

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»

для направления подготовки

09.03.04 «Программная инженерия» профиль «Управление разработкой программных проектов».

форма обучения – очная

курс – 3,4

семестр – 6,7

зачетных единиц – 5 (2,3)

часов в неделю – 2,3

всего часов – 180 (72, 108)

в том числе:

лекции – 32 (16,16)

практические занятия – 48 (16,32)

лабораторные занятия – нет

самостоятельная работа – 100 (40,60)

зачет – 6 семестр

экзамен – 7 семестр

РГР – нет

курсовая работа – нет

курсовой проект – нет

Рабочая программа обсуждена на заседании кафедры ЕМН
«27» июня 2022 года, протокол № 9

Заведующий кафедрой  /Жилина Е.В./

Рабочая программа обсуждена на УМКН ИВЧТ
«27» июня 2022 года, протокол № 5

Председатель УМКН  /Жилина Е.В./

1. Цели и задачи освоения дисциплины

Целями преподавания дисциплины Б.1.1.14 «Защита информации» являются 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 учебного плана ОПОП ВО (бакалавриат) направления подготовки 09.03.04 «Программная инженерия» профиль «Управление разработкой программных проектов».

Для ее изучения необходимы знания, умения и компетенции, формируемые следующими дисциплинами: «Математика», «Вычислительная математика», «Информатика», «ЭВМ и периферийные устройства», «Операционные системы», «Сети и телекоммуникации» и «Программирование».

Полученные знания, умения и навыки могут быть использованы студентами при изучении дисциплин «Принципы и технологии создания электронных образовательных ресурсов», «Среды инженерного проектирования и вычислительного моделирования», при прохождении производственной практики, подготовке курсовых проектов (работ) и выпускной квалификационной работы.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций:

ОПК-2 - способен понимать принципы работы современных информационных технологий и программные средства, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности

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

В результате освоения дисциплины студент должен:

3.1. Знать: основные информационные системы и информационно-коммуникационные технологии управления бизнесом; принципы построения и архитектуру вычислительных систем; рынки программно-информационных продуктов и услуг; виды контента информационных ресурсов предприятия и Интернет-ресурсов; процессы управления жизненным циклом цифрового контента, процессы создания и использования информационных сервисов (контент-сервисов), а также современные технические и программные средства взаимодействия с ЭВМ; методы и средства обеспечения информационной безопасности компьютерных систем

3.2. Уметь проектировать, внедрять в организации эксплуатацию информационных систем и информационно-коммуникационных технологий; управлять процессами жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами создания и использования информационных сервисов (контент-сервисов)% работать с

современными системами программирования, включая объектно-ориентированные для реализации криптографических алгоритмов.

3.3. Владеть навыками работы с различными операционными системами и их администрирования, навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств; методами и инструментальными средствами разработки программ; методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия.

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

3 Код и наименование компетенции 4 (результат освоения)	Код и наименование индикатора достижения компетенции (составляющей компетенции)
ОПК-2 Способен понимать принципы работы современных информационных технологий и программные средства, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ИД-1 _{ОПК-2} Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
	ИД-2 _{ОПК-2} Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
	ИД-3 _{ОПК-2} Имеет навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
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	ИД-1 _{ОПК-3} Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ИД-2 _{ОПК-3} Умеет решать стандартны задачи профессионально деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности.
	ИД-3 _{ОПК-3} Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ИД-1 _{ОПК-2} Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной	Знает основные информационные системы и информационно-коммуникационные технологии управления бизнесом; принципы построения и архитектуру вычислительных систем; рынки программно-информационных продуктов и услуг; виды контента информационных ресурсов предприятия и

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
деятельности.	Интернет-ресурсов.
ИД-2 _{ОПК-2} Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	Умеет проектировать, внедрять в организации эксплуатацию информационных систем и информационно-коммуникационные технологий; управлять процессами жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами создания и использования информационных сервисов (контент-сервисов)
ИД-3 _{ОПК-2} Имеет навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Владеет навыками работы с различными операционными системами и их администрирования, навыками конфигурирования локальных сетей, реализации сетевых протоколов с помощью программных средств.
ИД-1 _{ОПК-3} Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знает процессы управления жизненным циклом цифрового контента, процессы создания и использования информационных сервисов (контент-сервисов), а также современные технические и программные средства взаимодействия с ЭВМ; методы и средства обеспечения информационной безопасности компьютерных систем.
ИД-2 _{ОПК-3} Умеет решать стандартные задачи профессионально деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Умеет работать с современными системами программирования, включая объектно-ориентированные для реализации криптографических алгоритмов.
ИД-3 _{ОПК-3} Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Владеет методами и инструментальными средствами разработки программ; методами проектирования, разработки и реализации технического решения в области создания систем управления контентом Интернет-ресурсов и систем управления контентом предприятия

4. Распределение трудоемкости (час) дисциплины по темам и видам занятий

№ модуля	№ темы	Наименование темы	Часы					СРС
			все-го	лек-ции	кол-лок-виу-мы	лабо-ра-тор-ные	прак-ти-чес-кие	
6 семестр								
1	1	Введение в предмет.	4	2	-	-	-	2
1	2	Основные понятия информационной безопасности.	16	8	-	-	-	8
1	3	Средства защиты от несанкционированного доступа	10	6	-	-	-	4
2	4	Криптография	42	-	-	-	16	26
Итого:			72	16	-	-	16	40
7 семестр								
1	1	Технические аспекты обеспечения информационной безопасности вычислительных систем	108	16	-	-	32	60
Итого:			108	16	-	-	32	60
Всего:			180	32	-	-	48	100

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1			4	5
6 семестр				
1	2	1	Введение в предмет. Предмет защиты (информация – определение, свойства: важность, ценность; жизненный цикл, виды и формы представления)	3
2	8	2-5	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.	2-5
3	6	6-8	Средства защиты от несанкционированного доступа. Обзор рынка программно-аппаратных комплексов защиты информации.	3-5
7 семестр				

1	16	1-8	Технические аспекты обеспечения информационной безопасности вычислительных систем. Излучения ПЭВМ, параметры информационно-опасных сигналов, экранирование каналов утечек информации, экранирование помещений.	2-5
---	----	-----	--	-----

6. Содержание коллоквиумов

По данной дисциплине коллоквиумы не предусмотрены учебным планом.

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	3	4	5
6 семестр				
4	8	1-4	Основы криптографии: понятия, методы шифрования: <ul style="list-style-type: none"> - 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. 	1
	6	5-7	Элементы криптоанализа: элементы частотности символов в тексте.	1
	2	8	Компьютерные алгоритмы шифрования: RSA, DES и др.	1,3,4
7 семестр				
1	16	1-8	Слабости парольных защит	3-5
	16	9-16	Количественная оценка стойкости парольных защит	3-5

8. Перечень лабораторных работ

По данной дисциплине лабораторные работы не предусмотрены учебным планом

9. Задания для самостоятельной работы студентов

Самостоятельная работа осуществляется индивидуально и является обязательной, определяющей подготовку студента к текущим лекционным и практическим занятиям. Баллы, полученные студентом по результатам аудиторной работы, формируют рейтинговую оценку текущей успеваемости студента.

Для закрепления и систематизации знаний, обязательной самостоятельной работой является обработка лекции (дополнение) с помощью учебной литературы по дисциплине.

№ темы	Всего часов	Вопросы для самостоятельного изучения (задания)	Учебно-методическое обеспечение
6 семестр			
1	2	Введение в предмет	3
2	8	Изучение изменений нормативно-правовой базы по обеспечению защиты информации от несанкционированного доступа	2-5
3	4	Средства защиты от несанкционированного доступа: обзор рынка современных программно-аппаратных комплексов средств защиты от несанкционированного доступа	3-5
4	26	Криптография (изучение методов шифрования, не входящих в перечень шифров, входящих в лабораторные работы)	1
	40		
7 семестр			
1	60	Технические аспекты обеспечения информационной безопасности вычислительных систем: обзор рынка современных средств обеспечения экранирования персональных ЭВМ и систем	3-5
	60		

10. Расчетно-графическая работа (учебным планом не предусмотрена).

11. Курсовая работа (учебным планом не предусмотрена).

12. Курсовой проект (учебным планом не предусмотрен)

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

В процессе обучения студент должен полностью выполнить учебный план, предусмотренный в рабочей программе дисциплины, по всем видам учебных занятий и набрать 5 зачетных единиц трудоемкости.

В процессе освоения образовательной программы у студентов формируется следующие компетенции:

№ пп	Название компетенции	Составляющие действия компетенции	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
3	ОПК-2 Способен понимать принципы работы современных информационных технологий и программные средства, в том числе отечественного производства, и	Студент должен знать : основные понятия и средства информационной безопасности, методы, лежащие в основе атак несанкционированного доступа (НСД) Студент должен уметь : определить и применить оптимальные способы предотвращения НСД (в т.ч. криптографические)	Лекции, практические работы, СРС Лекции, практические работы, СРС	Тестирование, индивидуальные задания, зачет, экзамен Тестирование, индивидуальные задания

	использовать их при решении задач профессиональной	Студент должен владеть: навыками применения и создания прикладных программ по обеспечению защиты информации	Практические работы, зачет	Тестирование, индивидуальные задания
	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Студент должен знать: основные понятия и жизненный цикл цифрового контента, задачи защиты информации и документы регламентирующие их, способы обеспечения защиты информационно-коммуникационных технологий управления бизнесом. Студент должен уметь: ориентироваться в процессах жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами использования информационных сервисов (контент-сервисов) Студент должен владеть: навыками применения криптографических алгоритмов, способных обеспечить безопасность документов профессиональной деятельности	Лекции, практические работы, СРС Лекции, практические работы, СРС Практические работы	Тестирование, индивидуальные задания, зачет, экзамен Тестирование, индивидуальные задания Тестирование, индивидуальные задания

Уровни освоения компонент компетенции ОПК-2

Ступени уровней освоения компетенции	Отличительные признаки
1	2
Пороговый (удовлетворительный)	Знает: основные понятия и задачи информационной безопасности. Способы обеспечения защиты от несанкционированного доступа: общая классификация, технические методы, меры защиты в глобальных и региональных сетях. Умеет: использовать средства защиты информации, встроенные в операционные системы Владеет: навыками применения криптографических алгоритмов
Продвинутый (хорошо)	Знает: базовые понятия, средства защиты от несанкционированного доступа: системы парольной защиты, системы привязки к ПК, программно-аппаратные системы; модели основных криптографических атак. Умеет: выполнять анализ способов нарушения информационной безопасности. Владеет: навыками разработки приложений на основе криптографических алгоритмов.
Высокий (отлично)	Знает: базовые понятия, средства защиты от несанкционированного доступа: системы парольной защиты,

	<p>системы привязки к ПК, программно-аппаратные системы; модели основных криптографических атак и технические аспекты защиты информации.</p> <p>Умеет: определить оптимальный способ организации защиты данных на основании классификации типа информации.</p> <p>Собственности</p> <p>Владеет: навыками создания прикладных приложений по обеспечению информационной безопасности интеллектуальной собственности</p>
--	---

Уровни освоения компонент компетенции ОПК-3

Ступени уровней освоения компетенции	Отличительные признаки
1	2
<p>Пороговый (удовлетворительный)</p>	<p>Знает: основные понятия и жизненный цикл цифрового контента, задачи защиты информации и документы регламентирующие их, способы обеспечения защиты информационно-коммуникационных технологий управления бизнесом.</p> <p>Умеет: ориентироваться в процессах жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами использования информационных сервисов (контент-сервисов).</p> <p>Владеет: навыками применения криптографических алгоритмов, способных обеспечить безопасность документов профессиональной деятельности.</p>
<p>Продвинутый (хорошо)</p>	<p>Знает: понятия и документы, регламентирующие деятельность по обеспечению информационной безопасности, принципы построения и архитектуру вычислительных систем; рынки программно-информационных продуктов и услуг; виды контента информационных ресурсов предприятия и Интернет-ресурсов; средства защиты от несанкционированного доступа к ним.</p> <p>Умеет: ориентироваться в нормативно-правовых документах по защите информации в профессиональной сфере деятельности и управлять процессами жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами создания и использования информационных сервисов (контент-сервисов).</p> <p>Владеет : навыками применения нормативно-правовых регламентов при разработке приложений.</p>
<p>Высокий (отлично)</p>	<p>Знает: понятия и документы, регламентирующие деятельность по обеспечению защиты информации, средства защиты от несанкционированного доступа к информационным системам и информационно-коммуникационные технологиям управления бизнесом: системы парольной защиты, системы привязки к ПК, программно-аппаратные системы; модели основных криптографических атак и технические аспекты защиты информации.</p> <p>Умеет : анализировать соответствующую нормативно-правовую базу для определения оптимальных способов организации защиты данных на основании классификации типа информации.</p> <p>Владеет: навыками применения нормативно-правовых регламентов при создания прикладных приложений по обеспечению защиты интеллектуальной собственности</p>

Текущий контроль, зачет и экзамен по дисциплине выставляется на основании положительных результатов выполнения практических работ (дифференцированно оцененных преподавателем), а так же выполнение заданий, предназначенных для

самостоятельной работы студентов (в том числе, ответа на вопросы, предназначенные для самоконтроля знаний).

14. Образовательные технологии

В рамках учебного курса предусмотрено чтение лекций с применением мультимедийных технологий по всем модулям дисциплины, проведение практических работ, с разбором конкретных ситуаций связанных со спецификацией в форме деловой игры.

15. Перечень учебно-методического обеспечения для обучающихся по дисциплине

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

Программное обеспечение и Интернет-ресурсы

1. [http://www \Secret Net\ЭРИМЕКС_ Новосибирск Средства защиты информации - Secret Net.htm](http://www.SecretNet.ru).
2. [http://www \Комплекс ср_защ 'Гриф'\Институт компьютерных технологий - Защита информации в ПЭВМ.htm](http://www.complex-sp-zashchita-grif.ru).
3. [http://www \П-А комплекс 'Мастер паролей'\Программно-аппаратный комплекс «Мастер Паролей.htm](http://www.p-a-complex-master-paroley.ru).
4. [http://www \П-А комплекс 'Шипка'\ВНИИПВТИ - Программно-аппаратный комплекс средств защиты от несанкционированного доступа к информации ШИПКА.htm](http://www.p-a-complex-shipka.ru).
5. [http://www \Электр замок 'Соболь'\ЭРИМЕКС_ Новосибирск Средства защиты информации - Электронный замок Соболь.htm](http://www.electr-zamok-sobol.ru).

16. Материально-техническое обеспечение дисциплины (модуля):

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации по дисциплине «Защита информации» укомплектована специализированной мебелью и техническими средствами обучения: 20 столов, 40 стульев; рабочее место преподавателя; мультимедийная доска; проектор BENQ 631, системный блок (Atom2550/4Гб/500, клавиатура, мышь), подключенный в сеть с выходом в Интернет и доступом в информационно-образовательную среду ЭТИ (филиал) СГТУ имени Гагарина Ю.А., учебно-наглядные пособия, обеспечивающие тематические иллюстрации по рабочей программе дисциплины

Программное обеспечение: MicrosoftWindows 7, MicrosoftOffice 2010 (Word, Excel, PowerPoint), GoogleChrome, ПО для мультимедийной доски

Учебная аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля укомплектована специализированной мебелью и техническими средствами обучения: 12 столов, 12 стульев; рабочее место преподавателя; маркерная доска, 12 компьютеров (I 3/ 8 Гб/ 500), мониторы 24' BENQ, LG, Philips, клавиатура, мышь). Компьютеры объединены в локальную сеть с выходом в Интернет и доступом в информационно-образовательную среду ЭТИ (филиал) СГТУ имени Гагарина Ю.А., учебно-наглядные пособия, обеспечивающие тематические иллюстрации по рабочей программе дисциплины.

Программное обеспечение: Microsoft Windows 7, Microsoft Office 2010 (Word, Excel, PowerPoint), MSDN Academic Alliance (Visual Studio; Корпоративные серверы .NET: Windows Server, SQL Server, Exchange Server, Commerce Server, Biz Talk Server, HostIntegration Server, Application Center Server, Systems Management Server); GNU Privacy Guard, Sn1per Community edition, OWASP ZAP, информационно-справочная система «Гарант»; GoogleChrome.

Рабочую программу
составил
доцент кафедры ЕМН



/Ершов А.С./

17. 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 _____ / _____ /