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

09.03.01 «Информатика и вычислительная техника»

профиль «Программное обеспечение средств вычислительной техники и автоматизированных систем»

форма обучения – заочная
курс – 4,5
семестр – 8,9
зачетных единиц – 5 (2,3)
всего часов – 180 (72, 108)
в том числе:
лекции – 14 (6,8)
практические занятия – 12 (4,8)
лабораторные занятия – нет
самостоятельная работа – 154 (62,92)
зачет – 8 семестр
экзамен – 9 семестр
РГР – нет
курсовая работа – нет
курсовой проект – нет
контрольная работа – 8,9 семестры

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./

Энгельс 2022

## 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 09.03.01 «Информатика и вычислительная техника» профиль: «Программное обеспечение средств вычислительной техники и автоматизированных систем».

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-коммуникационные 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.

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

| № модуля | № темы | Наименование темы | Часы | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | всего | лекции | коллоквиумы | лабораторные | практические | СРС |
| **8 семестр** | | | | | | | | |
| 1 | 1 | Основные понятия информационной безопасности. | 12 | 2 | - | - | - | 10 |
| | 2 | Средства защиты от несанкционированного доступа | 12 | 4 | - | - | - | 10 |
| | 3 | Криптография | 28 | - | - | - | 4 | 22 |
| | | Выполнение контрольной работы | 20 | - | - | - | - | 20 |
| **Итого:** | | | **72** | **6** | **-** | **-** | **4** | **62** |
| **9 семестр** | | | | | | | | |
| 1 | 1 | Технические аспекты обеспечения информационной безопасности вычислительных систем | 52 | 8 | - | - | 8 | 36 |
| | | Выполнение контрольной работы | 20 | - | - | - | - | 20 |
| | | Подготовка к экзамену | 36 | - | - | - | - | 36 |
| **Итого:** | | | **108** | **8** | **-** | **-** | **8** | **92** |
| **Всего:** | | | **180** | **14** | **-** | **-** | **12** | **154** |

## 5. Содержание лекционного курса

| № темы | Всего часов | № лекции | Тема лекции. Вопросы, отрабатываемые на лекции | Учебно-методическое обеспечение |
|---|---|---|---|---|
| 1 | | | 4 | 5 |
| | | | **8 семестр** | |
| 1 | 2 | 1 | **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 |
| 2 | 2 | 2 | **Средства защиты от несанкционированного доступа.** Обзор рынка программно-аппаратных комплексов | 3-5 |

| | | | | |
|---|---|---|---|---|
| | | | защиты информации. | |
| | | | **9 семестр** | |
| 1 | 6 | 1-3 | **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 |
| | | | **8 семестр** | |
| 3 | 2 | 1 | Основы криптографии: понятия, методы шифрования:<br>- шифр Цезаря,<br>- шифр Виженера,<br>- алгоритм простой вертикальной перестановки,<br>- алгоритм одиночной перестановки,<br>- алгоритм двойных перестановок,<br>- метод магического квадрата,<br>- метод Полибианского квадрата,<br>- многоалфавитная замена,<br>- метод Кардано для квадрата и прямоугольника. | 1 |
| | 2 | 2 | Элементы криптоанализа: элементы частотности символов в тексте. | 1 |
| | 2 | 3 | Компьютерные алгоритмы шифрования: RSA, DES и др. | 1,3,4 |
| | | | **9 семестр** | |
| 1 | 6 | 1-3 | Слабости парольных защит | 3-5 |
| | 4 | 4-5 | 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.

| № | Всего | Вопросы для самостоятельного изучения (задания) | Учебно- |
|---|---|---|---|

| темы | часов | | методическое обеспечение |
|---|---|---|---|
| **8 семестр** | | | |
| 2 | 10 | Изучение изменений нормативно-правовой базы по обеспечению защиты информации от несанкционированного доступа | 2-5 |
| 3 | 10 | Средства защиты от несанкционированного доступа: обзор рынка современных программно-аппаратных комплексов средств защиты от несанкционированного доступа | 3-5 |
| 4 | 22 | Криптография (изучение методов шифрования, не входящих в перечень шифров, входящих в лабораторные работы) | 1 |
| | 20 | Выполнение контрольной работы | |
| | **62** | | |
| **9 семестр** | | | |
| 1 | 36 | Технические аспекты обеспечения информационной безопасности вычислительных систем: обзор рынка современных средств обеспечения экранирования персональных ЭВМ и систем | 3-5 |
| | 20 | Выполнение контрольной работы | |
| | 36 | Подготовка к экзамену | |
| | **92** | | |

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

**11. Курсовая работа (учебным планом не предусмотрена).**

**12. Курсовой проект (учебным планом не предусмотрен)**

**13. Контрольная работа**

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. Вариант задания назначает преподаватель.

**14. 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 | Студент должен **знать**: основные понятия и средства информационной безопасности, методы, лежащие в основе атак несанкционированного доступа | Лекции, практические работы, СРС | Тестирование, индивидуальные задания, зачет, экзамен |

| | | | | |
|---|---|---|---|---|
| | технологий и программные средства, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности | (НСД) | | |
| | | Студент должен **уметь**: определить и применить оптимальные способы предотвращения НСД (в т.ч. криптографические) | Лекции, практические работы, СРС | Тестирование, индивидуальные задания |
| | | 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 с 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. | Лекции, практические работы, СРС | Тестирование, индивидуальные задания, зачет, экзамен |
| | | Студент должен **уметь**: ориентироваться в процессах жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами использования информационных сервисов (контент-сервисов) | Лекции, практические работы, СРС | Тестирование, индивидуальные задания |
| | | Студент должен **владеть**: навыками применения криптографических алгоритмов, способных обеспечить безопасность документов профессиональной деятельности | Практические работы | 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.<br>***Умеет:***. использовать средства защиты информации, встроенные в операционные системы<br>***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.<br>***Владеет:*** навыками разработки приложений на основе криптографических алгоритмов. |
| Высокий (отлично) | ***Знает:*** базовые понятия, средства защиты от несанкционированного доступа: системы парольной защиты, системы привязки к ПК, программно-аппаратные системы; модели основных криптографических атак и технические аспекты защиты информации.<br>***Умеет:*** определить оптимальный способ организации защиты данных на основании классификации типа информации. Собственности<br>***Владеет:*** навыками создания прикладных приложений по обеспечению информационной безопасности интеллектуальной собственности |

Уровни освоения компонент компетенции ОПК-3

| Ступени уровней освоения компетенции | Отличительные признаки |
|---|---|
| 1 | 2 |
| Пороговый (удовлетворительный) | **Знает**: основные понятия и жизненный цикл цифрового контента, задачи защиты информации и документы регламентирующие их, способы обеспечения защиты информационно-коммуникационных технологий управления бизнесом.<br>**Умеет:** ориентироваться в процессах жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами использования информационных сервисов (контент-сервисов).<br>**Владеет:** навыками применения криптографических алгоритмов, способных обеспечить безопасность документов профессиональной деятельности. |
| Продвинутый (хорошо) | **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.<br>**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).<br>**Владеет :** навыками применения нормативно-правовых регламентов при разработке приложений. |
| Высокий (отлично) | **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.<br>**Умеет :** анализировать соответствующую нормативно-правовую базу для определения оптимальных способ организации защиты данных на основании классификации типа информации.<br>**Владеет:** навыками применения нормативно-правовых |

| | |
|---|---|
| | регламентов при создания прикладных приложений по обеспечению защиты интеллектуальной собственности |

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).

## 15. 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.

## 16.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 c. — ISBN 5-98003-002-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/90248.html (дата обращения: 11.10.2021). — 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 c. — ISBN 978-5-9275-3546-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/107955.html (дата обращения: 11.10.2021). — 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 c. — ISBN 978-5-9275-3571-2 (ч.1), 978-5-9275-3526-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/107943.html (дата обращения: 11.10.2021). — 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 c. — ISBN 978-5-4497-1164-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/108227.html (дата обращения: 11.10.2021). — Режим доступа: для авторизир. пользователей
5. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 581 c. — ISBN 978-5-4497-0560-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/94863.html (дата обращения: 11.10.2021). — Режим доступа: для авторизир. пользователей


Программное обеспечение и Интернет-ресурсы

1. http://www \Secret Net\ЭРИМЕКС_ Новосибирск Средства защиты информации - Secret Net.htm.
2. http://www \Комплекс ср_защ 'Гриф'\Институт компьютерных технологий - Защита информации в ПЭВМ.htm.

3. http://www \П-А комплекс 'Мастер паролей'\Программно-аппаратный комплекс «Мастер Паролей.htm.

4. http://www \П-А комплекс 'Шипка'\ВНИИПВТИ - Программно-аппаратный комплекс средств защиты от несанкционированного доступа к информации ШИПКА.htm.

5. http://www \Электр замок 'Соболь'\ЭРИМЕКС_ Новосибирск Средства защиты информации - Электронный замок Соболь.htm.

## 17. 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» у**комплектована 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./

## 18. 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 _____/_____/