Энгельсский технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

Кафедра «Естественные и математические науки»

РАБОЧАЯ ПРОГРАММА

по дисциплине

Б.1.1.14 «Защита информации»

направления подготовки
09.03.01 «Информатика и вычислительная техника»

профиль
«Программное обеспечение средств вычислительной техники и автоматизированных систем»

Формы обучения: очная, заочная
Объем дисциплины:
в зачетных единицах: 5 з.е.
в академических часах: 180 ак.ч.

Энгельс 2024

Рабочая программа по дисциплине Б.1.1.14 «Защита информации» для направления подготовки 09.03.01 «Информатика и вычислительная техника», профиль: «Программное обеспечение средств вычислительной техники и автоматизированных систем» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования 09.03.01 «Информатика и вычислительная техника», утвержденным приказом Минобрнауки России № 929 от 19.09.2017 г. с изменениями внесенными приказом № 1456 от 26 11.2020 г.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры «Естественные и математические науки» от «07» июня 2024 г., протокол № 20.

Заведующий кафедрой _____/Жилина Е.В./
подпись Ф.И.О.

одобрена на заседании УМКН от «20» июня 2024 г., протокол № 5.

Председатель УМКН /Жилина Е.В./

1. Цели и задачи освоения дисциплины

Целью преподавания дисциплины Б.1.1.14 «Защита информации» является изучение методов и средств защиты информации, исключающих несанкционированный доступ к информации, хранящейся и обрабатываемой в ЭВМ, обеспечение информационной безопасности организации, обеспечение комплексной защиты объектов информации от различных угроз.

Задачами изучения дисциплины являются:

- ознакомление с основными понятиями, источниками, рисками и формами атак на информацию, политикой и стандартами безопасности, составляющими ядро дисциплины «Защита информации»;
- исследование и использование криптографии и криптоанализа с помощью служебного, прикладного и инструментального программного обеспечения компьютера

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б.1.1.14 «Защита информации» относится к обязательной части Блока 1 «Дисциплины (модули)».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы:

Код и наименование компетенции (результат освоения)	Код и наименование индикатора достижения компетенции (составляющей компетенции)	Наименование показателя оценивания (результата обучения по дисциплине)
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных	**ИД-1** $_{\text{ОПК-3}}$ Решает задачи диагностики и настройки активного сетевого оборудования	**Знает:** принципы функционирования и устройство коммутаторов и маршрутизаторов; принцип многоуровневого функционирования компьютерных сетей на основе модели OSI; различные версии протокола Ethernet; алгоритмы функционирования протокола 802.1Q, STP, VTP; протокол IP, классы адресов, принципы расчета подсетей;

технологий и с учетом основных требований информационной безопасности		технологии передачи данных по различным физическим средам передачи; особенности протоколов транспортного уровня TCP и UDP. **Умеет:** выполнять установку и настройку сетевого интерфейса персонального компьютера; проектировать и создавать локальные компьютерные сети организаций, включая соединение с Интернет; выявлять и устранять неисправности локальных компьютерных сетей организаций, включая неисправности соединения с Интернет. **Владеет**: навыками установки и настройки сетевого интерфейса персонального компьютера; навыками проектирования и создания локальных компьютерных сетей организаций, включая соединение с Интернет; навыками диагностики и устранения неисправностей локальных компьютерных сетей организаций, включая неисправности соединения с Интернет.

4. Объем дисциплины и виды учебной работы

очная форма обучения

Вид учебной деятельности	ак.часов		
	Всего	по семестрам	
		6 семестр	7 семестр
1. Аудиторные занятия, часов всего, в том числе:	80	32	48
• занятия лекционного типа,	32	16	16
• занятия семинарского типа:	-	-	-
практические занятия	48	16	32
лабораторные занятия	-	-	
в том числе занятия в форме практической подготовки	-	-	-
2. Самостоятельная работа студентов, всего	100	40	60
– курсовая работа (проект)	-	-	-
– расчетно-графическая работа	-	-	-
3.Промежуточная аттестация: *экзамен, зачет с оценкой, зачет*		*зачет*	*экзамен*
Объем дисциплины в зачетных единицах	5	2	3
Объем дисциплины в акад. часах	180	72	108

заочная форма обучения

Вид учебной деятельности		Заочная форма обучения (акад. часов)		
		Всего	по семестрам	
			8 семестр	9 семестр
1. Аудиторные занятия, часов всего, в том числе:		20		
• занятия лекционного типа,		6	6	8
• занятия семинарского типа:		-	-	-
практические занятия		6	4	8
лабораторные занятия		-		-
в том числе занятия в форме практической подготовки		-		-
2. Самостоятельная работа студентов, всего		96	62	92
– курсовая работа (проект)		-	-	-
– расчетно-графическая работа		-	-	-
– контрольная работа			+	+
3.Промежуточная аттестация: *экзамен, зачет с оценкой, зачет*			*зачет*	*экзамен*
ИТОГО:	ак.часов	108	72	108
Общая трудоемкость	зач. ед.	3	2	3

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

6 семестр

Тема 1. Введение в предмет.

Предмет защиты (информация – определение, свойства: важность, ценность; жизненный цикл, виды и формы представления)

Тема 2. Основные понятия информационной безопасности.

Документы, регламентирующие деятельность по ее обеспечению; задачи информационной безопасности; классификация методов защиты; методы, лежащие в основе атак, и каналы утечки информации.

Тема 3. Средства защиты от несанкционированного доступа.

Обзор рынка программно-аппаратных комплексов защиты информации.

7 семестр

Тема 4. Технические аспекты обеспечения информационной безопасности вычислительных систем.

Излучения ПЭВМ, параметры информационно-опасных сигналов, экранирование каналов утечек информации,
экранирование помещений.

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в акад.часах)			Код индикатора достижения компетенции
		занятия лекционного типа	Практические занятия / из них в форме практической подготовки	самос–тоятельная работа	
	6 семестр				
1	Тема 1. Введение в предмет	2	8/-	8	ИД-1 $_{ОПК-3}$
2	Тема 2. Основные понятия информационной безопасности.	8	6/-	4	ИД-1 $_{ОПК-3}$
3	Тема 3. Средства защиты от несанкционированного доступа.	6	2/-	26	ИД-1 $_{ОПК-3}$
	Всего за 6 семестр	**16**	**16/-**	**40**	
	7 семестр				
4	Тема 4. Технические аспекты обеспечения информационной безопасности вычислительных систем.	16	32/-	24	ИД-1 $_{ОПК-3}$
5	Подготовка к экзамену	-	-	36	ИД-1 $_{ОПК-3}$
	Всего за 7 семестр	**16**	**32/-**	**60**	
	Итого:	**32**	**48/-**	**100**	

заочная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в акад.часах)			Код индикатора достижения компетенции
		занятия лекционного типа	Практические занятия / из них в форме практической подготовки	самос–тоятельная работа	
	6 семестр				
1	Тема 1. Введение в предмет	2	2/-	10	ИД-1 $_{ОПК-3}$
2	Тема 2. Основные понятия информационной безопасности.	2	2/-	12	ИД-1 $_{ОПК-3}$
3	Тема 3. Средства защиты от несанкционированного доступа.	2	-	20	ИД-1 $_{ОПК-3}$

4	Выполнение контрольной работы	-	-	20	ИД-1 $_{ОПК-3}$
	Всего за 6 семестр	**6**	**4/-**	**62**	
	7 семестр				
5	Тема 4. Технические аспекты обеспечения информационной безопасности вычислительных систем.	8	8/-	36	ИД-1 $_{ОПК-3}$
6	Выполнение контрольной работы	-	-	20	ИД-1 $_{ОПК-3}$
7	Подготовка к экзамену	-	-	36	ИД-1 $_{ОПК-3}$
	Всего за 7 семестр	**8**	**8/-**	**92**	
	Итого:	**32**	**48/-**	**100**	

5.2. Перечень практических занятий

№ п/п	Наименование раздела, темы дисциплины	Наименование практического занятия	Объем дисциплины в акад. часах		
			очная форма обучения	очно-заочная форма обучения	заочная форма обучения
1.	Тема 1. Введение в предмет	Основы криптографии: понятия, методы шифрования: -шифр Цезаря, - шифр Виженера, - алгоритм простой вертикальной перестановки, - алгоритм одиночной перестановки, - алгоритм двойных перестановок, - метод магического квадрата, - метод Полибианского квадрата, - многоалфавитная замена, метод Кардано для квадрата и прямоугольника.	8	-	2
2.	Тема 2. Основные понятия информационной безопасности.	Элементы криптоанализа: элементы частотности символов в тексте.	6	-	2
3.	Тема 3. Средства защиты от несанкционированного доступа.	Компьютерные алгоритмы шифрования: RSA, DES и др.	2	-	-
	Всего за 6 семестр		**16**	**-**	**4**

4.	Тема 4. Технические аспекты обеспечения информационной безопасности вычислительных систем	Слабости парольных защит	16	-	4
		Количественная оценка стойкости парольных защит	16	-	4
	Всего за 7 семестр		**32**	**-**	**8**
	Итого:		**48**	**-**	**12**

5.3. Перечень лабораторных работ

Лабораторные работы не предусмотрены.

5.4. Задания для самостоятельной работы студентов

№ п/п	Наименование раздела, темы дисциплины	Задания, вопросы, для самостоятельного изучения (задания)	Объем дисциплины в акад. часах		
			очная форма обучения	очно-заочная форма обучения	заочная форма обучения
1	Тема 1. Введение в предмет	Изучение изменений нормативно-правовой базы по обеспечению защиты информации от несанкционированного доступа	8	-	10
2	Тема 2. Основные понятия информационной безопасности.	Средства защиты от несанкционированного доступа: обзор рынка современных программно-аппаратных комплексов средств защиты от несанкционированного доступа	4	-	12
3	Тема 3. Средства защиты от несанкционированного доступа.	Криптография (изучение методов шифрования, не входящих в перечень шифров, входящих в лабораторные работы)	26	-	20
4	Выполнение контрольной работы		-	-	20
	Всего за 6 семестр		**40**	**-**	**62**
5	Тема 4. Технические аспекты обеспечения информационной безопасности вычислительных систем	Обзор рынка современных средств обеспечения экранирования персональных ЭВМ и систем	24	-	36
6	Выполнение контрольной работы		-	-	20
7	Подготовка к экзамену		36	-	36
	Всего за 7 семестр		**60**	**-**	**92**
	Итого:		**100**	**-**	**154**

6. Расчетно-графическая работа

Расчетно-графическая работа не предусмотрена.

7. Курсовая работа

Курсовая работа не предусмотрена.

8. Курсовой проект

Курсовой проект не предусмотрен.

9. Контрольная работа

Контрольная работа предусмотрена в 8 и 9 семестрах для студентов заочной формы обучения.

Контрольная работа выполняется по вариантам и заключается в описании алгоритма или метода шифрования. Отчет должен содержать информацию о предпосылках и истории появления, принцип работы, сильные и слабы стороны, области применения алгоритма или метода. При необходимости текст сопровождается иллюстрациями, блок-схемами, таблицами.

10. Оценочные средства для проведения текущего контроля и промежуточной аттестации

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с Фондом оценочных средств.

Вопросы к зачету:

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
2. Определение информационной безопасности.
3. Функции и объекты защиты информации.
4. Степени секретности информации.
5. Субъекты и причины совершения компьютерных преступлений.
6. Уровни информационной защиты.
7. Ответственность за нарушение информационной безопасности.
8. Принципы информационной безопасности.
9. Определение конфиденциальности, целостности, доступности информации.
10. Предмет криптографии. Определения. Задачи. Исторические примеры.
11. Виды атак на криптографические алгоритмы. Понятие стойкости.
12. Классификация алгоритмов шифрования. Примеры простейших шифров.
13. Шифры замены.
14. Шифры перестановки.
15. Шифры гаммирования.
16. Проблемы и особенности защиты информации в компьютерных сетях.
17. Виды угроз информационной безопасности. Основные нарушения.
18. Характер происхождения угроз.

19. Источники угроз (непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию).
20. Классы каналов несанкционированного получения информации.
21. Классификация методов и средств обеспечения безопасности
22. Методы обеспечения безопасности сетей
23. Понятие актуальности угрозы безопасности.
24. Понятие модели угроз. Этапы проведения оценки угроз безопасности.
25. Основные нормативные документы, необходимые для составления модели угроз.
26. Понятие нарушителя. Типы нарушителей, их возможности и цели (по методическому документу ФСТЭК «Методика оценки угроз безопасности информации» от 05.02.2021).
27. Определение средств защиты информации (СЗИ).
28. Классификация средств защиты информации.
29. Инженерно-техническая защита информации.
30. Физические средства защиты.
31. Аппаратные средства защиты.
32. Программные средства защиты.
33. Криптографические средства защиты информации.
34. Встроенные средства защиты операционных систем (ОС).
35. Идентификация и аутентификация.
36. Управление доступом.
37. Протоколирование и аудит.
38. Антивирусная защита. Методы антивирусной защиты. Виды антивирусных программ.
39. Межсетевые экраны. Основные компоненты и технологии.
40. Недостатки, связанные с применением межсетевого экрана.
41. VPN. Классификация VPN сетей.
42. Принципы построения VPN сетей. VPN на базе брэндмауэров, VPN на базе маршрутизаторов, VPN на базе программного обеспечения. VPN на базе аппаратных средств.
43. Протоколы VPN сетей. Методы реализацииVPN сетей (туннелирование, аутентификация, шифрования).
44. Определение прокси-сервера. Цели применения прокси-сервера. Виды прокси-серверов.
45. Система обнаружения вторжений (IDS). Классификация IDS.
46. Архитектура IDS.
47. Перечислить основные элементы локальной архитектуры систем обнаружения вторжений.
48. Глобальная архитектура систем обнаружения вторжений.
49. Система предотвращения вторжений.
50. Перечислить цели использования IPS-систем.
51. Классификация IPS-систем.
52. Криптографические средства защиты информации.
53. Перечислить требования, предъявляемые к криптосистемам.

54. Раскрыть понятие «электронная подпись».

11. Учебно-методическое обеспечение дисциплины

11.1. Рекомендуемая литература

1. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. — Москва : СОЛОН-Пресс, 2016. — 256 с. — ISBN 5-98003-002-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/90248.html. — Режим доступа: для авторизир. пользователей

2. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий: учебное пособие / А. Б. Арзуманян. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 140 с. — ISBN 978-5-9275-3546-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/107955.html. — Режим доступа: для авторизир. пользователей

3. Брюхомицкий, Ю. А. Безопасность информационных технологий. В 2 частях. Ч.1 : учебное пособие / Ю. А. Брюхомицкий. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 171 с. — ISBN 978-5-9275-3571-2 (ч.1), 978-5-9275-3526-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/107943.html. — Режим доступа: для авторизир. Пользователей

4. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/108227.html . — Режим доступа: для авторизир. Пользователей

5. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с. — ISBN 978-5-4497-1653-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/120489.html . — Режим доступа: для авторизир. пользователей

11.2. Периодические издания

1. Вопросы защиты информации: научно-практический журнал / Федеральное государственное унитарное предприятие "Научно-технический центр оборонного комплекса "Компас". – 1974 - . - Выходит 4 раза в год. — ISSN 2073-2600. - URL: http://izdat.ntckompas.ru/editions/detail.php?SECTION_ID=155

2. Программные продукты и системы: научно-практический журнал /

учредитель Куприянов В.П. : главный редактор журнала Савин Г.И. – 1988 - . — Выходит 4 раза в год. — ISSN 0236-235X. — URL: https://www.iprbookshop.ru/25852.html. — Текст: электронный.

11.3. Нормативно-правовые акты и иные правовые документы

1. ГОСТ Р 50922-2007 Защита информации. Термины и определения.
2. ГОСТ Р 51275-2007 Защита информации. Объекты информатизации. Факторы, воздействующие на информацию. Общие положения.
3. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения.
4. ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищённом исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям.

11.4 Перечень электронно-образовательных ресурсов

1. Учебно-методические материалы по дисциплине «Защита информации» (электронный образовательный ресурс размещен в ИОС ЭТИ (филиал) СГТУ имени Гагарина Ю.А.

http://techn.sstu.ru/new/SubjectFGOS/Default.aspx?kod=814

2. Сайт ЭТИ (филиал) СГТУ имени Гагарина Ю.А. http://techn.sstu.ru/

11.5 Электронно-библиотечные системы

1. «ЭБС IPR SMART»,
2. «ЭБС elibrary»
3. ЭБС «КОНСУЛЬТАНТ СТУДЕНТА»

11.6. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Средства защиты информации - Secret Net.htm. https://www.securitycode.ru/products/secret-net-studio/
2. Электронный замок «Соболь» https://www.polikom.ru/

11.7. Печатные и электронные образовательные ресурсы в формах, адаптированных для студентов с ограниченными возможностями здоровья (для групп и потоков с такими студентами)

1. Адаптированная версия НЭБ, для использования инвалидами и лицами с ограниченными возможностями здоровья

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

12. Информационно-справочные системы и профессиональные базы данных

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных

технологий, к современным профессиональным базам данных и информационным справочным системам.

12.1 Перечень информационно-справочных систем

Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс» Docs.cntd.ru

12.2 Перечень профессиональных баз данных

не используются

12.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения

Образовательный процесс по дисциплине обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (подлежит обновлению при необходимости).

1) Лицензионное программное обеспечение

Microsoft Windows10, Microsoft Office 2010 (Word, Excel, PowerPoint), Matlab, SimInTech.

2) Свободно распространяемое программное обеспечение

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной системе и электронной информационно-образовательной среде.

13. Материально-техническое обеспечение

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебные аудитории оснащенны оборудованием и техническими средствами обучения, которые включают в себя учебную мебель, комплект мультимедийного оборудования, в том числе переносного (проектор, экран).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ЭТИ (филиал) СГТУ имени Гагарина Ю.А.

Рабочую программу составил
доцент кафедры ЕМН  /Ершов А.С./

14. Дополнения и изменения в рабочей программе

Рабочая программа пересмотрена на заседании кафедры
«____»_____ 20 ___ года, протокол № _____

Зав. кафедрой _____/_____/

Внесенные изменения утверждены на заседании УМКС/УМКН
«_____»_____ 20 __ года, протокол № ____
Председатель УМКС/УМКН _____/_____/