

**МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ТУЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

Институт прикладной математики и компьютерных наук
Кафедра «Информационная безопасность»

Утверждено на заседании кафедры
«Информационная безопасность»
«20» января 2023 г., протокол №5

Заведующий кафедрой ИБ

А.А.Сычугов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«Разработка и эксплуатация защищенных автоматизированных систем в защищенном исполнении»

основной профессиональной образовательной программы
высшего образования – программы специалитета
по специальности:

***10.05.03 Разработка автоматизированных систем в защищенном
исполнении***

с профилем:

Защищенные автоматизированные системы управления

Форма обучения: очная

Идентификационный номер образовательной программы: 100503-01-23

Тула 2023 год

ЛИСТ СОГЛАСОВАНИЯ
рабочей программы дисциплины (модуля)

Разработчик(и):

Баранов А.Н., доцент каф. ИБ, доцент, канд. техн., наук

(ФИО, должность, ученая степень, ученое звание)



(подпись)

1 Цель и задачи освоения учебной дисциплины (модуля)

Целью освоения дисциплины (модуля) «Разработка и эксплуатация защищенных автоматизированных систем» является формирование теоретической и практической подготовки специалистов в области проектирования и кодирования автоматизированных систем, а также организации их защиты на программном (программно-аппаратном), техническом и организационном уровнях.

Задачами освоения дисциплины (модуля) являются:

- изучение стандартов, применимых для проектирования автоматизированных систем;
- получение практических навыков разработки входной документации при разработке автоматизированных систем;
- изучение принципов и получение практических навыков определения класса (уровня) защищенности автоматизированных систем;
- изучение принципов и получение практических навыков выбора средств защиты разрабатываемых (внедряемых) автоматизированных систем.

2 Место учебной дисциплины (модуля) в структуре основной профессиональной образовательной программы

Дисциплина (модуль) относится к вариативной части основной профессиональной образовательной программы.

Дисциплина (модуль) изучается в восьмом семестре.

3 Перечень планируемых результатов обучения по дисциплине (модулю)

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы (формируемыми компетенциями), установленными в общей характеристике основной профессиональной образовательной программы, приведён ниже.

В результате изучения дисциплины обучающийся должен:

Знать:

- критерии целесообразности создания автоматизированной системы в защищенном исполнении (ОПК-8.1.1);
- как обеспечивать разработку проектных и организационных решений системы защиты информации автоматизированной системы в защищенном исполнении (ОПК-8.2.1);
- как организовывать и обеспечивать информационную безопасность процесса создания автоматизированной системы в защищенном исполнении (ОПК-8.3.1).

Уметь:

- обосновывать целесообразность создания автоматизированной системы в защищенном исполнении и формировать исходные требования к этой системе, процессу ее создания и эксплуатации (ОПК-8.1.2);
- обеспечивать и осуществлять разработку проектных и организационных решений, документировать системы защиты информации автоматизированной системы в защищенном исполнении (ОПК-8.2.2);
- организовывать и обеспечивать информационную безопасность процесса создания автоматизированной системы в защищенном исполнении (ОПК-8.3.2).

Владеть:

- методикой формирования исходных требований к автоматизированной системе в защищенном исполнении, процессу ее создания и эксплуатации (ОПК-8.1.3);

- методикой обеспечения и осуществления разработки проектных и организационных решений, документирования системы защиты информации автоматизированной системы в защищенном исполнении (ОПК-8.2.3);

- методикой организации и обеспечения информационной безопасности процесса создания автоматизированной системы в защищенном исполнении (ОПК-8.3.3).

4 Содержание и структура учебной дисциплины (модуля)

4.1 Объем дисциплины (модуля), объем контактной и самостоятельной работы обучающегося при освоении дисциплины (модуля), формы промежуточной аттестации по дисциплине (модулю)

Номер семестра	Формы промежуточной аттестации	Общий объем в зачетных единицах	Общий объем в академических часах	Объем контактной работы в академических часах						Объем самостоятельной работы в академических часах
				Лекционные занятия	Практические (семинарские) занятия	Лабораторные работы	Клинические практические занятия	Консультации	Промежуточная аттестация	
Очная форма обучения										
8	Э	4	144	32	-	32	-	2	0,25	77,75
Итого	—	4	144	32	-	32	-	2	0,25	77,75

Условные сокращения: Э – экзамен, ЗЧ – зачет, ДЗ – дифференцированный зачет (зачет с оценкой), КП – защита курсового проекта, КР – защита курсовой работы.

4.2 Содержание лекционных занятий

Очная форма обучения

№ п/п	Темы лекционных занятий
1.	Основы разработки автоматизированных систем в защищенном исполнении (АСЗИ)
1.1.	Понятие АС
1.2.	Понятие АСЗИ
1.3.	Общие сведения о проектировании, разработке и защите АС
2.	Терминология в области разработки и защиты АС
2.1.	Термины и определения
2.2.	Общепринятые сокращения
3.	Документы при разработке защищенных АС
3.1.	Федеральные законы
3.2.	Постановления правительства
3.3.	Приказы органов исполнительной власти
3.4.	Международные стандарты
3.5.	ГОСТы
4.	Содержание и порядок выполнения работ на стадиях и этапах создания АСЗИ
4.1	Комплекс работ при создании АСЗИ

4.2.	Требования к системе защиты АС
5.	Стадии создания АСЗИ
5.1.	Эскизный проект
5.2.	Техническое задание (ТЗ)
5.2.1.	Общие положения о процессе разработке ТЗ
5.2.2.	Состав и содержание ТЗ
5.2.3.	Правила оформления ТЗ
5.2.4.	Порядок разработки, согласования и утверждения ТЗ на АС
5.2.5.	Оформление титульного и последнего листов ТЗ
5.3.	Рабочая документация
5.4.	Проектирование АС
5.4.1.	Стандарты в области проектирования АС
5.4.2.	Автоматизация в сфере проектирования АС
5.4.3.	Стандарты группы IDF0- IDF14
6.	Содержание и порядок выполнения работ по защите информации о создаваемой АС в защищенном исполнении (АСЗИ)
6.1.	Разработка замысла ЗИ о создаваемой (модернизируемой) АС
6.2.	Определение защищаемой информации о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания
6.3.	Определение и технико-экономическое обоснование организационных и технических мероприятий, которые необходимо проводить в интересах ЗИ о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания
6.4.	Обоснование, разработка и/или закупка средств, необходимых для ЗИ о создаваемой (модернизируемой) АСЗИ
6.5.	Обоснование и разработка мероприятий по контролю состояния ЗИ о создаваемой (модернизируемой) АСЗИ на различных стадиях ее создания
6.6.	Разработка документов, регламентирующих организацию и осуществление ЗИ о создаваемой (модернизируемой) АСЗИ
7.	Разработка АС
8.	Внедрение защищенной АС
8.1.	Испытание и прием АС
8.2.	Тестирование АС
8.3.	Сертификация АС
8.4.	Ввод в действие АС
8.5.	Адаптация АС
8.6.	Адаптация персонала при работе с АС
9.	Эксплуатация АСЗИ
9.1.	Техническое обеспечение защиты помещений
9.2.	Программно-аппаратное обеспечение защиты помещений
9.3.	Организационное обеспечение защиты помещений

4.3 Содержание практических (семинарских) занятий

Занятия указанного типа не предусмотрены основной профессиональной образовательной программой.

4.4 Содержание лабораторных работ

№ п/п	Наименование лабораторных работ
<i>8 семестр</i>	
1	Разработка документа Задание на создание автоматизированной системы в за-

№ п/п	Наименование лабораторных работ
	щищенном исполнении (по выбранной предметной области проектирования и защиты АС)
2	Разработка функциональной модели автоматизированной системы в защищенном исполнении (по выбранной предметной области)
3	Разработка проекта защиты информации, обрабатываемой в АС (по выбранной предметной области)
4	Разработка проекта автоматизированной системы в соответствии со стандартом IDF0 (по выбранной предметной области)
5	Разработка документа Техническое задание (по выбранной предметной области)
6	Кодирование, тестирование и отладка АС ЗИ (по выбранной предметной области)

4.5 Содержание клинических практических занятий

Занятия указанного типа не предусмотрены основной профессиональной образовательной программой.

4.6 Самостоятельная работа студента

№ п/п	Виды и формы самостоятельной работы
<i>Очная форма</i>	
<i>8 семестр</i>	
1	Изучение дополнительного материала, законов, постановлений, приказов
2	Подготовка к лабораторным занятиям, оформление отчетов к лабораторным занятиям
3	Подготовка к промежуточной аттестации и ее прохождение

5 Система формирования оценки результатов обучения по дисциплине (модулю) в рамках текущего контроля успеваемости и промежуточной аттестации обучающегося

Очная форма обучения

Мероприятия текущего контроля успеваемости и промежуточной аттестации обучающегося			Максимальное количество баллов
<i>8 семестр</i>			
Текущий контроль успеваемости	Первый рубежный контроль	Оцениваемая учебная деятельность обучающегося:	
		Посещение лекционных занятий	15
		Выполнение лабораторной работы №1	5
		Выполнение лабораторной работы №2	5
		Выполнение лабораторной работы №3	5
		Итого	30
	Второй рубежный контроль	Оцениваемая учебная деятельность обучающегося:	
		Посещение лекционных занятий	15
		Выполнение лабораторной работы №4	5
		Выполнение лабораторной работы №5	5
		Выполнение лабораторной работы №6	5
		Итого	30

Мероприятия текущего контроля успеваемости и промежуточной аттестации обучающегося		Максимальное количество баллов
Промежуточная аттестация	Экзамен	40 (100*)

* В случае отказа обучающегося от результатов текущего контроля успеваемости

Шкала соответствия оценок в стобальной и академической системах оценивания результатов обучения по дисциплине (модулю)

Система оценивания результатов обучения	Оценки			
	0 – 39	40 – 60	61 – 80	81 – 100
Стобальная система оценивания				
Академическая система оценивания (экзамен, дифференцированный зачет, защита курсового проекта, защита курсовой работы)	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Академическая система оценивания (зачет)	Не зачтено	Зачтено		

6 Описание материально-технической базы (включая оборудование и технические средства обучения), необходимой для осуществления образовательного процесса по дисциплине (модулю)

6.1 Требования к аудиториям (помещениям, местам) для проведения занятий

Для осуществления образовательного процесса по дисциплине (модулю) требуется: для проведения лекционных занятий по дисциплине требуется стандартная аудитория, оснащенная доской, или аудитория, оснащенная видеопроектором, настенным экраном, ноутбуком.

Компьютерный класс должен быть оснащен операционными системами Windows/ Linux, офисным пакетом (MS Office, Open Office, Libro Office, МойОфис.), должна быть установлена среда разработки программного обеспечения на языке Object Pascal (Lazarus) или среда разработки программного обеспечения на языке Python (IDLE) или среда разработки программного обеспечения на языке C, C++ (Visual Studio, QT-creator).

6.2 Требования к оборудованию рабочих мест преподавателя и обучающихся

Рабочее место преподавателя может быть оснащено видеопроектором, ноутбуком. Специализированное оборудование не требуется.

6.3 Требования к специализированному оборудованию

Локальная вычислительная сеть с выходом в Интернет.

7 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература

1. Малюк А. А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин. - М.: Горячая линия - Телеком, 2005. - 147 с.

2. Мельников, В. П. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - Москва: Мир, 2011. - 336 с.
3. Переездчиков, И. В. Анализ опасностей промышленных систем человек-машина-среда и основы защиты / И.В. Переездчиков. - М.: КноРус, 2011. - 784 с.
4. Северин, В. А. Комплексная защита информации на предприятии / В.А. Северин. - М.: Городец, 2008. - 368 с.
5. Соколов, А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. - М.: ДМК Пресс, 2002. - 656 с.

7.2 Дополнительная литература

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
3. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
5. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
6. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»;
7. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
8. - Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в системах персональных данных».
9. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
10. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
11. Приказ ФСТЭК России от 6.12.2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»
12. Приказ ФСТЭК России от 11.12. 2017 г. № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
13. Приказ ФСТЭК России от 21.12.2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»
14. Приказ ФСТЭК России от 22.12.2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»
15. Приказ ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
- 1 ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
16. ГОСТ 34.602-89. Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

7.3 Периодические издания

1. Мир ПК: журнал для пользователей персональных компьютеров. — М.: Открытые системы.
2. Калядин А.Ю. Использование масштабируемой архитектуры в АСУТП на промышленных предприятиях. Промышленные АСУ и контроллеры. 2001 №2
3. Норенков И.П., Автоматизированные системы управления технологическими процессами. Вестник МГТУ.
4. Программирование: журнал Российской академии наук. — М.: Наука, 2008 - 2016. — На рус. яз. - Выходит 6 раз в год. - Россия.
5. Мир ПК: журнал для пользователей персональных компьютеров. — М.: Открытые системы.
6. Информационные технологии: теоретический и прикладной научно-технический журнал. — М.: Новые технологии.
7. Наука и жизнь: научно-популярный журнал /учред. Автономная некоммерческая организация «Ред. журнала «Наука и жизнь» Computer. — IEEE Computer Society.
8. Журнал «Автоматизация и современные технологии». Индекс по каталогу «Роспечать» — 70537
9. Журнал «Вестник компьютерных и информационных технологий». Индекс по каталогу «Роспечать» — 84197

8 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Хабрахабр // Режим доступа: <http://habrahabr.ru/>, свободный. — Загл. с экрана.
2. Система ГАРАНТ, режим доступа <http://base.garant.ru>, свободный.- Загл. с экрана.

9 Перечень информационных технологий, необходимых для осуществления образовательного процесса по дисциплине (модулю)

9.1 Перечень необходимого ежегодно обновляемого лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. ОС Windows (Linux).
2. MS Office, Open Office, Libro Office, МойОфис.
3. Lazarus, IDLE, Visual Studio, QT-creator

9.2 Перечень необходимых современных профессиональных баз данных и информационных справочных систем

1. Электронный читальный зал «БИБЛИОТЕХ»: учебники авторов ТулГУ по всем дисциплин. нам. - Режим доступа: <https://tsutula.bibliotech.ru/>, по паролю.- Загл. с экрана
2. ЭБС IPRBooks универсальная базовая коллекция изданий. - Режим доступа: <http://www.iprbookshop.ru/>, по паролю.- Загл. с экрана
3. Научная Электронная Библиотека eLibrary - библиотека электронной периодики.- Режим доступа: <http://elibrary.ru/>, по паролю.- Загл. с экрана.
4. НЭБ КиберЛенинка научная электронная библиотека открытого доступа, режим доступа <http://cyberleninka.ru/>, свободный.- Загл. с экрана.