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.5.3 Производственная практика (эксплуатационная)

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

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 3
всего часов – 108
зачет с оценкой – 8 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 (эксплуатационной) практики** в 8 семестре является закрепление теоретических знания, полученные по дисциплинам 6-7 семестров, а также формирование следующих компетенций:

(ПК-29) способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;

(ПК-30) способностью организовать эксплуатацию автоматизированной системы с учетом требований информационной безопасности

(ПК-32) способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем с целью определения информационно-технологических ресурсов, подлежащих защите;

(ПК-34) способностью формировать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы

(ПК-35) способность обеспечивать эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;

(ПК-36) способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы;

(ПК-37) способность администрировать подсистему информационной безопасности автоматизированной системы;

(ПК-38) способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы;

(ПК-39) Способность управлять информационной безопасностью автоматизированной системы.

(ПК-40) способностью обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций

В результате прохождения практики студент должен:

знать:

- автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем
- Методы анализа особенностей деятельности организации и использования в ней автоматизированных систем
- правила, процедуры, практические приемы, руководящие принципы, методы, средства формирования комплекс мер для обеспечения информационной безопасности автоматизированной системы
- Принципы функционирования информационно-технологических ресурсов автоматизированной системы
- Принципы функционирования и структуру средств защиты информационно-технологических ресурсов автоматизированной системы
- Общие принципы администрирования подсистему информационной безопасности автоматизированной системы
- Методы мониторинга безопасности автоматизированной системы
- основные меры по защите информации в автоматизированных системах
- методы, способы и средства обеспечения отказоустойчивости автоматизированных систем
-

уметь

- проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы

- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем
- проводить анализ информационной структуры организации
- Применять правила, процедуры, практические приемы, руководящие принципы, методы, средства формирования комплекс мер для обеспечения информационной безопасности автоматизированной системы в практической деятельности
- эффективно применять информационно-технологические ресурсы автоматизированной системы с учетом требований информационной безопасности
- эффективно применять средств защиты информационно-технологических ресурсов автоматизированной системы
- администрировать подсистему информационной безопасности автоматизированной системы
- Проводить мониторинг безопасности автоматизированной системы
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем
- восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях

владеть:

- навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем
- навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем
- навыками использования программно-аппартаных средств для анализа информационной структуры организации
- навыками формирования комплекс мер для обеспечения информационной безопасности автоматизированной системы
- Навыком применения информационно-технологических ресурсов автоматизированной системы в практической деятельности
- навыком эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы
- навыком администрирования подсистемы информационной безопасности автоматизированной системы
- методами и средствами выявления угроз безопасности
- методами организации и управления деятельностью служб защиты информации на предприятии
- навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем