Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

АННОТАЦИЯ К ПРОГРАММЕ ПРАКТИКИ

С.5.2 Производственная практика (технологическая)

специальности подготовки
10.05.03 "Информационная безопасность автоматизированных систем"
Специализация «Создание автоматизированных систем в защищенном исполнении»

форма обучения – очная
курс – 3
семестр – 6
зачетных единиц – 3
всего часов – 108
зачет с оценкой – 6 семестр

1.ОБЩИЕ СВЕДЕНИЯ

Рабочая программа практики разработана в соответствии с Положением о порядке проведения практики студентов по программе высшего профессионального образования, утвержденного решением Ученого совета СГТУ от 2013 г.

Рабочая программа практики выдается студенту до прохождения практики с тем, чтобы студент мог обратить особое внимание на те вопросы, которые он должен осветить при выполнении индивидуального задания.

В программе излагаются вопросы организации практики, обязанности руководителей практики и студентов, цели и задачи практики, ее содержание, методические указания по ее проведению, требования к оформлению отчета по практике.

К практике допускаются студенты, изучившие основы техники безопасности.

Учебно-методическое руководство практикой осуществляется кафедрой согласно приказа ректора университета.

Студенты, не выполнившие программу практики, получившие отрицательный отзыв о работе в ходе практики или не защитившие результаты практики, *подлежит исключению из университета.*

2. ЦЕЛИ И ЗАДАЧИ ПРАКТИКИ

Основной целью прохождения **производственной (технологической) практики** в 6 семестре является закрепление, расширение, углубление и систематизация знаний, полученных при изучении общепрофессиональных, специальных и технологических дисциплин таких как «Криптографические методы защиты информации» «Сети и системы передачи информации», «Безопасность операционных систем», формирование следующих компетенций:

(ПК-17) способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем;

(ПК-18) способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;

(ПК-19) способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности;

(ПК-20) способность разрабатывать политики информационной безопасности автоматизированных систем;

(ПК-21) способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;

(ПК-22) способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы;

(ПК-23) способность проводить контрольные проверки работоспособности и эффективности применяемых программно-

аппаратных, криптографических и технических средств защиты информации;

(ПК-24) способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем;

(ПК-25) способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации;

(ПК-26) способность проводить инструментальный мониторинг защищенности автоматизированных систем;

(ПК-27) способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности

(ПК-28) способностью разрабатывать оперативные планы работы первичных подразделений

(ПК-33) способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

(ПСК 9.4) способность применять современные технологии проектирования автоматизированных систем в защищенном исполнении;

(ПСК 9.5) способность применять нормативные правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации автоматизированных систем в защищенном исполнении на различных стадиях их жизненного цикла.

В результате прохождения практики студент должен:

знать:

методы анализа проектных решений по обеспечению информационной безопасности

методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем

Современные средства разработки компонентов автоматизированных систем

принципы формирования политики информационной безопасности в автоматизированных системах

основные методы управления информационной безопасностью

методики проектирования средств защиты информации и средств контроля защищенности автоматизированной системы

содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем

организацию работы и нормативные правовые акты и стандарты по сертификации средств защиты автоматизированных систем

организацию работы и нормативные правовые акты и стандарты по аттестации автоматизированных систем

Методы мониторинга защищенности автоматизированных систем

общую методику организации работы малых коллективов исполнителей на этапах управленческого цикла.

основные методы управления деятельностью служб защиты информации на предприятии;

технические характеристики, показатели качества системы управления информационной безопасностью автоматизированной системы методы их оценки и пути совершенствования

принципы формирования политики информационной безопасности в автоматизированных системах;

Принципы проектирования и анализа автоматизированных систем в защищенном исполнении

основные нормативно-правовые акты, руководящие и методические документы, регламентирующие процессы создания и эксплуатации АСЗИ для конкретного предприятия

уметь:

Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем

проектировать и администрировать автоматизированные системы и подсистемы безопасности автоматизированных систем

проводить выбор эффективных способов реализации структур данных и конкретных алгоритмов при решении профессиональных задач

планировать политику безопасности операционных систем;

разрабатывать предложения по совершенствованию системы управления информационной безопасностью

применять компьютерные технологии при проектировании средств защиты информации

оценивать эффективность и надежность защиты автоматизированных систем

проводить работы по сертификации средств защиты автоматизированных систем

проводить работы по аттестации автоматизированных систем

выявлять уязвимости информационно- технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем

правильно организовывать свой труд и работу других исполнителей управленческих решений в рамках своей компетенции

разрабатывать оперативные планы работы первичных подразделений при решении задач обеспечения информационной безопасности

разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем

реализовывать политику безопасности компьютерной сети

применять современные технологии проектирования автоматизированных систем в защищенном исполнении

осуществлять поиск, анализ основных нормативно-правовых актов, руководящих и методических документов, регламентирующих процессы создания и эксплуатации АСЗИ для конкретного предприятия

и владеть:

навыками анализа основных узлов и устройств современных автоматизированных систем

навыками использования методов и технологий проектирования и моделирования автоматизированных систем и подсистем безопасности автоматизированных систем

навыками проектирования разработке компонентов автоматизированных систем с использованием средств автоматизации;

навыками разработки политик информационной безопасности автоматизированных систем

методами управления информационной безопасностью автоматизированных систем

методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем

навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем;

навыками применения нормативно правовых актов и стандартов при проведении работ по сертификации средств защиты автоматизированных систем

навыками применения нормативно правовых актов и стандартов при проведении работ по аттестации автоматизированных систем

методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем

навыками разработки и реализации управленческих решений в сфере профессиональной деятельности

методами организации и управления деятельностью служб защиты информации на предприятии

методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем

навыком формирования политики информационной безопасности организации

навыками применения современных технологий проектирования автоматизированных систем в защищенном исполнении

навыками применения нормативных правовых акты, руководящих и методических документов, регламентирующих процессы создания и эксплуатации автоматизированных систем в защищенном исполнении для конкретного предприятия