеспечения информационной безопасности

- **применять технические средства защиты информации;**

- использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;

- использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам;

- применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами.

ПМ.4. Выполнение работ по рабочей профессии: 161999 Оператор электронно-вычислительных машин

МДК.4.1. Технология создания и обработки мультимедийной информации

- подключать и настраивать параметры функционирования персонального компьютера, периферийного и мультимедийного оборудования;
- настраивать основные компоненты графического интерфейса операционной системы и специализированных программ редакторов;

- управлять файлами данных на локальных, съемных запоминающихся устройствах, а также на дисках локальной компьютерной сети и в Интернете;
- вводить цифровую и аналоговую информацию в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования;
- создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;
- Конвертировать файлы с цифровой информацией в различные форматы;
- производить сканирование прозрачных и непрозразных оригиналов;
- производить съемку и передачу цифровых изображений с фото- и видеокамеры на персональный компьютер;
- обрабатывать аудио, визуальный контент и медиа-файлы средствами звуковых, графических и видео-редакторов;
- создавать видео-ролики, презентации, слайд шоу, медиа-файлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов;
- воспроизводить аудио, визуальный контент и медиа-файлы средствами персонального компьютера и мультимедийного оборудования;
- производить распечатку, копирование и тиражирование документов на принтер и другие периферийные устройства вывода;
- использовать мультимедиа-проектор для демонстрации содержимого экранных форм с персонального компьютера;
- вести отчетную и техническую документацию;

ПМ.5. СЕТЕВЫЕ ТЕХНОЛОГИИ

МДК.5.2. Web-программирование

- администрировать локальные вычислительные сети;
- принимать меры по устранению возможных сбоев;
- устанавливать информационную систему;
- создавать и конфигурировать учетные записи отдельных пользователей и пользовательских групп;
- регистрировать подключение к домену, вести отчетную документацию;
- рассчитывать стоимость лицензионного программного обеспечения сетевой инфраструктуры;
- устанавливать и конфигурировать антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга,
- обеспечивать защиту при подключении к Интернет средствами операционной системы;
- разрабатывать и тестировать программы с применением программных средств, используемых в современных инфокоммуникационных технологиях
- использовать специальную литературу в изучаемой предметной области

ПМ.6. Участие в интеграции программных модулей

МДК.6.1. Технология разработки программного обеспечения

МДК.6.2. Инструментальные средства разработки программного продукта

- участия в выработке требований к программному обеспечению;
- участия в проектировании программного обеспечения с использованием специализированных программных пакетов;

3) Владеть

ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.1. Эксплуатация подсистем безопасности автоматизированных систем

МДК 1.2. Эксплуатация компьютерных сетей

- **эксплуатации компонентов подсистем безопасности автоматизированных систем, их диагностики, устранения отказов и восстановления работоспособности;**

- **администрирования подсистем безопасности автоматизированных информационных систем;**
- **установки компонентов подсистем безопасности автоматизированных информационных систем**

ПМ 2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

МДК 2.1. Программно-аппаратные средства обеспечения информационной безопасности

МДК 2.2. Криптографические средства и методы защиты информации

- применения программно-аппаратных средств обеспечения информационной безопасности;
- диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности;
- мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности;
- обеспечения учета, обработки, хранения и передачи конфиденциальной информации;
- решения частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов;
- применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами;

ПМ.3. Применение инженерно-технических средств обеспечения информационной безопасности

МДК 3.1. Применение инженерно-технических средств обеспечения информационной безопасности

- выявления технических каналов утечки информации;
- использования основных методов и средств инженерно-технической защиты информации;
- диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности;
- участия в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности;
- решения частных технических задач, возникающих при аттестации объектов, помещений, технических средств;

ПМ.4. Выполнение работ по рабочей профессии: 161999 Оператор электронно-вычислительных машин

МДК.4.1. Технология создания и обработки мультимедийной информации

- принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;
- виды и параметры форматов аудио-, графических- и видео-и мультимедийных файлов и методы их конвертирования;
- назначение, возможности, правила эксплуатации мультимедийного оборудования;
- основные типы интерфейсов для подключения мультимедийного оборудования;
- основные приемы обработки цифровой информации;
- назначение, разновидности и функциональные возможности программ обработки звука;
- назначение, разновидности и функциональные возможности программ графических изображений;

- назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента.

ПМ.5. Сетевые технологии

МДК. 5.1. Web-программирование

- по настройке сервера и рабочих станций для безопасной передачи информации;
- установки Web - сервера;
- организации доступа к локальным и глобальным сетям;
- сопровождению и контролю использования почтового сервера, SQL - сервера и др.;
- расчета стоимости лицензионного программного обеспечения сетевой инфраструктуры;
- сбора данных для анализа использования и функционирования программно-технических средств компьютерных сетей;

ПМ.6. Участие в интеграции программных модулей

МДК.6.1. Технология разработки программного обеспечения

МДК.6.2. Инструментальные средства разработки программного продукта

- участия в выработке требований к программному обеспечению;

участия в проектировании программного обеспечения с использованием специализированных программных пакетов.

3. Краткое содержание производственной практики

Разделы (этапы) практики
Подготовительный этап, включающий установочную конференцию (инструктаж по технике безопасности)
ПМ 1. Эксплуатация подсистем безопасности автоматизированных систем
МДК 1.1. Эксплуатация подсистем безопасности автоматизированных систем МДК 1.2. Эксплуатация компьютерных сетей
Производственная практика Виды работ • **эксплуатирование компонентов подсистем безопасности автоматизированных систем;** • **обеспечение работоспособности, обнаружение и устранение неисправности подсистем безопасности автоматизированных систем согласно технической документации;** • **комплектование, конфигурирование, настройка подсистем безопасности автоматизирован**ных систем; • установка, адаптация и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы;
ПМ 2. Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах МДК 2.1. Программно-аппаратные средства обеспечения информационной безопасности МДК 2.2. Криптографические средства и методы защиты информации
Виды работ: • **применение программно-аппаратных средств обеспечения информационной безопасности;** • диагностировать, устранять отказы и обеспечивать работоспособность программно-аппаратных средств обеспечения информационной безопасности; • оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;

⬥ участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; ⬥ решать частные технические задачи, возникающих при аттестации объектов, помещений, программ, алгоритмов; ⬥ использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись; ⬥ применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами;
ПМ.3. Применение инженерно-технических средств обеспечения информационной безопасности МДК 3.1. Применение инженерно-технических средств обеспечения информационной безопасности
Виды работ: ⬥ **применять технические средства защиты информации;** ⬥ **использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;** ⬥ **использовать средства защиты информации от несанкционированного съёма и утечки по техническим каналам;**
ПМ.4. Выполнение работ по рабочей профессии: 161999 Оператор электронно-вычислительных машин МДК.4.1. Технология создания и обработки мультимедийной информации
Производственная практика Виды работ ⬥ Методы обработки фотографий ⬥ Технологии создания и обработки мультимедийной информации
ПМ.5. Сетевые технологии МДК. 5.1. Web-программирование
Производственная практика Виды работ ⬥ Установка и настройка стека TCP/IP. ⬥ Установка сетевого программного обеспечения общего назначения ⬥ Программное обеспечение поиска неисправностей в сетях, анализа и моделирования сетей ⬥ Внедрение удаленного доступа ⬥ Установка и настройка Windows Server 2008 ⬥ Протокола RADIUS ⬥ Сервер сетевых политик (Network Policy Server – NPS) ⬥ Разработка статического сайта ⬥ Разработка динамического сайта
ПМ.6. Участие в интеграции программных модулей МДК.6.1. Технология разработки программного обеспечения МДК.6.2. Инструментальные средства разработки программного продукта
Производственная практика Виды работ: ⬥ Разработка технологической документации; ⬥ Разработка программного продукта с использованием ООП Разработка программного продукта с использованием ООП; ⬥ Автоматизированное тестирование; ⬥ Работа с CASE-средством; ⬥ Организация работ при коллективной разработке программных продуктов

Организация работ при коллективной разработке программных продуктов;

5. Ресурсное обеспечение ОПОП

Ресурсное обеспечение ОПОП вуза формируется на основе требований к условиям реализации основных образовательных программ, определяемых ФГОС СПО по данному направлению подготовки **090000 Информационная безопасность** по специальности **090305 Информационная безопасность автоматизированных систем**, утвержденного приказом Министерства образования и науки Российской Федерации №708 от 24.06.2010 г.

Реализация образовательной программы обеспечивается **научно-педагогическими кадрами**, имеющими, как правило, базовое образование, соответствующее профилю преподаваемой дисциплины, и систематически занимающимися научной и научно-методической деятельностью.

Из числа работающих преподавателей имеют стаж более 20 лет -40%, более 10 лет - 54%. Таким образом, имеется возможность замены имеющих ученую степень специалистов преподавателями, имеющими стаж практической работы по данному направлению на должностях руководителей или ведущих специалистов более 10 лет.

Основная образовательная программа **обеспечивается учебно-методической документацией и материалами** по всем учебным дисциплинам, профессиональным модулям основной образовательной программы. Содержание каждой из таких учебных дисциплин и модулей представляется в сети Интернет и локальной сети института. Весь компьютерный парк института соответствует современным требованиям.

Внеаудиторная работа обучающихся сопровождается методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение.

Библиотечный фонд укомплектован печатными и электронными изданиями основной учебной литературы по дисциплинам базовой части всех циклов, изданными за последние 10 лет, из расчета не менее 25 экземпляров таких изданий на каждые 100 обучающихся.

Фонд дополнительной литературы помимо учебной включает официальные, справочно-библиографические и специализированные периодические издания в расчете 1-2 экземпляра на каждые 100 обучающихся.

Каждый обучающийся обеспечен доступом к электронно-библиотечной системе, содержащей издания по основным изучаемым дисциплинам и сформированной по согласованию с правообладателями учебной и учебно-методической литературы.

При этом обеспечена возможность осуществления одновременного индивидуального доступа к такой системе не менее чем для 25% обучающихся.

Электронно-библиотечная система обеспечивает возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет.

Оперативный обмен информацией с отечественными и зарубежными вузами и организации осуществляется с соблюдением требований законодательства Российской Федерации об интеллектуальной собственности и международных договоров Российской Федерации в области интеллектуальной собственности. Для обучающихся обеспечивается доступ к современным профессиональным базам данных, информационным справочным и поисковым системам.

Технологический институт, реализующий образовательную программу прикладного бакалавриата располагает **материально-технической базой**, обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, практической и научно-исследовательской работы обучающихся, предусмотренных учебным планом вуза и соответствующей действующим санитарным и противопожарным правилам и нормам. Образовательный процесс обеспечивается необходимым комплектом лицензионного программного обеспечения, также лабораторным оборудованием и базой

лабораторий кафедры: лаборатории разработки информационных технологий, лаборатории технических средств информатизации, лаборатории программирования.

6. Характеристики среды учебного заведения, обеспечивающие развитие общекультурных (социально-личностных) компетенций выпускников.

Для развития общекультурных (социально-личностных) компетенций выпускников университет создает социокультурную среду, условия, необходимые для всестороннего развития и социализации личности, сохранения здоровья обучающихся, способствует развитию воспитательного компонента образовательного процесса, включая развитие студенческого самоуправления, участие обучающихся в работе общественных организаций, спортивных и творческих клубов, научных кружков:

- в культурном центре «Сергеляхские огни» работают 22 студий;
- в спортивном комплексе «Юность» работают 16 секций;
- в Технологическом институте работают**:**

✓ **Спортивные секции** по волейболу, баскетболу, футболу, кикбоксингу**,** вольной борьбе, легкой атлетике;

✓ **творческие клубы:** Театральная студия, КВН, «Студия национального шитья и народных промыслов», «Вокально – инструментальная группа», «Брейк – данс»;

✓ **научные кружки:** «Создание различных баз данных»; «Создание различных программных средств»; «Проектирование средств и установок для технического обслуживания компьютерных сетей»; «Создание программных средств»; «Создание различных информационных ресурсов»; «Создание цифровых образовательных устройств»; «Разработка интеллектуальных игр и виртуальных приложений»; «Создание электронных образовательных средств»; «Некоторые методы защиты информации»; «Создание комплекта для дошкольников на якутском языке»; «Защита и мониторинг ЛВС»; «Создание робота - IT»; «Администрирование серверов»; «Техническое обслуживание средств ВТ»; «Программирование на различных языках» и др.

Также используются в целях реализации компетентностного подхода в образовательном процессе активные и интерактивные формы проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций, психологических и иных тренингов, групповых дискуссий) в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся.

Обучающиеся имеют следующие права и обязанности:

при формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения (в том: числе и в других образовательных учреждениях), который освобождает обучающегося от необходимости их повторного освоения;

в целях воспитания и развития личности, достижения результатов при освоении основной профессиональной образовательной программы в части развития общих компетенций обучающиеся могут участвовать в развитии студенческого самоуправления, работе общественных организаций, спортивных и творческих клубов;

общающиеся обязаны выполнять в установленные сроки все задания, предусмотренные основной профессиональной образовательной программой;

обучающимся должна быть предоставлена возможность оценивания содержания, организации и качества образовательного процесса.

7. Нормативно-методическое обеспечение системы оценки качества освоения обучающимися ООП

7.1. Текущий контроль успеваемости и промежуточная аттестация.

Текущий контроль успеваемости проводится с целью проверки хода и качества усвоения учебного материала, стимулирования учебной работы студентов и

совершенствования методики проведения занятий.

Текущий контроль освоения студентами программного материала учебных дисциплин и междисциплинарных курсов может иметь следующие ***виды***: ***входной, оперативный и рубежный контроль.***

Входной контроль знаний студентов проводится в начале изучения дисциплины, междисциплинарного курса с целью выстраивания индивидуальной траектории обучения студентов.

Оперативный контроль проводится с целью объективной оценки качества освоения программ дисциплин, междисциплинарных курсов, профессиональных модулей, а также стимулирования учебной работы студентов, мониторинга результатов образовательной деятельности (мониторинга уровня освоения содержания дисциплин, уровня сформированности общих и профессиональных компетенций), подготовки к промежуточной аттестации и обеспечения максимальной эффективности учебно-воспитательного процесса.

Оперативный контроль проводится преподавателем на любом из видов учебных занятий. Формы оперативного контроля (контрольная работа, тестирование, опрос, выполнение и защита практических и лабораторных работ, выполнение отдельных разделов курсового проекта (работы), выполнение рефератов (докладов), подготовка презентаций и т.д.) выбираются преподавателем исходя из методической целесообразности, специфики учебной дисциплины, междисциплинарного курса.

Рубежный контроль является контрольной точкой по завершению каждой раздела учебной дисциплины или междисциплинарного курса и проводится с целью комплексной оценки уровня освоения программного материала.

Оценка знаний, умений студентов в ходе текущего контроля осуществляется на основе **рейтинговой системы**. Принципы и технология рейтинговой системы закрепляются соответствующим локальным актом института.

Оценка уровня сформированности общих и профессиональных компетенций студентов в ходе текущего контроля осуществляется на основе оценочных, оценочно - диагностирующих средств. Принципы и технология мониторинга сформированности компетенций закрепляются соответствующим локальным актом.

˜организация консультаций:

консультации предусмотрены в объеме 100 часов на учебную группу на каждый учебный год. Формы – групповые и индивидуальные, устные;

˜порядок проведения учебной и производственной практики:

Учебная практика и производственная практика (по профилю специальности) проводятся при освоении студентами профессиональных компетенций в рамках профессиональных модулей и реализуются концентрированно в несколько периодов.

Аттестацию по итогам практики выполняет руководитель практики на основании отзыва руководителя от организации (предприятия, НИИ, фирмы) и отчета о выполненной работе по форме, устанавливаемой Институтом. Аттестация проводится по окончании профессионального модуля в виде защиты отчета перед комиссией, в состав которой входят: заведующий кафедрой, руководители практики от предприятия и института, также преподаватели МДК профессиональных модулей.

Преддипломная практика является завершающим этапом обучения студентов и проводится для овладения ими первоначальным профессиональным опытом, проверки готовности будущего техника к самостоятельной профессиональной деятельности, сбора и обобщения материалов к выпускной квалификационной работе. Продолжительность преддипломной практики – 4 недели.

Промежуточная аттестация проводится с целью определения соответствия уровня и качества подготовки техников - программистов требованиям к результатам освоения основной профессиональной образовательной программы и осуществляется в двух основных направлениях:

- оценка уровня сформированности общих и профессиональных компетенций обучающихся.
- Для юношей предусматривается оценка результатов освоения основ военной службы.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям ОПОП создаются фонды оценочных средств, которые предварительно одобряет работодатель.

Основными видами промежуточной аттестации являются:

1. с учетом времени на промежуточную аттестацию:

1. экзамен по дисциплине;
2. экзамен по междисциплинарному курсу;
3. квалификационный экзамен по профессиональному модулю;

2. без учета времени на промежуточную аттестацию:

1. зачет по дисциплине;
2. зачет по междисциплинарному курсу;
3. зачет по учебной, производственной практике.

При освоении проведение экзаменов или зачетов по данному междисциплинарному курсу в каждом из семестров;

проведение в семестрах, предшествующих последнему семестру изучения, зачета по междисциплинарному курсу.

Промежуточная аттестация по каждому профессиональному модулю осуществляется в форме квалификационного экзамена, который носит комплексный характер.

Промежуточная аттестация по учебной, производственной практике в рамках освоения программ профессиональных модулей осуществляется в форме зачета.

Основными формами аттестационных испытаний для выявления уровня освоенности содержания учебных дисциплин являются: устная, письменная и смешанная формы.

Основными формами аттестационных испытаний по МДК, профессиональным модулям являются: устная, письменная и смешанная формы, для выявления уровня сформированности компетенций является комплексное экспертное испытание (с практическими задачами профессионального характера).

В качестве внешних экспертов будут привлекаться работодатели, преподаватели, читающие смежные дисциплины.

Структура фондов оценочных средств:

1. Задания для оценки освоения МДК;
2. Оценочные средства по учебной и (или) производственной практике;
3. Оценочные средства для оценки освоения профессиональных модулей на квалификационном экзамене.

7.2. Итоговая государственная аттестация выпускников ООП

Целью итоговой государственной аттестации является установление уровня подготовки выпускников к выполнению профессиональных задач и соответствия их подготовки требованиям государственных образовательных стандартов СПО.

В соответствии с ФГОС итоговая государственная аттестация выпускников по специальности среднего профессионального образования 090305 Информационная безопасность автоматизированных систем укрупненной группы направлений подготовки и специальностей 090000 Информационная безопасность, является обязательной, и завершается присваиванием квалификации техника - программиста с выдачей **диплома.**

Итоговая государственная аттестация осуществляется государственной аттестационной комиссией (ГАК), организуемой по основной профессиональной образовательной программе и утвержденной в установленном порядке.

Основные функции государственной аттестационной комиссии: комплексная

оценка уровня профессиональной подготовки, уровня сформированности общих и профессиональных компетенций выпускника и соответствие его подготовки требованиям ФГОС СПО решение вопроса о присвоении квалификации по результатам итоговой аттестации и выдаче выпускнику соответствующего диплома, разработка рекомендаций по совершенствованию подготовки выпускников на основании результатов работы.

Итоговая государственная аттестация предусматривает подготовку и защиту выпускной квалификационной работы (дипломная работа, дипломный проект) для установления уровня теоретической подготовленности и сформированности общих и профессиональных компетенций выпускника к решению профессиональных задач. Обязательное требование – соответствие тематики выпускной квалификационной работы содержанию одного или нескольких профессиональных модулей.

Итоговая государственная аттестация выпускника в нашем ОУ состоит из одного вида испытания: **защиты выпускной квалификационной работы**.

К защите выпускных квалификационных работ допускаются лица, завершившие полный курс обучения по основной профессиональной образовательной программе по специальности среднего профессионального образования 090305 Информационная безопасность автоматизированных систем укрупненной группы направлений подготовки и специальностей 090000 Информационная безопасность и успешно прошедшие все предшествующие аттестационные испытания, предусмотренные учебным планом. Допуск к защите выпускных квалификационных работ проводится на основании следующих документов:

- заверенная справка о выполнении выпускником учебного плана (учебная карточка) с указанием среднего балла успеваемости;
- документ о соответствии уровня сформированности общих и профессиональных компетенций выпускника требованиям к результатам освоения основной образовательной программы;
- карта успешности студента (карта личных достижений студента) с копиями дипломов, сертификатов о достигнутых результатах на олимпиадах, конкурсах, выставках, научно – практических конференциях, о выполнении творческих работ по специальности;
- характеристики с мест прохождения практик;
- зачетная книжка студента;
- отзыв руководителя;
- рецензия на выпускную квалификационную работу (представляются в сроки, установленные решением Ученого совета) – при защите ВКР;
- в ГАК могут быть представлены также другие материалы, характеризующие научную и практическую ценность выпускной квалификационной работы, статьи по теме проекта (работы), и документы о практическом применении проекта (работы).

Выпускная квалификационная работа представляет собой законченную разработку, в которой на основе профессионально ориентированной теоретической подготовки и сформированности общих и профессиональных компетенций выпускника решаются конкретные практические задачи, предусмотренные квалификацией и профессиональным (в том числе должностным) предназначением выпускника в соответствии с ФГОС СПО.

Секретарь ГАК перед началом заседания получает книгу протоколов и личные дела студентов.

Защита выпускных квалификационных работ проводится на заседании государственной аттестационной комиссии соответственно с участием не менее двух третей ее состава. Решение комиссии принимается на закрытом заседании простым большинством голосов членов комиссии, участвующих в заседании. При равном числе голосов голос председателя является решающим.

Кроме членов аттестационной комиссии на защите будут присутствовать научный руководитель и рецензент выпускной квалификационной работы, а также возможно присутствие студентов и преподавателей. Отзывы научного руководителя и рецензента, представленные в ГАК, должны быть оформлены в соответствии с требованиями, указанными в "Методических рекомендациях по разработке и защите выпускных квалификационных работ".

Перед началом защиты председатель ГАК знакомит студентов с порядком проведения защиты, а секретарь комиссии дает краткую информацию по личному делу студента.

Защита ВКР прикладного бакалавра начинается с доклада студента по теме выпускной квалификационной работы. Продолжительность защиты ВКР не должна превышать 30 минут. На доклад по ВКР отводится до 15 минут. Студент должен излагать основное содержание своей выпускной квалификационной работы свободно.

После завершения доклада члены ГАК задают студенту вопросы как непосредственно связанные с темой ВКР, так и близко к ней относящиеся. При ответах на вопросы студент имеет право пользоваться своей работой.

После ответов студента на вопросы слово предоставляется научному руководителю. В конце своего выступления научный руководитель дает свою оценку выпускной квалификационной работе, которая отражена в отзыве.

После выступления научного руководителя слово предоставляется рецензенту. В конце своего выступления рецензент дает свою оценку работе. После окончания дискуссии студенту предоставляется заключительное слово. В своем заключительном слове студент должен ответить на замечания рецензента.

Результаты итоговой государственной аттестации, определяются оценками "отлично", "хорошо" "удовлетворительно", "неудовлетворительно" и объявляются после оформления в установленном порядке протокола заседания ГАК.

8. Другие нормативно-методические документы и материалы, обеспечивающие качество подготовки обучающихся.

Положение об учебной и производственной практике студентов (курсантов), осваивающих основные профессиональные образовательные программы среднего профессионального образования, утверждено приказом Минобрнауки России от 26.11.2009 №673. Настоящее Положение определяет правила организации и проведения учебной и производственной практики студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования (далее - ОПОП СПО).

Настоящее Положение определяет правила организации и проведения учебной и производственной практики студентов (курсантов) (далее - студенты), осваивающих основные профессиональные образовательные программы среднего профессионального образования (далее - ОПОП СПО).

1. Видами практики студентов, осваивающих ОПОП СЛО, являются: учебная практика и производственная практика.
2. Учебная и производственная практики студентов являются составной частью ОПОП СПО, обеспечивающей реализацию федерального государственного образовательного стандарта среднего профессионального образования (далее - ФГОС СПО).
3. Учебная и производственная практики имеют целью комплексное освоение студентами всех видов профессиональной деятельности по специальности СПО, формирование общих и профессиональных компетенций, а также приобретение необходимых умений и опыта практической работы студентов по специальности.
4. Учебная практика направлена на формирование у студентов практических профессиональных умений, приобретение первоначального практического опыта, реализуется в рамках профессиональных модулей ОПОП СПО по основным видам

профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по избранной специальности.

5. Учебная практика может быть направлена на освоение рабочей профессии, если это является одним из видов профессиональной деятельности в соответствии с ФГОС СПО по специальности. В этом случае студент может получить квалификацию по рабочей профессии.
6. Производственная практика включает в себя следующие этапы: практика по профилю специальности и преддипломная практика. Практика по профилю специальности направлена на формирование у студента общих компетенций, а также профессиональных компетенций, приобретение практического опыта и реализуется в рамках профессиональных модулей ОПОП СПО по каждому из видов профессиональной деятельности, предусмотренных ФГОС СПО по специальности.

   Преддипломная практика направлена на углубление студентом первоначального профессионального опыта, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы (дипломного проекта или дипломной работы) в организациях различных организационно-правовых форм (далее - организация).
7. Содержание учебной и производственной практики определяется требованиями к результатам обучения по каждому из профессиональных модулей в соответствии с ФГОС СПО, профессиональных модулей, разрабатываемыми и утверждаемыми образовательным учреждением самостоятельно.
8. Учебная практика проводится, как правило, в учебных, учебно-производственных мастерских, лабораториях, учебных хозяйствах, учебно-опытных участках, полигонах, бизнес- инкубаторах, ресурсных центрах и других вспомогательных объектах образовательного учреждения.

   Учебная практика может также проводиться в организациях в специально-оборудованных помещениях на основе прямых договоров между организацией и образовательным учреждением.
9. Производственная практика проводится, как правило, в организациях на основе прямых договоров, заключаемых между образовательным учреждением и каждой организацией, куда направляются студенты.
10. Производственная практика студентов образовательных учреждений, реализующих ОПОП СПО, может проводиться как на возмездной, так и на безвозмездной основе в соответствии с договором между образовательным учреждением и организацией.

    Во время преддипломной практики при наличии вакантных штатных должностей студенты могут зачисляться на них, если работа соответствует требованиям программы преддипломной практики.
11. Сроки проведения учебной и производственной практики устанавливаются образовательным учреждением в соответствии с особенностями ОПОП СПО, возможностями учебно-производственной базы образовательных учреждений, условиями договоров с организациями.
12. Учебная практика и практика по профилю специальности проводятся как непрерывно, так и путем чередования с теоретическими занятиями по дням (неделям) при условии обеспечения связи между содержанием учебной практики и результатами обучения в рамках профессиональных модулей ОПОП СПО по видам профессиональной деятельности.
13. Преддипломная практика проводится непрерывно после освоения учебной практики и практики по профилю специальности.

12. В организации и проведении практик участвуют:

- образовательные учреждения, реализующие ОПОП СПО;
- организации.

13. Образовательные учреждения;
    - планируют и утверждают в учебном плане все виды практики в соответствии с ОПОП СПО, с учетом договоров с организациями;
    - заключают договоры на организацию и проведение практики;
    - разрабатывают и согласовывают с организациями программу, содержание и планируемые результаты практики;
    - осуществляют руководство практикой;
    - контролируют реализацию программы и условии проведения практики организациями, в том числе требования охраны труда, безопасности жизнедеятельности и пожарной безопасности в соответствии с правилами и нормами, в том числе отраслевыми;
    - формируют группы в случае применения групповых форм проведения практики;
    - организовывают процедуру оценки общих и профессиональных компетенций студентов, освоенных ими в ходе прохождения практики;
    - разрабатывают и согласовывают с организациями формы отчетности и оценочный материал прохождения практики.
14. Организации, участвующие в организации и проведении практики:
    - заключают договора на организацию и проведение практики;
    - согласовывают программу практики, планируемые результаты практики, задание на практику;
    - предоставляют " рабочие места практикантам, назначают руководителей практики от организации, определяют наставников;
    - участвуют в организации и оценке результатов освоения профессиональных компетенций, полученных в период прохождения практики;
    - участвуют в формировании оценочного материала для оценки профессиональных компетенций, освоенных студентами в ходе прохождения практики;
    - обеспечивают безопасные условия прохождения практики студентами;
    - проводят инструктаж студентов по ознакомлению с требованиями охраны труда и техники безопасности в организации.
15. Студенты, осваивающие ОПОП СПО при прохождении практики в организациях:
    - полностью выполняют задания, предусмотренные программами практик;
    - соблюдают действующие в организациях правила внутреннего трудового распорядка;
    - строго соблюдают требования охраны труда и правила пожарной безопасности;
    - получают документы (свидетельства о квалификации, сертификаты и т.д.), содержащие и подтверждающие оценку общих и профессиональных компетенций, полученную ими в период прохождения учебной и производственной практик.
16. Учебная практика, как правило, проводится мастерами производственного обучения и (или) преподавателями дисциплин профессионального цикла. Учебная нагрузка мастеров производственного обучения, преподавателей и специалистов определяется, исходя из количества учебных часов, предусмотренных учебным планом.
17. Организацию и руководство практикой по профилю специальности и преддипломной практикой осуществляют руководители практики от образовательного учреждения и от организации.

18. Оплата труда студентов в период учебной и производственной практики при выполнении ими производительного труда осуществляется в порядке, предусмотренном законодательством Российской Федерации для организаций соответствующей отрасли, а также в соответствии с договорами, заключаемыми образовательными учреждениями с организациями, в том числе на условиях целевой контрактной подготовки или взаимовыгодного сотрудничества между образовательным учреждением и организацией.
19. Студенты за период прохождения учебной и всех этапов производственной практики, связанной с выездом из места нахождения образовательного учреждения, образовательным учреждением выплачиваются суточные в размере 50% от нормы суточных, установленных законодательством Российской Федерации для возмещения дополнительных расходов, связанных с командировками работников организаций за каждый день, включая время нахождения в пути к месту практики и обратно. Проезд к месту практики и обратно оплачивается в полном размере.
20. С момента зачисления студентов в период практики на вакантные штатные места, па них распространяются требования охраны труда и правила внутреннего распорядка, действующие в организации, а также трудовое законодательство Российской Федерации, в том числе в части государственного социального страхования.
21. Результаты учебной и производственной практики определяются программами практик, разрабатываемыми образовательным учреждением совместно с организациями.
22. Аттестация по итогам производственной практики проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций.
23. Учебная и производственная практика завершаются оценкой и/или зачетом студентами освоенных общих и профессиональных компетенций.

Если ФГОС СПО в рамках одного из видов профессиональной деятельности предусмотрено освоение рабочей профессии, то по результатам освоения профессионального модуля, который включает в себя учебную практику, студенты получают документ (свидетельство) об уровне квалификации. Присвоение квалификации по рабочей профессия должно проводиться с участием работодателей и при необходимости соответствующих органов государственного надзора и контроля. Документы с результатами по учебной практике и всем этапам производственной практики (свидетельства о квалификации, сертификаты, выполненные задания, отчеты и т.д.) представляются студентом и учитываются при государственной (итоговой) аттестации.

Федеральные органы исполнительной власти, имеющие в своем ведении образовательные учреждения СПО, могут разрабатывать на основании настоящего Положения рекомендации по организации и проведению учебной и производственной практики студентов, осваивающих ОПОП СПО с учетом особенностей отрасли.

117

Приложение 2

Аннотация
к рабочей программе дисциплины
Математика

Направление подготовки	090305 Информационная безопасность автоматизированных систем
Профиль подготовки	Базовый
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	ЕН.00 Математический и общий естественнонаучный цикл ЕН.01 Математика
Семестр(ы) изучения	1,2
Количество зачетных единиц (кредитов)	
Форма промежуточной аттестации (зачет/экзамен)	Зачет/Экзамен
Количество часов всего, из них:	*180*
лекционные	86
практические	34
семинары	-
СРС	60
на контрольную работу/зачет	8/9

1. Цели освоения дисциплины

Целями изучения дисциплины Математика являются:

- воспитание достаточно высокой математической культуры;
- привитие навыков современных видов математического мышления;
- обеспечение математической базы, необходимой для успешного усвоения студентами знаний по другим дисциплинам.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины.

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Быть готовым к смене технологий в профессиональной деятельности.

ОК 11. Формулировать задачи логического характера и применять средства математической логики для их решения.

ПК 1.1. 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.

ПК 1.2. Выполнять работы по администрированию подсистем безопасности автоматизированных систем.

ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.

ПК 2.2. 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.

ПК 2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.

В результате освоения дисциплины обучающийся должен:

Знать:

- основы линейной алгебры и аналитической геометрии;
- основные положения теории множеств;
- основные понятия и методы дифференциального и интегрального исчисления;
- основные понятия и методы теории вероятностей и математической статистики;
- логические операции, законы и функции алгебры логики

Уметь:

- выполнять операции над матрицами и решать системы линейных уравнений;
- выполнять операции над множествами;
- применять методы дифференциального и интегрального исчисления:
- использовать основные положения теории вероятностей и математической статистики;
- применять стандартные методы и модели к решению типовых вероятностных и статистических задач;

3. Краткое содержание дисциплины

Раздел 1. Элементы линейной алгебры

Тема 1.1.Матрицы. Основные понятия. Операции над матрицами.

Тема 1.2. Определители. Понятие определителя. Свойства определителей.

Тема 1.3. Невырожденные матрицы. Обратная матрица. Ранг матрицы.

Тема 1.4. Решение систем линейных уравнений. Основные понятия. Формулы Крамера. Метод Гаусса.

Раздел II. Элементы аналитической геометрии

Тема 2.1.Прямая на плоскости. Основные понятия. Уравнение прямой на плоскости.

Тема 2.2. Кривые второго порядка. Окружность. Эллипс. Гипербола. Парабола.

Раздел 3. Основы математического анализа

Тема 3.1. Функция. Предел функции. Понятие функции. Числовые функции. Способы задания функций. Обратная функция. Сложная функция. Функции и их графики. Предел функции, операции над пределами функции. Виды пределов.

Тема 3.2. Производная функции. Геометрический и физический смысл производной. Производная сложной и обратной функций. Производные основных элементарных функций. Исследование и построение графика функции .

Тема 3.3. Неопределенный интеграл. Определенный интеграл. Первообразная функции, основные понятия. Свойства неопределенного интеграла. Интегралы основных элементарных функций. Основные понятия и свойства определенного интеграла.

Формула Ньютона-Лейбница

Тема 3.4. Дифференциальные уравнения. Основные понятия и определения. Дифференциальные уравнения первого порядка. Уравнения второго порядка, допускающие понижение порядка.

Раздел 4. Теория множеств

Тема 4.1. Множества. Операции над множествами; Диаграммы Венна; Прямое произведение множеств; Подмножества; Мультимножества.

Раздел 5. Основы математической логики.

Основные понятия логики высказываний. Таблицы истинности.

Раздел 6. Элементы теории вероятности и математической статистики.

Тема 6.1. Формулы перестановок, размещений и сочетаний. Основные формулы комбинаторики.

Тема 6.2.Вероятность события. Случайные события. Алгебра событий. Классическое и статистическое определения вероятностей события.

Тема 6.3. Математическое ожидание и дисперсия случайной дискретной величины. Математическое ожидание и его. Дисперсия и её свойства.

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению 090305 Информационная безопасность автоматизированных систем

2. Аннотация к РПД утверждена на заседании кафедры (протокол №___ от «__»____20_г.)

Аннотация
к рабочей программе дисциплины
Физика

Направление подготовки	230000 Информатика и вычислительная техника
Профиль подготовки	090305 Информационная безопасность автоматизированных систем
Квалификация (степень) выпускника	Техник
Цикл, раздел учебного плана	ЕН.3 Математический и общий естественнонаучный цикл.
Семестр (ы) изучения	2-3 семестр
Количество зачетных единиц (кредитов)	3
Форма промежуточной аттестации (зачет/экзамен)	Контрольная работа
Количество часов всего, из них:	144
Лекционные	56
Практические	40
семинары	-
СРС	48
на экзамен/зачет	Контрольная работа

1. Цели освоения дисциплины Формировать общекультурные и профессиональные компетенции старший техник по безопасности информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате освоения дисциплины обучающийся должен:

1.Знать:

фундаментальные законы природы и основные физические законы в области механики, термодинамики, электричества и магнетизма, атомной физики;

устройства и принцип действия полупроводниковых приборов

понятийный аппарат физики в объеме данного курса,

современную физическую картину мира.

2. уметь:

использовать физическое моделирование, законы физики для объяснения механизмов природных явлений и процессов,

читать и переводить графическую информацию,

3.Владеть:

переводом графической информации

обрабатыванием полученных результатов

применением физических законов для решения практических задач

3. Краткое содержание дисциплины Программа учебной дисциплины является частью примерной основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО.

Программа учебной дисциплины может быть использована техник по защите информации, в которой включены следующие разделы:

Раздел 1. Физические основы механики

Раздел 2. Молекулярная физика и термодинамика.

Раздел 3. Электричество и магнетизм.

Раздел 4. Колебания и волны.

Раздел 5 . Оптика. Квантовая физика.

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению ; 230000 Информатика и вычислительная техника

2. ООП СПО по направлению: 090305 Информационная безопасность автоматизированных систем

3. Аннотация к РПД утверждена на заседании кафедры (протокол №___ от «__»____20_г.)

Аннотация
к рабочей программе дисциплины
«Основы информационной безопасности»

Направление подготовки	230000 Информатика и вычислительная техника
Специальность:	090305 ***Информационная безопасность автоматизированных систем***
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	П. Профессиональный цикл ОП. Общепрофессиональные дисциплины ОП.1 Основы информационной безопасности
Семестр(ы) изучения	1
Количество зачетных единиц (кредитов)	-
Форма промежуточной аттестации (зачет/экзамен)	Дифференциальный зачет
Количество часов всего, из них:	
лекционные	40

лабораторные	20
семинары	
СРС	30
на экзамен/зачет	

1. Цели освоения дисциплины

1. Основная образовательная ***цель*** дисциплины ОП.1 **Основы информационной безопасности:**

создать у студента фундамент знаний и умений по информационной безопасности, который способен в дальнейшем обеспечить успешное применение методов и средств в процессе освоения дисциплин специальности, а также в профессиональной деятельности по специальности.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате изучения обязательной части цикла общепрофессиональных дисциплин обучающийся должен**:**

1.1. уметь:

1.1.1. классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

1.1.2. применять основные правила и документы системы сертификации Российской Федерации;

1.1.3. классифицировать основные угрозы безопасности информации;

1.2. знать:

1.2.1. сущность и понятие информационной безопасности, характеристику ее составляющих;

1.2.2. место информационной безопасности в системе национальной безопасности страны;

1.2.3. источники угроз информационной безопасности и меры по их предотвращению;

1.2.4. жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;

1.2.5. современные средства и способы обеспечения информационной безопасности

Дисциплина «Основы информационной безопасности» имеет своей целью формировать у обучающихся общие компетенции (ОК-5, ОК-8, ОК-9, ОК-10) и профессиональные компетенции (ПК-2.6., ПК-3.3., ПК-3.5.), в соответствии с требованиями ФГОС СПО по направлению подготовки 090000 Информационная безопасность по специальности 090305 *Информационная безопасность автоматизированных систем* (квалификация: техник – по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

Должны быть сформированы следующие компетенции:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

ПК.2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

Краткое содержание дисциплины

Дисциплина «Методы и средства защиты информации» состоит из следующих разделов:

1. Введение. *Информационные системы*

2. Информационная безопасность

Тема 2.1. *Современная ситуация в области информационной безопасности*

Тема 2.2. *Основные виды и источники атак на информацию*

Тема 2.3. *Угроза безопасности информации*

Тема 2.4. *Факторы угроз безопасности информации*

Тема 2.5. *Критерии и нормы безопасности информации*

Тема 2.6. *Категории информационной безопасности*

Тема 2.7. *Жизненные циклы конфиденциальной информации*

3. Современные средства и способы обеспечения информационной безопасности

Тема 3.1. *Абстрактные модели защиты информации*

Тема 3.2. *Наиболее распространенные методы взлома*

Тема 3.3. *Средства и способы обеспечения информационной безопасности*

4. Нормативно- правовое обеспечение информационной безопасности

Тема 4.1. *Основные правила и документы системы сертификации РФ*

Тема 4.2. *Нормативно- правовое обеспечение информационной безопасности программно-аппаратными средствами*

Тема 4.3. *Нормативно-правовое обеспечение информационной безопасности инженерно-техническими средствами*

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению 090000 Информационная безопасность по специальности 090305 *Информационная безопасность автоматизированных систем* (квалификация: техник – по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

2. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от «01» сентября 2011 г.)

Аннотация
к рабочей программе дисциплины
Организационно - правовое обеспечение информационной безопасности

Направление подготовки	**090000 Информационная безопасность**
Специальность:	090305 ***Информационная безопасность автоматизированных систем***
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	П. Профессиональный цикл ОП. Общепрофессиональные дисциплины ОП.3. **Организационно - правовое обеспечение информационной безопасности**
Семестр(ы) изучения	5
Количество зачетных единиц (кредитов)	-
Форма промежуточной аттестации (зачет/экзамен)	Экзамен
Количество часов всего, из них:	
лекционные	30
лабораторные	10
семинары	
СРС	3
на экзамен/зачет	

1. Цели освоения дисциплины

2. Основная образовательная ***цель*** дисциплины ОП.3. **Организационно - правовое обеспечение информационной безопасности:**

создать у студента фундамент знаний и умений по организационно - правовому обеспечению информационной безопасности, который способен в дальнейшем обеспечить успешное применение в процессе освоения дисциплин специальности, а также в профессиональной деятельности по специальности.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате изучения обязательной части цикла общепрофессиональных дисциплин обучающийся должен**:**

В результате освоения дисциплины обучающийся должен:

2.1. уметь:

2.1.1. осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации;

2.1.2. применять нормативные правовые акты и методические документы в области защиты информации

2.1.3. выявлять каналы утечки информации на защиты;

2.1.4. контролировать соблюдение персоналом требований режима защиты информации;

2.1.5. оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;

2.1.6. защищать свои права в соответствии с трудовым законодательством;

2.2. **знать:**

2.2.1. 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;

2.2.2. правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

2.2.3. правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны **и** сертификации средств защиты информации;

2.2.4. организацию ремонтного обслуживания аппаратуры и средств защиты информации;

2.2.5. принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;

2.2.6. правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность)

Дисциплина «**Организационно - правовое обеспечение информационной безопасности»** имеет своей целью формировать у обучающихся общие компетенции (ОК-5, ОК-8, ОК-9, ОК-10) и профессиональные компетенции (ПК-2.6., ПК-3.3., ПК-3.5.), в соответствии с требованиями ФГОС СПО по направлению подготовки **090000 Информационная безопасность** по специальности **090305** ***Информационная безопасность автоматизированных систем*** (квалификация: техник по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

Должны быть сформированы следующие **компетенции**:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

ОК 13. Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах.

ПК 1.4. Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.

ПК 1.5. Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.

ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

ПК.2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

Краткое содержание дисциплины

Дисциплина «**Организационно - правовое обеспечение информационной безопасности»** состоит из следующих разделов:

1. Организационно-правовое обеспечение информационной безопасности

Тема 1.1. *Информационное право*

Тема 1.2. *Правовая защита информации*

2. Законодательство в области интеллектуальной собственности

Тема 2.1. *Интеллектуальная собственность в России*

Тема 2.2. *Охрана конфиденциальной информации*

Тема 2.3. *Органы и защита исключительных прав владельцев объектов информационных систем*

3. Правовая защита программ и информационных технологий

Тема 3.1. *Правовая защита программ и информационных технологий*

Тема 3.2. *Федеральные законы по охране программ и информационных технологий*

4. Мероприятия по охране труда и технике безопасности

Тема 4.1. *Организационные мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них*

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению **090000 Информационная безопасность** по специальности 090305 ***Информационная безопасность автоматизированных систем*** (квалификация: техник – по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

2. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от «01» сентября 2011 г.

Аннотация
к рабочей программе дисциплины
ОП.04 Сети и системы передачи информации

Направление подготовки	**210700 Информационная Безопасность**
Специальность:	**090305. Информационная безопасность автоматизированных систем**
Профиль подготовки	
Квалификация (степень) выпускника	**техник по защите информации**
Цикл, раздел учебного плана	П.00 Профессиональный цикл ПМ.5 Сетевые технологии ОП.2 Технические средства информатизации
Семестр(ы) изучения	*I*
Количество зачетных единиц (кредитов)	*102*
Форма промежуточной аттестации (зачет/экзамен)	*зачет*
Количество часов всего, из них:	*68*
лекционные	*48*
практические	*20*

семинары	
СРС	*34*
на экзамен/зачет	

1. Цели освоения дисциплины

Целью курса сформировать базовое представление, первичные знания, умения и навыки студентов по основам компьютерным сетям как научной фундаментальной и прикладной дисциплины, достаточные для дальнейшего продолжения образования и самообразования их в области вычислительной техники, информационных систем различного назначения и в смежных областях.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля).

ПК 1.1. 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.

ПК 1.3. Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.

ПК 1.4. Участвовать в разработке проекта производства работ с применением информационных технологий.

ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый к ней интерес.

ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.

ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Быть готовым к смене технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

В результате освоения дисциплины обучающийся должен:

1. Знать

- Применять полученные знания при решении практических задач защиты информации в системах и сетях связи;
- Организовывать предпроектные исследования по построению системы защиты информации в сетях связи.

2. Уметь

- Использовать средства ОС и сред для решения практических задач;
- Использовать сервисные средства, поставляемые с ОС;
- Устанавливать различные ОС;
- Подключать к ОС новые сервисные средства;
- Решать задачи обеспечения защиты ОС.

3. Краткое содержание дисциплины

Введение

Архитектура информационных сетей

Стандарты в области телекоммуникаций

Тенденции развития телекоммуникационных систем и сетей

Преобразование аналоговых сообщений в цифровую форму

Методы мультиплексирования и демультиплексирования

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению 230113·51 Компьютерные системы и комплексы *по направлению 230000 Информатика и вычислительная техника*
2. ООП СПО по направлению230113·51 Компьютерные системы и комплексы *по направлению 230000 Информатика и вычислительная техника*
3. Аннотация к РПД утверждена на заседании кафедры (протокол №1 от «1» 2011 года)

Аннотация
к рабочей программе дисциплины
ОП.5. Основы алгоритмизации и программирования

Направление подготовки	090000 Информационная безопасность
Профиль подготовки	090305 Информационная безопасность автоматизированных систем
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	ОП.00. Общепрофессиональный цикл вариативная часть. ОП.05. Основы алгоритмизации и программирования
Семестр(ы) изучения	1, 2, 3
Количество зачетных единиц (кредитов)	
Форма промежуточной аттестации (зачет/экзамен)	Квалификационный экзамен
Количество часов всего, из них:	304
лекционные	102
лабораторные	78
Курсовая работа	
семинары	
СРС	124
Учебная практика	
Производственная практика	
на экзамен/зачет	

1. Цели освоения модуля

Целями освоения дисциплины «Основы алгоритмизации и программирования» являются: формирование представлений о современном состоянии программирования, языков программирования и сред для разработки программ; совершенствование владения языками программирования высокого уровня и техникой программирования; знакомство с типовыми задачами программирования и методами их решения.

Дисциплина «Основы алгоритмизации и программирования» имеет своей целью формировать у обучающихся общекультурные (ОК-1, ОК–3, ОК-8, ОК-9) и

профессиональные (ПК-5.1, ПК-5.2, ПК-5.1) компетенции в соответствии с требованиями ФГОС СПО по направлению подготовки 090000 Информационная безопасность (квалификация техник по защите информации), утвержденного приказом Министерства образования и науки РФ от 24 июня 2010 г. №708.

2. Компетенции обучающегося, формируемые в результате освоения модуля

В результате освоения модуля обучающийся должен:

Знать:

- основы объектно-ориентированного подхода к программированию;
- технологию разработки алгоритмов и программ, методы отладки и решения задач на ЭВМ в различных режимах.

Уметь:

- ставить задачу и разрабатывать алгоритм ее решения, использовать прикладные системы программирования
- работать с современными системами программирования, включая объектно-ориентированные

Владеть:

- языками процедурного и объектно-ориентированного программирования,
- навыками разработки и отладки программ не менее чем на одном из алгоритмических процедурных языков программирования высокого уровня

Должны быть сформированы следующие **компетенции**:

ОК.1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК-5.1. осваивать методики использования программных средств для решения практических задач;

ПК-5.2. разрабатывать интерфейсы «человек - электронно-вычислительная машина»

ПК-5.3. разрабатывать компоненты программных комплексов и баз данных, использовать современные инструментальные средства и технологии программирования

1. Краткое содержание модуля

Модуль «Участие в интеграции программных модулей» состоит из следующих МДК:

Раздел 1. Основы алгоритмизации

Тема 1.1 основы алгоритмизации. Понятие алгоритма, свойства, способы описания

1.2. основные алгоритмические конструкции. Принципы построения алгоритмов, способы описания, блок-схемы, основные конструкции,

1.3. история и классификация языков программирования. Классификация языков программирования, обзор языков программирования

Раздел 2. Интегрированная среда Turbo Pascal -7

2.1. система программирования на языке высокого уровня. Назначение и возможности ТП, справочная система, запуск, компиляция и отладка программы

2.2. элементы языка. Редактор интегрированной среды, символы и слова в ТП, идентификаторы

2.3. типы данных. Перечень типов данных, тождественность и совместимость типов данных

2.4. структура программы на Turbo Pascal -7. Структура Pascal программы, выражения, операции и операнды, операции отношений структура линейных, ветвляющих и циклических программ

Раздел 3 Операторы Turbo Pascal -7

3.1. ввода и вывода, присваивания. Операторы write, writeln, read, readln, конструкция оператора присваивания

3.2. условный оператор

3.3. Логический оператор.

3.4.циклический оператор предусловия.

3.5. циклический оператор постусловия

3.6. циклический оператор по параметру

Раздел 4. Элементы структуризации программ

4.1. понятие процедуры и функции

4.2.массивы: одномерный, двумерный, многомерный

4.3.основные операции над массивами

4.4. множества

4.5. записи

4.6.строка

Раздел 5. Стандартные модули

5.1. стандартный модуль CRT . Основные процедуры и функции стандартных модулей

5.2. аппаратная поддержка графики. Адаптер и видеомонитор. Типы видеоадаптеров. Графические драйверы. Состав графических средств.

5.3. стандартные модули GRAPH. Основные процедуры и функции стандартных модулей CRT и GRAPH, построение простейших геометрических фигур, использование цикла в графике, движущиеся объекты.

Раздел 6 Основные принципы объектно-ориентированного программирования

6.1. элементы языка Object Pascal. Основные понятия объектно-ориентированного программирования, введение в Object Pascal,

6.2. структура программы DELPHI. Назначение и общее описание среды

6.3. свойства и методы использования в объектно-ориентированном программировании

Самостоятельная работа студента

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению 090000 Информационная безопасность по специальности 090305 Информационная безопасность в автоматизированных, утвержденный приказом Министерства образования и науки РФ от 24 июня 2010г. №708.

2. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от «01» сентября 2011

Аннотация.
к рабочей программе дисциплины
Электроника и схемотехника

Направление подготовки	230000 Информатика и вычислительная техника
Профиль подготовки	СПО 090305 Информационная безопасность автоматизированных систем
Квалификация (степень) выпускника	Техник по защите информации

Цикл, раздел учебного плана	ОП.06 Общепрофессиональный цикл
Семестр(ы) изучения	3-4 семестр
Форма промежуточной аттестации (зачет/экзамен)	зачет
Количество часов всего, из них:	74
лекционные	54
практические	20
семинары	-
СРС	37
на экзамен/зачет	экзамен

1. Цели освоения дисциплины

Целями изучения дисциплины электроники и схемотехники являются преподавания: создание у студентов запаса знаний и навыков, достаточного для успешного усвоения других, связанных с электроникой дисциплин; освоение основ практической работы по сборке электрических схем и измерению различных электротехнических величин.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате освоения дисциплины обучающийся должен:
1.Знать:
- принципы работы типовых электронных устройств.
2. Уметь:
- рассчитывать типовые электронные устройства;
- читать электрические принципиальные схемы;

3. Краткое содержание дисциплины:
Учебная программа содержит следующие разделы:
Раздел 1. Полупроводники и приборы на их основе.
Раздел 2. Основы микроэлектроники
Раздел 3. Аналоговая схемотехника
Раздел 4. Усилители и генераторы.
Раздел 5. Микропроцессорные средства

4. Аннотация разработана на основании:
1. ФГОС СПО по направлению 230000 Информатика и вычислительная техника
2. ООП СПО по направлению СПО 090305 Информационная безопасность автоматизированных систем
3. Аннотация к РПД утверждена на заседании кафедры (протокол №___ от «__»____20_г.)

Аннотация
к рабочей программе дисциплины
Операционные системы

Направление подготовки	**090000 Информационная безопасность**
Специальность:	**090305 Информационная безопасность автоматизированных систем**
Профиль подготовки	

Квалификация (степень) выпускника	**Техник по защите информации**
Цикл, раздел учебного плана	П.00 Профессиональный цикл ОП.00 Общепрофессиональные дисциплины ОП.07. Операционные системы
Семестр(ы) изучения	*I, II*
Количество зачетных единиц (кредитов)	*114*
Форма промежуточной аттестации (зачет/экзамен)	*экзамен*
Количество часов всего, из них:	*114*
лекционные	*72*
практические	*18*
семинары	
СРС	*42*
на экзамен/зачет	

3. Цели освоения дисциплины

Целями изучения дисциплины Операционные системы являются сформировать общие и профессиональные компетенции программиста

4. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля).

В результате освоения дисциплины обучающийся должен:

- Использовать средства ОС и сред для решения практических задач;
- Использовать сервисные средства, поставляемые с ОС;
- Устанавливать различные ОС;
- Подключать к ОС новые сервисные средства;
- Решать задачи обеспечения защиты ОС.

В результате освоения учебной дисциплины обучающийся должен ***знать:***

- основные функции операционных систем;
- машинно- независимые свойства ОС;
- принципы построения ОС;
- сопровождение ОС.

5. Краткое содержание дисциплины

- ***Понятие операционных систем Функции операционных систем***
- Архитектура операционных систем
- Процессы в операционных системах
- Управление задачами
- Управление памятью в операционных системах
- Управление вводом-выводом в операционных системах
- Файловые системы
- Обзор современных операционных систем
- Сетевые операционные системы

6. Аннотация разработана на основании:

4. ФГОС СПО по направлению 090305 Информационная безопасность автоматизированных систем
   по направлению 090000 Информационная безопасность
5. ООП СПО по направлению090305 Информационная безопасность автоматизированных систем
   по направлению 090000 Информационная безопасность

6. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от 1 сентября 2011 года)

Аннотация
к рабочей программе дисциплины
БАЗЫ ДАННЫХ

Направление подготовки	**090000 Информационная безопасность**
Специальность:	**090305 Информационная безопасность автоматизированных систем**
Профиль подготовки	
Квалификация (степень) выпускника	**Техник по защите информации**
Цикл, раздел учебного плана	П.00 Профессиональный цикл ОП.00 Общепрофессиональные дисциплины ОП.08. Системы управления базами данных
Семестр(ы) изучения	*IV*
Количество зачетных единиц (кредитов)	*86*
Форма промежуточной аттестации (зачет/экзамен)	*экзамен*
Количество часов всего, из них:	*86*
лекционные	*36*
практические	*28*
семинары	
СРС	*22*
на экзамен/зачет	*зачет*

5. Цели освоения дисциплины

Целями изучения дисциплины Системы управления базами данных являются сформировать общие и профессиональные компетенции программиста

6. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля).

В результате освоения дисциплины обучающийся должен уметь:

- Проводить анализ, выделять сущности и связи предметной области и отображать ее на конкретную модель данных;
- Нормализовывать отношения при проектировании реляционной базы данных;
- Работать с системами управления базами данных;
- Применять методы манипулирования данными;
- Строить запросы;
- Использовать встроенные механизмы защиты информации в системах управления базами данных.

В результате освоения учебной дисциплины обучающийся должен ***знать:***

- Основные понятия теории баз данных, модели данных;
- Основные принципы и этапы проектирования баз данных;
- Логическую и физическую структуру баз данных;
- Реляционную алгебру;
- Средства проектирования структур баз данных;
- Базовые понятия и классификацию систем управления базами данных;
- Методы и приемы манипулирования данными;

- Построение запросов в системах управления базами данных;
- Перспективы развития современных баз данных.

7. Краткое содержание дисциплины

- Теория проектирования баз данных
- Реляционные базы данных

Введение в язык SQL

Организация запросов SQL

8. Аннотация разработана на основании:

7. ФГОС СПО по направлению 090305 Информационная безопасность автоматизированных систем

   по направлению 090000 Информационная безопасность
8. ООП СПО по направлению090305 Информационная безопасность автоматизированных систем

   по направлению 090000 Информационная безопасность
9. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от 1 сентября 2011 года)

Аннотация
к рабочей программе дисциплины
Экономика организации

Направление подготовки	**090000 Информационная безопасность**
Специальность:	090305 ***Информационная безопасность автоматизированных систем***
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	ПП. Профессиональная подготовка ОГСЭ. Общий гуманитарный и социально- экономический цикл ОГСЭ.6 Экономика предприятия
Семестр(ы) изучения	3
Количество зачетных единиц (кредитов)	-
Форма промежуточной аттестации (зачет/экзамен)	Зачет
Количество часов всего, из них:	
лекционные	40
лабораторные	4
семинары	
СРС	22
на экзамен/зачет	

1. Цели освоения дисциплины:

Целями освоения дисциплины «Экономика предприятия» являются: Изучение студентами общих принципов и положений экономики предприятия и на этой основе получения ими специальных знаний по экономике, необходимых для практической деятельности по повышению эффективности производства путем его интенсификации. Вооружить студентов теоретическими знаниями и практическими навыками, которые будут им необходимы в их дальнейшей самостоятельной работе на предприятии, в организации и на фирме в рыночных условиях

Дисциплина «Экономика предприятия» имеет своей целью формировать у

обучающихся общекультурные (ОК-1- ОК-10) и профессиональные (ПК-4.1, ПК-4.2, ПК-4.3) компетенции в соответствии с требованиями ФГОС СПО по направлению подготовки **090000 Информационная безопасность** по специальности 090305 ***Информационная безопасность автоматизированных систем*** (квалификация: техник – по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате освоения дисциплины обучающийся должен:

2.1.знать:

- состав материальных, трудовых и финансовых ресурсов организации, показатели их эффективного использования;
- методы комплексного экономического анализа условий и результатов деятельности предприятия;
- механизмы ценообразования;
- формы оплаты труда в современных условиях

2.2.уметь:

- рассчитывать основные экономические показатели деятельности предприятия
- владеть методами сбора, обработки и анализа внешней и внутренней информации;
- находить и использовать необходимую экономическую информацию

Должны быть сформированы следующие **компетенции**:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

ПК.4.1. Участвовать в планировании и организации работы структурного подразделения .

ПК.4.2. Участвовать в руководстве работой структурного подразделения.

ПК.4.3. Участвовать в анализе процесса и результатов деятельности подразделения.

Краткое содержание дисциплины

Дисциплина **Экономика предприятия** состоит из следующих разделов:

Раздел 1.Предприятие в рыночной экономике

Тема 1.1.Организационно-правовые формы предприятия

Тема 1.2.Организационно-правовые формы предприятия

Тема 1.3.Отраслевые особенности предприятий

Тема 1.4. Структура предприятия

Раздел 2.Материально-техническая база предприятия

Тема 2.1.Имущество предприятия

Тема 2.2Основные фонды предприятия

Тема 2.3Оборотные средства предприятий

Тема 2.4Инвестиции и капитальные вложения

Раздел 3 Трудовые ресурсы предприятия

Тема 3.1Персонал, организация и оплата труда

Тема 3.2Формы и системы оплаты труда

Раздел 4.Ценообразование и ценовая политика предприятия

Тема 4.1.**Производственно-хозяйственная деятельность предприятий**

Тема 4.2.Себестоимость продукции, прибыль, рентабельность

Тема 4.3.Цена, предложение, спрос.

Раздел 5 **Планирование и организация производственно-хозяйственной деятельности предприятия**

Тема 5.1.Задачи и виды внутрипроизводственного планирования

Тема 5.2Производственная программа предприятия

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению **090000 Информационная безопасность** по специальности 090305 ***Информационная безопасность автоматизированных систем*** (квалификация: техник – по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

2. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от «01» сентября 2011 г.)

Аннотация
к рабочей программе дисциплины
Методы и средства защиты информации

Направление подготовки	230000 Информатика и вычислительная техника
Специальность:	090305 ***Информационная безопасность автоматизированных систем***
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	П. Профессиональный цикл ОП. Общепрофессиональные дисциплины ОП.11 Методы и средства защиты информации
Семестр(ы) изучения	1
Количество зачетных единиц (кредитов)	-
Форма промежуточной аттестации (зачет/экзамен)	Дифференциальный зачет
Количество часов всего, из них:	
лекционные	48
лабораторные	20

семинары	
СРС	34
на экзамен/зачет	

1. Цели освоения дисциплины

Основная образовательная ***цель*** дисциплины ОП.11 «Методы и средства защиты информации»: - создать у студента фундамент знаний и умений по защите информации, который способен в дальнейшем обеспечить успешное применение методов и средств в процессе освоения дисциплин специальности, а также в профессиональной деятельности по специальности.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Студент после изучения дисциплины должен:

1.1. иметь представление:

1.1.1. о многообразии инструментальных и прикладных программных средств, проблемах и перспективах развития программного (антивирусного) обеспечения;

1.2. знать:

1.2.1.методы и приемы программной защиты информации;

1.3. уметь:

1.3.1. осуществлять программную защиту информации.

Дисциплина «Методы и средства защиты информации» имеет своей целью формировать у обучающихся общие компетенции (ОК-1, ОК–2, ОК-3, ОК-4, ОК-5, ОК-6, ОК-7, ОК-8, ОК-9, ОК-10) и профессиональные компетенции (ПК-2.1., ПК-2.2., ПК-2.3., ПК-2.4., ПК-2.5., ПК-2.6.), в соответствии с требованиями ФГОС СПО по направлению подготовки **090000 Информационная безопасность** по специальности 090305 ***Информационная безопасность автоматизированных систем*** (квалификация: техник – по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

Должны быть сформированы следующие **компетенции**:

В результате освоения дисциплины обучающийся должен:

3.1.знать:

1. 3.1.1. Защиту информации в информационных системах

3.1.2. Организационно-правовое обеспечение информационной безопасности

3.2. уметь:

3.2.1. применять вычислительную технику для решения практических задач;

3.3. владеть:

2. 3.3.1. Методами и средствами защиты информации.

Должны быть сформированы следующие **компетенции**:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

ПК.2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах.

ПК.2.2. 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.

ПК.2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

ПК.2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

ПК.2.5. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.

ПК.2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

Краткое содержание дисциплины

Дисциплина «Методы и средства защиты информации» состоит из следующих разделов:

1. Введение

2. Методы и средства защиты информации

Тема 2.1. *Проблемы защиты информации.*

Тема 2.2. *Система защиты информации*

Тема 2.3. *Защита информации от технических разведок*

Тема 2.4. *Способы защиты информации от технических разведок*

Тема 2.5. *Средства защиты от технических разведок*

3. Защита информации при ее обработке техническими средствами

Тема 3.1. *Технические средства обработки информации (ТСОИ).*

Тема 3.2. *Защита информации при ее обработке техническими средствами.*

Тема 3.3. *Защита информации от утечки за счет ПЭМИ и ПЭМН.*

Тема 3.4. *Защита информации от НСД штатными техническими средствами.*

Тема 3.5. *Защита информации от воздействия специальных электронных закладных устройств (аппаратных закладок) и внешних воздействий*

Тема 3.6. *Криптографическая защита информации.*

Тема 3.7. *Методы антивирусной защиты информации*

2. Защита информации в информационных системах

Тема 4.1. *Вычислительные сети и защита информации*

Тема 4.2. *Защита локальных сетей и операционных систем*

Тема 4.3. *Проблемы защиты информации в Интернет. Рекомендации по защите информации в Интернет*

Тема 4.4. *Информационная безопасность в Intranet*

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению **090000 Информационная безопасность** по

специальности 090305 ***Информационная безопасность автоматизированных систем*** (квалификация: техник – по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

2. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от «01» сентября 2011 г.)

Аннотация.
к рабочей программе дисциплины
ЭЛЕКТРОТЕХНИКА

Направление подготовки	230000 Информатика и вычислительная техника
Профиль подготовки	СПО 090305 Информационная безопасность автоматизированных систем
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	ОП.00.Общепрофессиональная дисциплина. ОП.12.Электротехника.
Семестр(ы) изучения	1-2 семестр
Форма промежуточной аттестации (зачет/экзамен)	Контрольная работа
Количество часов всего, из них:	102
лекционные	48
практические	20
семинары	-
СРС	34
на экзамен/зачет	9

1. Цели освоения дисциплины

Целями изучения дисциплины основы электротехники являются преподавания электротехники являются: создание у студентов запаса знаний и навыков, достаточного для успешного усвоения других, связанных с электротехникой дисциплин; освоение основ практической работы по сборке электрических схем и измерению различных электротехнических величин.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате освоения дисциплины обучающийся должен:

1.Знать:

основные характеристики, параметры и элементы электрических цепей при гармоническом воздействии в установившемся воздействии в установившемся режиме; свойства основных электрических RC и RLC-цепочек, цепей с взаимной индукцией;

трехфазные электрические цепи;
понятие линейного четырехполюсника;
основные свойства фильтров;
непрерывные и дискретные сигналы;

2. Уметь:

применять основные определения и законы теории электрических цепей;

учитывать на практике свойства цепей с распределенными параметрами и нелинейных электрических цепей;

различать непрерывные и дискретные сигналы и их параметры;

3. Владеть:

автоматизацией измерений;
навыками измерения тока, напряжения и мощности;
параметрами и характеристиками электрорадиотехнических цепей и компонентов.

3. Краткое содержание дисциплины:

Учебная программа содержит следующие разделы:

Раздел 1. Электрические цепи постоянного тока. Методы расчёта.
Раздел 2. Магнитные цепи постоянного тока
Раздел 3. Электромагнитная индукция
Раздел 5. Электрические цепи несинусоидального тока
Раздел 6. Трёхфазные цепи
Раздел 7. Длинные линии

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению 230000 Информатика и вычислительная техника
2. ООП СПО по направлению СПО 090305 Информационная безопасность автоматизированных систем
3. Аннотация к РПД утверждена на заседании кафедры (протокол №___ от «__»____20_г.)

Аннотация
к рабочей программе дисциплины (модуля)
ОП.13 Компьютерная графика

Направление подготовки	090000 Информационная безопасность
Профиль подготовки	090305 Информационная безопасность автоматизированных систем
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	Общепрофессиональные дисциплины
Семестр(ы) изучения	2
Количество зачетных единиц (кредитов)	2
Форма промежуточной аттестации (зачет/экзамен)	Зачет
Количество часов всего, из них:	128
Лекционные	42
Практические	44
Семинары	
СРС	42
на экзамен/зачет	2

1. Цели освоения дисциплины

Целями изучения дисциплины «Компьютерная графика» являются: формирование базового представления, первичных знаний, умений и навыков у студентов по основам компьютерной графики как научной фундаментальной и прикладной дисциплины, достаточных для дальнейшего продолжения образования и самообразования их в области вычислительной техники, информационных систем различного назначения и в смежных информатике областях.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля).

В результате освоения дисциплины обучающийся должен:

1. Знать:

- Виды компьютерной графики
- Основы представления графических данных
- Средства для создания графических изображений
- Приемы создания и обработки изображений,
- Методы создания чертежа

2 . Уметь:

- Обрабатывать изображения с помощью редактора Adobe Photoshop, владеть приемами ретуши, монтажа композиций, применять фильтры.
- Выполнять чертежные и оформительские работы с использованием редактора CorelDraw.
- Моделировать физические объекты с помощью редактора 3D studio MAX

3. Краткое содержание дисциплины

Компьютерная графика - как новое направление человеческой деятельности. Области применения компьютерной графики: полиграфия, реклама, дизайн (интерьера, промышленных изделий, предметно-пространственной среды и т.д.), разработка и дизайн Web приложений в Internet, создание анимационных фильмов, компьютерных игр, графическое оформление официальных документов, создание презентаций и т.д. Классификация средств и методов компьютерной графики. Технология работы над проектами и особенности работы в коллективе.

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению 090000 Информационная безопасность по специальности **090305 Информационная безопасность автоматизированных систем**

2. Аннотация к РПД утверждена на заседании кафедры протокол №1 от «1»сентября 2011г.

Аннотация
к рабочей программе дисциплины
Метрология, стандартизация и сертификация

Направление подготовки	***090000 Информационная безопасность***
Специальность:	**090305** ***Информационная безопасность автоматизированных систем***
Квалификация (степень) выпускника	техник по защите информации
Цикл, раздел учебного плана	П. Профессиональный цикл ОП. Общепрофессиональные дисциплины ОП.14 Метрология, стандартизация и сертификация
Семестр(ы) изучения	5
Количество зачетных единиц (кредитов)	-
Форма промежуточной аттестации (зачет/экзамен)	Зачет
Количество часов всего, из них:	
лекционные	34
лабораторные	10
семинары	
СРС	16
на экзамен/зачет	

1. Цели освоения дисциплины

Основная образовательная ***цель*** дисциплины ОП.14 «**Метрология, стандартизация и сертификация**»:

- создать у студента фундамент знаний и умений по метрологии, стандартизации и сертификации, который способен в дальнейшем обеспечить успешное применение их в процессе освоения дисциплин специальности, а также в профессиональной деятельности по специальности.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Студент после изучения дисциплины должен:

2.1. знать:

2.1.1. правовые основы метрологии, стандартизации и сертификации;

2.1.2. основные понятия и определения метрологии, стандартизации и сертификации;

2.1.3. основные положения систем (комплексов) общетехнических и организационно-методических стандартов;

2.1.4. показатели качества и методы их оценки;

2.2. уметь:

2.2.1. применять требования нормативных документов к основным видам продукции (услуг) и процессов;

2.2.2. применять документацию систем качества;

2.2.3. применять основные правила и документы системы сертификации Российской Федерации;

Дисциплина «**Метрология, стандартизация и сертификация**» имеет своей целью формировать у обучающихся общие компетенции (ОК-1, ОК–2, ОК-3, ОК-4, ОК-5, ОК-6, ОК-7, ОК-8, ОК-9, ОК-10) и профессиональные компетенции (ПК-4.1, ПК-4.2, ПК-4.3., ПК-4.4, ПК-4.5, ПК-4.6), в соответствии с требованиями ФГОС СПО по направлению подготовки**:** ***090000 Информационная безопасность*** по специальности **090305** ***Информационная безопасность автоматизированных систем*** (квалификация: техник по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

Должны быть сформированы следующие **компетенции**:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

ПК 4.1. Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.

ПК 4.2. Выполнять интеграцию модулей в программную систему.

ПК 4.3. Выполнять отладку программного продукта с использованием специализированных программных средств.

ПК 4.4. Осуществлять разработку тестовых наборов и тестовых сценариев.

ПК 4.5. Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.

ПК 4.6. Разрабатывать технологическую документацию.

Краткое содержание дисциплины

Дисциплина **«Метрология, стандартизация и сертификация»** состоит из следующих разделов:

1. Введение.

Содержание дисциплины и ее задачи. Связь с другими дисциплинами

2. Метрология

Тема 2.1. Структурные элементы метрологии, ее цели и задач

Тема 2.2. Объекты и субъекты метрологии

Тема 2.3. Основы теории измерений

Тема 2.4. Государственная система обеспечения единства измерений

3. Стандартизация

Тема 3.1. Стандартизация. Принципы и методы стандартизации

Тема 3.2. Государственная и межгосударственная системы стандартизации.

Тема 3.3. Правовая база стандартизации.

Тема 3.4. Международное и региональное сотрудничество в области стандартизации

4. Сертификация

Тема 4.1. Сертификация, ее основные составные элементы

Тема 4.2. Правила проведения сертификации потребительских товаров

Тема 4.3. Испытания и контроль качества продукции.

Тема 4.4. Управление качеством продукции.

5. Правовое обеспечение информационных технологий

Тема 5.1. Информационное право. Сертификация информационных систем.

Тема 5.2. Правовая охрана товарных знаков. ФЗ « О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров».

Тема 5.3. Патентное законодательство. ФЗ « Патентный закон».

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению ***090000 Информационная безопасность*** по специальности **090305** ***Информационная безопасность автоматизированных систем*** (квалификация: техник – по защите информации), утвержденного приказом Министерства образования и науки РФ от 24.06.2010 г. №708.

2. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от «01» сентября 2011 г.)

Аннотация
к рабочей программе дисциплины
«Безопасность жизнедеятельности»

Направление подготовки	230000 Информатика и вычислительная техника
Профиль подготовки	090305 Информационная безопасность автоматизированных систем
Квалификация (степень) выпускника	техник по защите информации
Цикл, раздел учебного плана	П.00. Профессиональный цикл. ОП. Общепрофессиональные дисциплины ОП.11. Безопасность жизнедеятельности
Семестр(ы) изучения	5,6
Форма промежуточной аттестации (зачет/экзамен)	зачет
Количество часов всего, из них:	108
лекционные	34
практические	34
семинары	-
СРС	40
на экзамен/зачет	9

1. Цели освоения дисциплины

Цели:

- обеспечение комфортных условий деятельности человека на всех стадиях его жизненного цикла и нормативно допустимых уровней воздействия негативных факторов на человека и природную среду;

- формирование личности, знающей основы защиты человека, общества, государства от современного комплекса опасных факторов и умеющей применить эти знания на практике.

Задачи:

- выбор принципа защиты;

- разборка и рациональное использование средств защиты человека и природной среды от негативных воздействий техногенных источников и стихийных явлений.

- реализация новых методов защиты;

- моделирование чрезвычайных ситуаций;

- изучение и освоение основ медицинских знаний и правил оказания первой медицинской помощи в опасных и чрезвычайных ситуациях;

- изучение основ военной службы, обеспечивающей аспект национальной безопасности;

- теоретический анализ и разработка методов идентификации опасных и вредных факторов.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины.

В результате освоения учебной дисциплины обучающийся **должен уметь**:

- организовывать и проводить мероприятия по защите работающих и населения от негативных воздействий чрезвычайных ситуаций;

- предпринимать профилактические меры для снижения уровня опасностей различного вида и их последствий в профессиональной деятельности и быту;
- использовать средства индивидуальной и коллективной защиты от оружия массового поражения;
- применять первичные средства пожаротушения;
- ориентироваться в перечне военно-учетных специальностей и самостоятельно определять среди них родственные полученной специальности;
- применять профессиональные знания в ходе исполнения обязанностей военной службы на воинских должностях в соответствии с полученной специальностью;
- владеть способами бесконфликтного общения и саморегуляции в повседневной деятельности и экстремальных условиях военной службы;
- оказывать первую помощь пострадавшим.

В результате освоения учебной дисциплины обучающийся **должен знать**:

- 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;
- основные виды потенциальных опасностей и их последствия в профессиональной деятельности и быту, принципы снижения вероятности их реализации;
- основы военной службы и обороны государства;
- задачи и основные мероприятия гражданской обороны;
- способы защиты населения от оружия массового поражения; меры пожарной безопасности и правила безопасного поведения при пожарах;
- организацию и порядок призыва граждан на военную службу и поступления на нее в добровольном порядке;
- основные виды вооружения, военной техники и специального снаряжения, состоящих на вооружении (оснащении) воинских подразделений, в которых имеются военно-учетные специальности, родственные специальностям СПО;
- область применения получаемых профессиональных знаний при исполнении обязанностей военной службы;
- порядок и правила оказания первой помощи пострадавшим.

Должны быть сформированы следующие **компетенции**:

1. **Общекультурные компетенции:**

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

2. Профессиональные компетенции:

ПК 1.1. Участвовать в эксплуатации компонент подсистем безопасности автоматизированных систем, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.

ПК 1.2. Выполнять работы по администрированию подсистем безопасности автоматизированных систем.

ПК 1.3. Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем.

ПК 1.4. Организовывать мероприятия по охране труда и технике безопасности в процессе эксплуатации автоматизированных систем и средств защиты информации в них.

ПК 1.5. Вести техническую документацию, связанную с эксплуатацией средств технической защиты и контроля информации в автоматизированных системах.

ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности.

ПК 2.2. Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и ПК 2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.

ПК 2.4. Участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

ПК 2.5. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов.

ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.

ПК 3.2. 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.

ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.

ПК 3.4. Решать частные технические задачи, возникающие при проведении всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.

ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

3. Краткое содержание дисциплины

Чрезвычайные ситуации мирного и военного времени, природного и

техногенного характера, их последствия.

Устойчивость производств в условиях ЧС.

Организационные основы по защите населения от чрезвычайных ситуаций мирного и военного времени. Назначение и задачи гражданской обороны.

Организация защиты и жизнеобеспечения населения в ЧС.

Основы медицинских знаний

Основы военной службы

Основы обороны государства

Вооруженные силы РФ

Военная служба – особый вид Федеральной государственной службы

Боевые традиции

Символы воинской чести

Идентификация травмирующих и вредных факторов, воздействие негативных факторов на человека

Особенности обеспечения безопасных условий труда в сфере профессиональной деятельности

4 Аннотация разработана на основании:

1. ФГОС ВПО по направлению 230000 Информатика и вычислительная техника.

2. ООП СПО по направлению 090305 Информационная безопасность автоматизированных систем

3. Аннотация к РПД утверждена на заседании кафедры (протокол №___ от «__»____20_г.)

Аннотация
к рабочей программе модуля
ПМ.03. Применение инженерно-технических средств обеспечения информационной безопасности

Направление подготовки	***090000 Информационная безопасность***
Специальность:	**090305. Информационная безопасность автоматизированных систем**
Профиль подготовки	
Квалификация (степень) выпускника	**техник**
Цикл, раздел учебного плана	ПМ.00 Профессиональные модули. ПМ.03 Применение инженерно-технических средств обеспечения информационной безопасности МДК.03.01. Применение инженерно-технических средств обеспечения информационной безопасности
Семестр(ы) изучения	*III, IV*
Количество зачетных единиц (кредитов)	*235*
Форма промежуточной аттестации (зачет/экзамен)	*зачет*
Количество часов всего, из них:	*235*
лекционные	*144*
практические	*12*
семинары	
СРС	*79*
на экзамен/зачет	

7. Цели освоения дисциплины

Целями изучения модуля Применение инженерно-технических средств обеспечения информационной безопасности являются

С целью овладения указанным видом професиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

ПК 1.1. Разрабатывать схемы цифровых устройств на основе интегральных схем разной степени интеграции.

ПК. 1.2. Выполнять требования технического задания на проектирование цифровых устройств.

ПК 1.3. Использовать средства и методы автоматизированного проектирования при разработке цифровых устройств.

ПК 1.4. Определять показатели надежности и качества проектируемых цифровых устройств.

ПК 1.5. Выполнять требования нормативно-технической документации.

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый к ней интерес.

ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышения квалификации.

ОК 9. Ориентироваться в условиях частной смены технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

8. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля).

В результате освоения дисциплины обучающийся должен:

3. Знать

- Понятие, виды и структуру автоматизированных систем
- Понятие и составляющие безопасности автоматизированных систем
- Схемы каталогизации угроз безопасности КС, способы их идентификации, спецификации и оценивания, роль человеческого фактора в угрозах безопасности КС
- Понятия функциональной и системной архитектуры КС, ядра (монитора, системы) безопасности КС
- Общую характеристику и методологию руководящих документов Гостехкомиссии/ФСТЭК по защите СВТ и АС от НСД к информации, классы

защищенности и структуру функциональных требований к подсистемам защиты информации 4

- Общую характеристику и структуру стандартов по безопасности информационных технологий, виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований безопасности к изделиям ИТ, общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия
- Общую характеристику стандартов и особенности регламентации
- архитектуры систем защиты информации при взаимодействии открытых систем
- Модель жизненного цикла и порядок создания АС, стандарты и их содержание по регламентации стадий и этапов создания АС, структуру, порядок составления, оформления и утверждения Технического задания по созданию АС, состав и структуру основных документов, отрабатываемых на этапе технорабочего проектирования

4. Уметь

- Идентифицировать и оценивать угрозы безопасности при формировании требований пользователя к КС
- Определять и оформлять класс защищенности создаваемой КС
- Составлять и правильно оформлять основные разделы Технического задания на создание несложных КС (системы защиты информации КС)
- Составлять отдельные разделы Профиля защиты применительно к простым видам изделий ИТ
- Составлять диаграммы Гантта и сетевые графики несложных процессов проектирования, осуществлять их анализ и оптимизацию
- Планировать индивидуально-групповою структуру пользователей КС и структуру разделяемых (коллективных) информационных ресурсов
- Разрабатывать политику и регламентации технологических процедур генерации, хранения и эксплуатации парольных и других средств аутентификации пользователей КС, архивирования информационных ресурсов, эксплуатации сменных носителей информации

5. Владеть

- применения интегральных схем разной степени интеграции при разработке цифровых устройств и проверки их на работоспособность;
- проектирование цифровых устройств на основе пакетов прикладных программ;
- оценки качества и надежности цифровых устройств;
- применения нормативно-технической документации.

9. Краткое содержание дисциплины

МДК.03.01. ***Применение инженерно-технических средств обеспечения информационной безопасности***

- Введение

Защищенные компьютерные системы и требования к ним

Порядок создания и проектирования защищенных КС

Эксплуатация защищенных КС

10. Аннотация разработана на основании:

10. ФГОС СПО по направлению 090305. Информационная безопасность автоматизированных систем

по направлению 090000 Информационная безопасность

11. ООП СПО по 090305. Информационная безопасность автоматизированных систем

по направлению 090000 Информационная безопасность

12. Аннотация к РПД утверждена на заседании кафедры (протокол №1 от «1» 09 2011 года)

Аннотация
к рабочей программе модуля

СЕТЕВЫЕ ТЕХНОЛОГИИ

Направление подготовки	**210700 Информационная безопасность**
Специальность:	**090305 Информационная безопасность автоматизированных систем**
Профиль подготовки	
Квалификация (степень) выпускника	**техник по защите информации**
Цикл, раздел учебного плана	ПМ.00 Профессиональные модули. ПМ.В. Вариативная часть по циклу ПМ ПМ.05. Сетевые технологии МДК.05.01. Web-программирование
Семестр(ы) изучения	*IV*
Количество зачетных единиц (кредитов)	-
Форма промежуточной аттестации (зачет/экзамен)	*зачет*
Количество часов всего, из них:	*98*
лекционные	*35*
практические	*30*
семинары	
СРС	*33*
на экзамен/зачет	

Цели освоения дисциплины

Целями изучения модуля ПМ.05 Сетевые технологии являются

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

ПК 8.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев;

ПК 8.2. Администрировать сетевые ресурсы в информационных системах;

ПК 8.3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей;

ПК 8.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

1. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля).

В результате освоения дисциплины обучающийся должен:

1. Знать

- основные направления администрирования компьютерных сетей;
- типы серверов, технологию «клиент-сервер»; способы установки и управления сервером; утилиты, функции, удаленное управление сервером;
- технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в Web;
- использование кластеров;

- мониторинг и настройку производительности;
- технологию ведения отчетной документации;
- классификацию программного обеспечения сетевых технологий, и область его применения;
- лицензирование программного обеспечения;
- оценку стоимости программного обеспечения в зависимости от способа и места его использования
- основные технологии программирования в программных средствах, используемых в современных инфокоммуникационных технологиях.

2. ***Уметь***
    - администрировать локальные вычислительные сети;
    - принимать меры по устранению возможных сбоев;
    - устанавливать информационную систему;
    - создавать и конфигурировать учетные записи отдельных пользователей и пользовательских групп;
    - регистрировать подключение к домену, вести отчетную документацию;
    - рассчитывать стоимость лицензионного программного обеспечения сетевой инфраструктуры;
        - устанавливать и конфигурировать антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга,
    - обеспечивать защиту при подключении к Интернет средствами операционной системы;
    - разрабатывать и тестировать программы с применением программных средств, используемых в современных инфокоммуникационных технологиях
    - использовать специальную литературу в изучаемой предметной области
3. Владеть
    - по настройке сервера и рабочих станций для безопасной передачи информации;
    - установки Web - сервера;
    - организации доступа к локальным и глобальным сетям;
    - сопровождению и контролю использования почтового сервера, SQL - сервера и др.;
    - расчета стоимости лицензионного программного обеспечения сетевой инфраструктуры;
    - сбора данных для анализа использования и функционирования программно-технических средств компьютерных сетей;

3. Краткое содержание дисциплины

МДК.05.01. Web-программирование

- Программирование на стороне клиента
- Программирование на стороне сервера

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению *090305 Информационная безопасность автоматизированных систем* по направлению *210700 Информационная безопасность*
2. ООП СПО по направлению *090305 Информационная безопасность автоматизированных систем*
3. по направлению *090305 Информационная безопасность автоматизированных систем* аннотация к РПД утверждена на заседании кафедры (протокол № 1 от «01» сентября 2011 г.)

Аннотация
к рабочей программе модуля
ПМ.03. Участие в интеграции программных модулей

Направление подготовки	090000 Информационная безопасность
Профиль подготовки	090305 Информационная безопасность
Квалификация (степень) выпускника	Техник по защите информации
Цикл, раздел учебного плана	П.00. Профессиональный цикл ПМ.00. Профессиональные модули
Семестр(ы) изучения	5, 6
Количество зачетных единиц (кредитов)	
Форма промежуточной аттестации (зачет/экзамен)	Квалификационный экзамен
Количество часов всего, из них:	512
лекционные	185
лабораторные	90
Курсовая работа	30
семинары	
СРС	153
Учебная практика	18 ч.
Производственная практика	36 ч.
на экзамен/зачет	1 зачетная единица

1. Цели освоения модуля

Целями освоения модуля «Участие в интеграции программных модулей» являются: формирование у студентов компетенций по участию в интеграции программных модулей, достаточных для профессиональной деятельности в области вычислительной техники, информационных систем различного назначения и в смежных областях.

Модуль «Участие в интеграции программных модулей» имеет своей целью формировать у обучающихся общекультурные (ОК-1 – ОК-10) и профессиональные компетенции (ПК-4.1. – ПК-4.6.) в соответствии с требованиями ФГОС СПО по направлению подготовки 090000 Информационная безопасность (квалификация техник по защите информации), утвержденного приказом Министерства образования и науки РФ от 24 июня 2010 г. №708.

2. Компетенции обучающегося, формируемые в результате освоения модуля

В результате освоения модуля обучающийся должен:

2.1.знать:

2.1.1. модели процесса разработки программного обеспечения;
2.1.2. основные принципы процесса разработки программного обеспечения;
2.1.3. основные подходы к интегрированию программных модулей;
2.1.4. основные методы и средства эффективной разработки;
2.1.5. основы верификации и аттестации программного обеспечения;
1.1.6. концепции и реализации программных процессов;
1.1.7. принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного обеспечения;
1.1.8. методы организации работы в коллективах разработчиков программного обеспечения;

1.1.9. основные положения метрологии программных продуктов, принципы построения, проектирования и использования средств для измерений характеристик и параметров программ, программных систем и комплексов

2.2. уметь:

2.2.1. владеть основными методологиями процессов разработки программного обеспечения;

2.2.2. использовать методы для получения кода с заданной функциональностью и степенью качества;

2.3. иметь практический опыт:

2.3.1. участия в выработке требований к программному обеспечению;

2.3.2. участия в проектировании программного обеспечения с использованием специализированных программных пакетов;

Должны быть сформированы следующие **компетенции**:

ОК.1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.

ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

ПК 4.1. Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.

ПК 4.2. Выполнять интеграцию модулей в программную систему.

ПК 4.3. Выполнять отладку программного продукта с использованием специализированных программных средств.

ПК 4.4. Осуществлять разработку тестовых наборов и тестовых сценариев.

ПК 4.5. Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.

ПК 4.6. Разрабатывать технологическую документацию.

2. Краткое содержание модуля

Модуль «Участие в интеграции программных модулей»состоит из следующих МДК:

МДК.03.01. Технология разработки программного обеспечения

Раздел 1. Общие принципы разработки программных продуктов

Тема 1.1. Программные продукты и их основные характеристики
Тема 1.2. Классификация программных продуктов
Тема 1.3. Жизненный цикл программ
Тема 1.4. Стадии разработки программ и программной документации
Тема 1.5. Документирование программных средств
Раздел 2. Методология проектирования программных продуктов
Тема 2.1 Методы проектирования ПП
Тема 2.2. Структура ПП
Тема 2.3. Проектирование интерфейса пользователя
Раздел 3. Разработка программных продуктов
Тема 3.1. Стиль программирования
Тема 3.2. Языки программирования
Тема 3.3. Модульное программирование
Тема 3.4. Структурное программирование
Тема 3.5. Объектно-ориентированное программирование
Тема 3.6. Эффективность и оптимизация программ
Тема 3.7. Обеспечение качества программного продукта
Раздел 4. Отладка, тестирование и сопровождение программ
Тема 4.1. Ошибки программного обеспечения
Тема 4.2. Отладка программ
Тема 4.3. Тестирование программ
МДК.03.02. Инструментальные средства разработки программного обеспечения
Раздел 5. Инструментальные средства разработки программ
Тема 5.1. Общая характеристика инструментальных средств разработки программ
Тема 5.2. Применение CASE-средств
Раздел 6. Коллективная разработка программных средств
Тема 6.1. Организация работ при коллективной разработке программных продуктов
Тема 6.2. Экономические аспекты создания и использования программных средств
Учебная практика
Производственная практика

4. Аннотация разработана на основании:

1. ФГОС СПО по направлению 090000 Информационная безопасность по специальности 090305 Информационная безопасность в автоматизированных, утвержденный приказом Министерства образования и науки РФ от 24 июня 2010г. №708.

2. Аннотация к РПД утверждена на заседании кафедры (протокол № 1 от «01» сентября 2011 г.)

Приложение 1

ПРОТОКОЛ СОГЛАСОВАНИЯ

ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

КОД 090000 НАИМЕНОВАНИЕ ПРОГРАММЫ Информационная безопасность

НАИМЕНОВАНИЕ СПЕЦИАЛЬНОСТИ 090305 Информационная безопасность автоматизированных систем

Рассмотрев основную образовательную программу 090305 Информационная безопасность автоматизированных систем ООО «Эльф - Инфор» одобряет ее содержание.

Предлагаем внести следующие дополнения *(при их отсутствии не заполняется)*:

_____

_____

_____

_____

_____

_____.

Руководитель проектной группы по разработке ОПОП:

Зав. кафедрой

ЭОИС КТ ТИ СВФУ (должность),

Протодьяконова Г.Ю.(Ф.И.О.)

_____(подпись)

Представитель работодателя:

Руководитель

Кондаков А.А.

_____(подпись)

М.П.

Приложение 1

ПРОТОКОЛ СОГЛАСОВАНИЯ

ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

КОД 090000 НАИМЕНОВАНИЕ ПРОГРАММЫ Информационная безопасность

НАИМЕНОВАНИЕ СПЕЦИАЛЬНОСТИ 090305 Информационная безопасность автоматизированных систем

Рассмотрев основную образовательную программу 090305 Информационная безопасность автоматизированных систем ОАО «Информационно – технический центр АПК» одобряет ее содержание.

Предлагаем внести следующие дополнения *(при их отсутствии не заполняется)*:

_____

_____

_____

_____

_____

_____.

Руководитель проектной группы по разработке ОПОП:

Зав. кафедрой

ЭОИС КТ ТИ СВФУ

Протодьяконова Г.Ю.

_____(подпись)

Представитель работодателя:

Генеральный директор

Кривошапкин А.Е.

_____(подпись)

М.П.