Государственное образовательное учреждение
«Приднестровский государственный университет
имени Т.Г. Шевченко»

Рыбницкий филиал
Кафедра информатики и программной инженерии

УТВЕРЖДАЮ
Директор филиала
ПГУ им. Т.Г. Шевченко в г. Рыбница
профессор _____ И.А. Павлинов
«29» сентября 2021 г.

РАБОЧАЯ ПРОГРАММА

на 2021/2022 учебный год
Учебной ДИСЦИПЛИНЫ
«ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки:
2.09.03.04 «Программная инженерия»

Профиль подготовки:
«Разработка программно-информационных систем»

квалификация (степень) выпускника
Бакалавр

Форма обучения:
очная

Год набора:
2018

Рыбница 2021

Рабочая программа дисциплины «***Защита информации***» / сост. Л.Я. Козак. – Рыбница: филиал ПГУ им. Т.Г. Шевченко в г. Рыбница, 2021. – 20 с.

РАБОЧАЯ ПРОГРАММА ПРЕДНАЗНАЧЕНА ДЛЯ ПРЕПОДАВАНИЯ ВАРИАТИВНОЙ ЧАСТИ БЛОКА ОБЯЗАТЕЛЬНЫХ ДИСЦИПЛИН (МОДУЛЕЙ) СТУДЕНТАМ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 2.09.03.04 – *«ПРОГРАММНАЯ ИНЖЕНЕРИЯ»* ПРОФИЛЬ ПОДГОТОВКИ *«РАЗРАБОТКА ПРОГРАММНО-ИНФОРМАЦИОННЫХ СИСТЕМ»*.

Рабочая программа составлена с учетом Федерального Государственного образовательного стандарта высшего образования по направлению подготовки 2.09.03.04 – *«Программная инженерия»*, утвержденного приказом Министерства образования и науки Российской Федерации № 229 от 12 марта 2015 года.

Составитель _____ **Л.Я. Козак, канд. техн. наук, доцент**

1. *Цели и задачи освоения дисциплины*

Цель освоения учебной дисциплины «Защита информации» – ознакомить студентов с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами; изучить методы идентификации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

Задачами освоения учебной дисциплины являются:

– иметь представление об использовании основных положений теории информационной безопасности в различных областях АСОИУ и иметь представление о направлении развития и перспективах защиты информации;

– знать правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации в АСОИУ, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов;

– уметь применять методы защиты компьютерной информации при проектировании АСОИУ в различных предметных областях.

2. *Место дисциплины в структуре ООП ВО*

Дисциплина «Защита информации» относится к вариативной части блока (Б1.В.12) обязательных дисциплин (модулей) для направления подготовки 2.09.03.04 «Программная инженерия».

Для освоения дисциплины «Защита информации» обучающиеся используют знания, умения, навыки, способы деятельности и установки, сформированные в ходе изучения дисциплин: «Исследование операций», «Основы программирования» «Операционные системы», «Архитектура ЭВМ», «Введение в алгоритмы».

Освоение дисциплины «Защита информации» является основой для последующего написания выпускной квалификационной работы.

3. *Требования к результатам освоения дисциплины*

Изучение дисциплины направлено на формирование следующих компетенций:

Код компетенции	Формулировка компетенции
ПК-1	Готовность применять основные методы и инструменты разработки программного обеспечения.
ПК-21	Владение навыками чтения, понимания и выделения главной идеи прочитанного исходного кода, документации.

В результате освоения дисциплины студент должен:

3.1. Знать:

– основы базовой подготовки специалистов, необходимой для успешного изучения специальных дисциплин и последующей научно-технической и организационно-методической деятельности, связанной с проведением научных исследований и оценкой эффективности разработанных предложений, их внедрением в различных областях;

- различные методы защиты информации;
- различные способы защиты информации;
- этапы реализации компьютерных математических моделей.

3.2. Уметь:

- решать проблемы защиты информации, стоящие перед современной вычислительной техникой;
- использовать полученные знания для правильного выбора решений при разработке криптографических средств защиты информации.

3.3. Владеть:

– теоретическими знаниями и практическими навыками при решении типовых задач по обеспечению информационной безопасности;
– методами и средствами защиты информации в различных предметных областях;
– основными методами и средствами защиты компьютерной информации.
– методикой вычислительного эксперимента на компьютере.

4. Структура и содержание дисциплины

4.1. Распределение* трудоемкости в з.е./часах *по видам аудиторной и самостоятельной работы студентов по семестрам

Семестр	Количество часов						Форма итогового контроля
	Трудоем-кость, з.е./часы	В том числе					
		Аудиторных				Самост. работа	
		Всего	Лекций	Лаб. раб.	Практич. занятия		
7	5/180	72	36	36	–	72	Экзамен
Итого:	**5/180**	**72**	**36**	**36**	–	**72**	**Экзамен**

4.2. Распределение видов учебной работы и их трудоемкости по модулям дисциплины

№ раз-дела	Наименование модулей	Количество часов				
		Всего	Аудиторная работа			Внеауд работа (СР)
			Л	ПЗ	ЛР	
1	Основы информационной безопасности. Основные понятия и определения. Политика государства в области информационной безопасности. Угрозы и нарушители безопасности информации	6	6	-	-	-
2	Исторический обзор криптографических методов защиты информации. Меры обеспечения защиты информации	20	4	-	-	16
3	Криптографические методы защиты информации. Стеганграфическая защита информации	38	8	-	14	16
4	Модель угроз безопасности информации. Методы контроля разграничения доступа. Организационные меры защиты информации	40	10	-	14	16
5	Техническая защита информации. Программно-технические методы защиты информации	24	4	-	-	20
6	Политика безопасности. Системы обнаружения и предотвращения компьютерных атак	16	4	-	8	4
	Итого:	**144**	**36**	**-**	**36**	**72**

4.3. Тематический план по видам учебной деятельности

Лекции

№ п/п	Номер раздела дисциплины	Объем часов	Тема лекции	Учебно-наглядные пособия
1	1	2	Базовые направления криптографии: шифрование, кодирование и стеганография. Основные различия.	–
2		2	Стеганография. Подготовка и использование симпатических чернил, цифровая стеганография. Методы определения «присутствия» информации.	–
3		2	Кодирование. Архивация - кодирование сжатием (методы Huffman, Lempel-Ziv, арифметические). Использование кодирования при передаче информации (методы Radix/Base64, UUE).	–
4	2	2	Древние методы шифрования. Шифры перестановок.	–
5		2	Древние методы шифрования. Шифры алфавитной замены. Статистические свойства языка. Вскрытие шифров алфавитной замены.	–
6	3	2	Симметричные криптосистемы (алгоритмы DES, 3-DES, AES, ГОСТ-28147-89). Принципы работы, назначение.	раздаточный материал
7		2	Асимметричные криптосистемы (алгоритм RSA). Цифровая подпись. Пространство ключей.	раздаточный материал
8		2	Требования к современным криптографическим системам и алгоритмам.	–
9		2	Другие криптографические алгоритмы. Вычисление контрольных сумм (CRC) и хеширование (MD4/5, SHA).	–
10	4	2	Защита носителей информации (Floppy/HDD/CD/DVD/Flash).	раздаточный материал
11		2	Защита программного обеспечения с помощью электронных ключей (LPT/COM/USB), HID-устройства, iButton.	–
12		2	Альтернативные методы защиты. Аутентификация по биометрическим данным (отпечаток пальца, геометрия руки, радужная оболочка глаза, сетчатка глаза, голосовая идентификация, геометрия лица, клавиатурный почерк).	–
13		2	Защита исходного кода программ – обфускация кода.	–
14		2	Вредоносное программное обеспечение как средство преодоления защиты информации.	–
15	5	2	Комплекс мер по защите информации. Разработка стратегии.	раздаточный материал
16		2	Организационные меры. Физическая, электромагнитная, активная и пассивная защита. Человеческий фактор.	–
17	6	2	Основные моменты гражданского и уголовного кодексов ПМР в отношении защиты информации. Основные моменты Конституции ПМР в отношении защиты личной информации.	–
18		2	Способы подделки документов и методы выявления подделок.	–
Итого:		**36 часов**		

Лабораторные работы

№ п/п	№ раздела дисципли-ны	Объем часов	Тема практического занятия	Наимено-вание лаборатор.	Учебно-наглядные пособия
1	3	2	Стеганография. Изготовление и использование симпатических чернил на основе молока, $NaHCO_3$, $FeCl_3$, $K_4[Fe(CN)_6]$ и др.	аудитория № 30	методич. пособие
2		2	Кодирование. Сравнение различных методов.	аудитория № 30	методич. пособие
3		2	Шифрование. Применение алгоритмов DES, 3DES, RSA для шифрования файлов. Использование библиотеки CAPICOM.DLL.	аудитория № 30	методич. пособие
4		2	Контрольные суммы файлов. Реализация алгоритма подсчета CRC.	аудитория № 30	методич. пособие
5		2	Хеширование. Реализация и применение алгоритма MD5.	аудитория № 30	методич. пособие
6		2	Реализация защиты прикладной программы.	аудитория № 30	методич. пособие
7		2	Преодоление защиты прикладных программ с использованием отладчика OllyDebugger. Выявление положительных и отрицательных сторон тех или иных методов защиты.	аудитория № 30	методич. пособие
8	4	2	Реализация защиты программного обеспечения от распространения на основе защиты носителя информации.	аудитория № 30	методич. пособие
9		2	Использование программных решений фирмы StarForce для защиты программного обеспечения.	аудитория № 30	методич. пособие
10		2	Использование PrettyGoodPrivacy. Генерация открытого/закрытого ключей. Использование цифровой подписи.	аудитория № 30	методич. пособие
11		2	Использование специализированного программного обеспечения для защиты пространства данных (создание виртуальных дисков).	аудитория № 30	методич. пособие
12		2	Использование электронных ключей для защиты программного обеспечения. Изучение продуктов фирмы KEYLOK.	аудитория № 30	методич. пособие
13		2	Защита программного обеспечения с помощью биометрических параметров (использование клавиатурного почерка).	аудитория № 30	методич. пособие
14		2	Анализ вредоносного программного обеспечения. Внедрение HTTP или FTP сервера в документ MS Word и/или MS Excel.	аудитория № 30	методич. пособие
15	6	2	Анализ возможностей программного обеспечения категории exploits.	аудитория № 30	методич. пособие
16		2	Разработка динамической библиотеки с базовым набором криптографических средств. Методы шифрования и расшифрования сообщений.	аудитория № 30	методич. пособие
17		2	Разработка динамической библиотеки с базовым набором криптографических средств. Методы шифрования и расшифрования файлов.	аудитория № 30	методич. пособие

18		2	Разработка динамической библиотеки с базовым набором криптографических средств. Функции подсчета контрольных сумм, хеш-функции.	аудитория № 30	методич. пособие
Итого:		**36 часов**			

Самостоятельная работа студента

Раздел дисциплины	№ п/п	Тема и вид СРС	Трудоемкость (в часах)
2	1	Криптографические протоколы: основные, промежуточные. *Работа с литературой*	8
	2	Криптографические протоколы: развитые, эзотерические. *Конспектирование*	8
3	3	Информационная безопасность автоматизированных систем. *Подготовка сообщения*	4
	4	Самотестирующиеся и самокорректирующиеся программы. *Конспектирование*	8
	5	Конфиденциальные вычисления. *Работа с литературой*	4
4	6	Системы защиты информации. *Работа с литературой*	4
	7	Развитие теории и практики защиты информации. *Подготовка сообщения*	4
	8	Сетевая защита. *Работа с литературой*	8
5	9	Симметричные криптосистемы. *Работа с литературой*	4
	10	Шифр простой перестановки, магический квадрат. *Подготовка сообщения*	4
	11	Перестановка «Магический квадрат». *Конспектирование*	4
	12	Асимметричные криптосистемы. *Работа с литературой*	4
	13	Хакерские атаки, способы борьбы с ними. *Работа с литературой*	4
6	14	Доктрина информационной безопасности ПМР. *Конспектирование*	4
Итого:			**72 часа**

5. Перечень тем курсовых работ

не предусмотрены

6. Образовательные технологии

Для повышения наглядности рассматриваемого материала применяются образовательные технологии, основанные на применении специализированных программных сред и технических средств работы с информацией. Например, лекции с мультимедийным сопровождением, с использованием электронных учебников.

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Кол-во часов
7	Л, ЛР	Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.	2
		Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения на всех уровнях. Мультимедийные программы предназначены как для аудиторной, так и самостоятельной работы студентов.	2
		Интернет-технологии – предоставляют широкие возможности для поиска информации и ведения научных исследований.	2

		Технология индивидуализации обучения – помогает реализовывать личностно-ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.	2
		Технология тестирования – используется для контроля уровня усвоения знаний в рамках модуля на определённом этапе обучения. Данная технология позволяет преподавателю выявить и систематизировать аспекты, требующие дополнительной проработки.	2
		Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.	2
Итого:			**24**

Для повышения наглядности рассматриваемого материала применяются образовательные технологии, основанные на применении специализированных программных сред и технических средств работы с информацией. Например, лекции с мультимедийным сопровождением, с использованием электронных учебников в дистанционной форме.

В рамках данной дисциплины применяются инновационные методы, основанные на использовании современных достижений науки и информационных технологий в образовании. Они предполагают применение информационных образовательных технологий, а также учебно-методических материалов, соответствующих современному мировому уровню, в процессе преподавания дисциплины:

- использование мультимедийных учебников, размещенных в ОНУ «Интуит»;
- использование обучающих Интернет-ресурсов;
- проведение лекций в дистанционной форме с использованием видео-конференции в Zoom;
- обмен методическими материалами посредством электронной почты, мессенджеров, социальных сетей;
- использование программно-педагогических тестовых сред для проверки знаний студентов.

Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения входного, текущего контроля и промежуточной аттестации. Фонд включает задания для контрольной работы, лабораторных работ, задания в тестовой форме, вопросы к экзамену, в том числе в виртуальной обучающей среде Moodle. Фонд оценочных средств представлен в учебно-методическом комплексе дисциплины. Используемые формы текущего контроля: контрольная работа; аудиторные самостоятельные работы; лабораторные работы; устный опрос; устное сообщение, доклад; тестирование (в том числе в виртуальной обучающей среде Moodle).

Предусмотрены самостоятельные работы, контрольные работы по темам: «Сущность проблемы и задачи защиты в компьютерных сетях. Методы обеспечения безопасности сетей» и «Угрозы, атаки и каналы утечки информации».

7. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Для оценки качества усвоения курса используются следующие формы контроля:

- **текущий** – контроль выполнения лабораторных работ, тестирование;
- **рубежный** предполагает использование тестовых материалов для контроля знаний;
- **итоговый** осуществляется посредством тестирования и экзамена.

Самостоятельная работа рассматривается как вид учебного труда студента, позволяющего целенаправленно формировать и развивать его самостоятельность как личностное качество при выполнении домашних заданий и проработке дополнительного учебного материала.

Самостоятельная работа студентов по дисциплине организуется в следующих формах:

– работе студентов с лекционным материалом, поиске и анализе литературы и электронных источников информации по заданной проблеме и выбранной теме индивидуального задания;

– выполнении домашних заданий;
– переводе материалов из тематических информационных ресурсов с иностранных языков;
– изучении тем, вынесенных на самостоятельную проработку;
– изучении теоретического материала к лабораторным занятиям;
– подготовке к экзамену.

В качестве учебно-методического обеспечения самостоятельной работы используется основная и дополнительная литература по дисциплине, Интернет-ресурсы, материалы лекций, указания, выданные преподавателем при проведении лабораторных работ.

№	Наименование работы	Число часов	Форма контроля
1	Проработка лекционного материала. Выполнение индивидуальных заданий	60	Отчет по индивидуальным заданиям. Экзамен
2	Подготовка к лабораторным занятиям и оформление отчетов	12	Отчет. Допуск к лабораторным работам. Защита отчетов

Всего часов самостоятельной работы – 72.

Программа самостоятельной работы по дисциплине «Защита информации» предполагает выполнение студентом в процессе обучения одного индивидуального задания из следующего списка индивидуальных заданий по компьютерным алгоритмам СЗИ:

1. Стандарт симметричного шифрования данных DES.
2. Блочный шифр IDEA.
3. Блочный шифр ГОСТ.
4. Блочный шифр CAST.
5. Блочный шифр BLOWFISH.
6. Блочный шифр RC5.
7. Блочный шифр LUCIFER.
8. Блочный шифр MADRYGA.
9. Блочный шифр NewDES.
10. Блочный шифр FEAL.
11. Блочный шифр REDOC.
12. Блочный шифр LOKI.
13. Блочный шифр KHUFU.
14. Блочный шифр RC2.
15. Блочный шифр MMB.
16. Блочный шифр CA-1.1.
17. Блочный шифр SKIPJACK.
18. Блочный шифр SAFER.
19. Блочный шифр 3-WAY.
20. Блочный шифр CRAB.
21. Блочный шифр SXAL8/MBAL.
22. Блочный шифр RC4.
23. Блочный шифр SEAL.
24. Асимметричный ранцевый криптоалгоритм.
25. Асимметричный алгоритм шифрования данных RSA.
26. Асимметричный алгоритм шифрования данных ElGamal.
27. Асимметричный алгоритм шифрования данных Pohlig-Hellman.
28. Асимметричный алгоритм шифрования данных Rabin.
29. Асимметричный алгоритм шифрования данных McEliece
30. Асимметричный алгоритм шифрования данных LUC.
31. Алгоритм цифровой подписи с открытым ключом DSA.
32. Алгоритм цифровой подписи с открытым ключом ГОСТ.
33. Однонаправленная хэш-функция Snefru.

34. Однонаправленная хэш-функция *N*-хэш.
35. Однонаправленная хэш-функция MD4.
36. Однонаправленная хэш-функция MD5.
37. Алгоритм безопасного хэширования (Secure Hash Algorithm, SHA).
38. Однонаправленная хэш-функция RIPE-MD.
39. Однонаправленная хэш-функция HAVAL.

Образец теста для проведения итогового контроля по итогам освоения дисциплины, а также для контроля самостоятельной работы студента.

Тест №1

для среза текущих знаний

1) Под угрозой безопасности информации в компьютерной системе (КС) понимают:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2) Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

3) Атакой на КС называют:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

4) Искусственные угрозы исходя из их мотивов разделяются на:

a) непреднамеренные и преднамеренные.

b) косвенные и непосредственные.

c) несанкционированные и сонкцианированные.

5) К непреднамеренным угрозам относятся:

a) ошибки в разработке программных средств КС.

b) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

c) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой.

6) К умышленным угрозам относятся:

a) несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС).

b) воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

c) ошибки пользователей КС.

7) Косвенными каналами утечки называют:

a) каналы, не связанные с физическим доступом к элементам КС.

b) каналы, связанные с физическим доступом к элементам КС.

c) каналы, связанные с изменение элементов КС и ее структуры.

8)К косвенным каналам утечки информации относятся:

a) использование подслушивающих (радиозакладных) устройств.

b) маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т.п.).

c) злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке.

9)Непосредственными каналами утечки называют:

a) каналы, связанные с физическим доступом к элементам КС.

b) каналы, не связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

10)К непосредственным каналам утески информации относятся:

a) обход средств разграничения доступа к информационным вследствие недостатков в их программном обеспечении и др.

b) перехват побочных электромагнитных излучений и (ПЭМИН).

c) дистанционное видеонаблюдение.

11) Избирательная политика безопасности подразумевает, что:

a) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

b) все субъекты и объекты системы должны быть однозначно идентифицированы.

c) каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации.

12) Полномочная политика безопасности подразумевает, что:

a) каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

b) все субъекты и объекты системы должны быть идентифицированы.

c) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

13) Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

c) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

14) Под защитой информации понимается

a) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам ПК и хранящимся в ней программам и данным.

b) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по реализации механизма виртуальной памяти с разделением адресных пространств.

c) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по разграничению прав пользователей и обслуживающего персонала.

15) Возможные каналы утечки информации по классификации разделяют:

a) человек, аппаратура, программа.

b) человек, линия связи.

c) коммутационное оборудование, человек.

16)К группе каналов утечки информации в которой основным средством является человек, относятся следующие утечки:

a) расшифровка программой зашифрованной информации.

b) несанкционированный доступ программы к информации.

c) копирование программой информации с носителей.

17) К группе каналов утечки информации в которой основным средством является аппаратура, относятся следующие утечки:

a) подключение к ПК специально разработанных аппаратных средств, обеспечивающих доступ к информации.

b) хищение носителей информации (магнитных дисков, дискет, лент).

c) копирование программой информации с носителей.

18) К группе каналов утечки информации в которой основным средством является программа, относятся следующие утечки:

a) несанкционированный доступ программы к информации.

b) хищение носителей информации (магнитных дисков, дискет, лент).

c) использование специальных технических средств для перехвата электромагнитных излучений технических средств ПК.

19) Идентификация объекта – это:

a) одна из функций подсистемы защиты.

b) взаимное установление подлинности объектов, связывающихся между собой по линиям связи.

c) сфера действий пользователя и доступные ему ресурсы КС.

20) Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:

a) авторизацией.

b) аутентификацией.

c) идентификация.

21) Авторизация – это:

a) предоставление полномочий.

b) подтверждение подлинности.

c) цифровая подпись.

22) Аутентификация – это:

a) подтверждение подлинности.

b) предоставление полномочий.

c) цифровая подпись.

23) Под компьютерным вирусом понимается:

a) автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ПК.

b) программа имеющая доступ к файлам системы, и имеющая возможность работать с процессами системы.

c) программа не имеющая доступ к файлам системы, и не имеющая возможность работать с процессами системы.

24) Трянские программы это:

a) программы, которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям.

b) программы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

c) программы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

ОТВЕТЫ

1	3	**6**	3	**11**	2	**16**	1	**21**	1
2	2	**7**	2	**12**	1	**17**	4	**22**	2
3	2	**8**	1	**13**	2	**18**	3	**23**	1
4	3	**9**	1	**14**	2	**19**	3	**24**	1
5	4	**10**	4	**15**	4	**20**	3		

Итоговый тест

1) К средствам активной защиты относятся:

a) искаженные программы (программы вирусы, искажение функций)
b) заказное проектирование
c) специальная аппаратура

2) К средствам пассивной защиты относятся:

a) частотный анализ
b) авторская эстетика
c) аппаратура защиты (ПЗУ, преобразователи)

3) К средствам собственной защиты относятся:

a) машинный код
b) сигнатура
c) корреляционный анализ

4) Под системой защиты от несанкционированного использования и копирования понимается:

a) комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов
b) комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации
c) комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности

5) Под надежностью системы защиты от несанкционированного копирования понимается:

a) способность противостоять попыткам изучения алгоритма ее работы и обхода реализованных в нем методов защиты
b) способность систем с открытыми ключами генерировать цифровые подписи, обеспечивающие различные функции защиты, компенсирует избыточность требуемых вычислений
c) способность к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ПК.

6) Методы, затрудняющие считывание скопированной информации основываются на

a) придании особенностей процессу записи информации, которые не позволяют считывать полученную копию на других накопителях, не входящих в защищаемую КС
b) разграничении прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц
c) использования дополнительных программных или аппаратно-программных средств

7) Для защиты от несанкционированного использования программ могут применяться электронные ключи?

a) да
b) нет
c) не знаю

8) Любая криптографическая система основана на использовании:

a) криптографических ключей
b) разомкнутых линии
c) односторонних функций

9) В симметричной криптосистеме отправитель и получатель сообщения используют

a) один и тот же секретный ключ
b) разные секретных ключи
c) вообще не используют секретных ключей

10) Асимметричная криптосистема предполагает использование

a) двух ключей открытого и личного (секретного)

b) системы разграничения доступа
c) переносных носителей для хранения секретной информации

11) Под ключевой информацией понимают:

a) совокупность всех действующих в АСОИ ключей
b) совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы
c) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации

12)Какая из функций не входит в процесс управления ключами?

a) переадресация ключей
b) генерация ключей
c) распределение ключей

13) Модификация ключа – это

a) генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонаправленной) функции
b) генерирование нового ключа из последующего значения ключа с помощью односторонней (однонаправленной) функции
c) генерирование нового ключа из предыдущего значения ключа с помощью двусторонней (двунаправленной) функции

14) Под функцией хранения ключей понимают

a) организацию их безопасного хранения, учета и удаления
b) организацию их генерации, учета и удаления
c) организацию их безопасного хранения, учета и сопоставления

15)В чем заключается правило разграничения доступа

a) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа
b) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа
c) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, не содержатся все категории, определенные для данного документа

16) Файловые вирусы это:

a) вирусы, заражающие файлы с программами
b) вирусы, заражающие программы, хранящиеся в системных областях дисков
c) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам

17) Резидентные вирусы это:

a) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам
b) вирусы, которые выполняются только в момент запуска зараженной программы
c) вирусы, заражающие программы, хранящиеся в системных областях дисков

18) Транзитные вирусы это:

a) вирусы, которые выполняются только в момент запуска зараженной программы
b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам
c) вирусы, заражающие программы, хранящиеся в системных областях дисков

19) Вирусы-мутанты (MtE-вирусы) это:

a) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса

b) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных

c) вирусы, заражающие программы, хранящиеся в системных областях дисков

20) Stealth-вирусы это:

a) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных

b) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса

c) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам

21) Загрузочные (бутовые) вирусы это:

a) вирусы, заражающие программы, хранящиеся в системных областях дисков

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам

c) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса

22) Основной проблемой создания высокоэффективной защиты от НСД является

a) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние

b) использование дополнительных программных или аппаратно-программных средств

c) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

23)Аппаратно-программмные средства криптографической защиты информации выполняют функции:

a) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись

b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС

c) проверяют на отсутствие закладок приборов, устройств

24) Использование аппаратных средств снимает проблему:

a) обеспечения целостности системы

b) разграничения прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

c) использования строго определенного множества программ

a) за один цикл, и тем самым уменьшает длительность процесса идентификации

b) внешней аутентификацией объекта, не принадлежащего системе

ОТВЕТЫ

1	3	**6**	3	**11**	2	**16**	1	**21**	2
2	2	**7**	2	**12**	1	**17**	4	**22**	2
3	2	**8**	1	**13**	2	**18**	3	**23**	2
4	3	**9**	1	**14**	2	**19**	3	**24**	3
5	4	**10**	4	**15**	4	**20**	3		

Примерный перечень вопросов к экзамену

1. Альтернативные методы защиты. Аутентификация по биометрическим данным (отпечаток пальца, геометрия руки, радужная оболочка глаза, сетчатка глаза, голосовая идентификация, геометрия лица, клавиатурный почерк)
2. Асимметричные криптосистемы (алгоритм RSA). Цифровая подпись. Пространство ключей.

3. Базовые направления криптографии: шифрование, кодирование и стеганография. Основные различия.

4. Вредоносное программное обеспечение как средство преодоления защиты информации.

5. Древние методы шифрования: методы перестановок; двойных перестановок. Шифр перестановок магическим квадратом.

6. Древние методы шифрования: шифры алфавитной замены; простой замены; сложной замены.

7. Другие криптографические алгоритмы. Вычисление контрольных сумм (CRC) и хеширование (MD4/5, SHA)

8. Защита исходного кода программ – обфускация кода.

9. Защита носителей информации (Floppy/HDD/CD/DVD/Flash)

10. Исследование уязвимостей операционных систем

11. Исследование уязвимостей прикладного программного обеспечения

12. Кодирование. Архивация – кодирование сжатием (методы Huffman, Lempel-Ziv, арифметические). Использование кодирования при передаче информации.

13. Комплекс мер по защите информации. Разработка стратегии.

14. Компьютерная разведка. Криптоаналитические атаки.

15. Организационные меры. Физическая, электромагнитная, активная и пассивная защита. Человеческий фактор.

16. Основные моменты гражданского и уголовного кодексов ПМР в отношении защиты информации.

17. Перестановка «Магический квадрат»

18. Разработка комплекса мер по защите информации в рамках организации.

19. Разработка системы защиты программного обеспечения распространяемого по Internet.

20. Разработка собственной криптографической системы.

21. Самотестирующиеся и самокорректирующиеся программы.

22. Симметричные криптосистемы (алгоритмы DES, 3-DES, AES, ГОСТ-28147-89). Принципы работы, назначение.

23. Способы подделки документов и методы выявления подделок.

24. Статистические свойства языка. Вскрытие шифров алфавитной замены.

25. Стеганография. Подготовка и использование симпатических чернил, цифровая стеганография. Методы определения «присутствия» информации.

26. Схема цифровой подписи. Схема шифрования Эль Гамаля.

27. Технические разведки. Компьютерная разведка.

28. Технические разведки. Компьютерная разведка. Методы взлома компьютерных систем. Программы-шпионы.

29. Требования к современным криптографическим системам и алгоритмам.

30. Хакерские атаки, способы борьбы с ними.

Контроль самостоятельной работы студентов

Формы контроля самостоятельной работы студентов: доклад, ответы на тестирование.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

1. Винокуров Андрей. Криптография, ее истоки и место в современном обществе (Цикл статей по криптографии) – М.: ЗАО "Издательство БИНОМ", 2018. – 208 с.: ил.

2. Жельников Владимир. Криптография от папируса до компьютера. – М.: "Нолидж", 2021. – 384 с., ил.

3. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов. 3-е изд. – М.: Горячая линия – Телеком, 2020. – 144 с.

4. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др]. – М.: Горячая линия – Телеком, 2019. – 544 с.

8.2. Дополнительная литература

1. Мещеряков Р.В. Информационная безопасность. – Томск: ТПУ, 2017.

2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 2018.

3. Насыпный В.В. Метод защиты арифметических вычислений в компьютерных системах. – М.: Прометей, 2019.

4. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 2015.

5. Безопасность информационных технологий. Выпуск 1. – М.: МИФИ. 2014.

6. Безопасность информационных технологий. Выпуск 3. – М.: МИФИ, 2017.

7. Вопросы защиты информации. – №1. – 2019.

8. Воронов М.В., Антонов Г.Н. К вопросу об устойчивости боевых систем. Военная мысль, 2017, 2. – с.75-76.

9. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

10. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

11. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 2016.

12. Насыпный В.В. Синтез систем обработки информации с защитой от программных закладок и вирусов. – М.: ВТИ, 2017.

13.Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. – М.:ГТК РФ, 2018.

14. Термины и определения в области защиты от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 2016.

8.3. Программное обеспечение и Интернет-ресурсы

1. Национальный открытый университет «Интуит» https://www.intuit.ru/ studies/courses/691/ 547/info.

2. Ресурсный центр помощи студентам (методические указания) – материалы сайта: http://vstuhelp.narod.ru/met/zi.html.

3. Алефиренко В.М. Основы защиты информации (методические указания) – материалы сайта: http://www.twirpx.com/files/informatics/security/technical/ft.guideline/.

4. Электронный портал факультета электроники и вычислительной техники – материалы сайта: http://fevt.ru/load/78.

8.4. Методические указания и материалы по видам занятий

Методические указания предоставляются студентам в виде теоретических предпосылок (в электронном виде) к лабораторным работам.

Отчеты по лабораторным работам следует оформлять в соответствии с общими требованиями и правилами оформления.

8.5. Программное обеспечение современных информационно-коммуникационных технологий

Windows 7, средства просмотра Opera/Google Chrome, MS Office 2010.

9. Материально-техническое обеспечение дисциплины

Для осуществления образовательного процесса по дисциплине «Защита информации» требуется наличие компьютерной техники с установленным соответствующим программным обеспечением и другого оборудования, поддерживающего проведение презентаций, построение проектной документации, ведение групповой обработки, выход в сеть Интернет. Также требуется обеспечение литературой, которую в достаточном объеме может предложить электронная

библиотека, читальный зал филиала ПГУ им. Т.Г. Шевченко в г. Рыбница и БД по дисциплине в виртуальной обучающей среде Moodle.

Карта обеспечения дисциплины учебными материалами:

№ п/п	Наименование	Вид	Форма доступа
1	Учебно-методическая литература по дисциплине «Защита информации»	Электронный	Электронная библиотека, кафедра ИиПИ
2	Описание лаб. работ	Электронный	Электронная библиотека, кафедра ИиПИ
3	Мультимедийные материалы	Сетевой	Медиатека кафедры ИиПИ
4	Электронная библиотека	Сетевой	Портал филиала ПГУ им. Т.Г. Шевченко в г. Рыбница/ Moodle

Карта обеспечения дисциплины оборудованием:

№ п/п	Номер аудитории	Кол-во	Наименование	Форма использования
1	Аудитория № 30	7	Персональные компьютеры, объединенные локальной сетью. ОС Windows 10. Расширенный пакет Office. Глобальная сеть Internet.	Организация лабораторных работ, доступ к образовательным ресурсам во время самостоятельной работы студентов, работа с мультимедийными материалами на лабораторных занятиях

10. Методические рекомендации по организации изучения дисциплины

Рабочая учебная программа по дисциплине «Защита информации» составлена в соответствии с требованиями Федерального Государственного образовательного стандарта ВО по направлению 2.09.03.04 «Программная инженерия» и учебного плана по профилю подготовки «Разработка программно-информационных систем».

Методические рекомендации для студентов

Методические рекомендации для студентов содержат:

– тематику лабораторных работ;

– планы лабораторных работ с указанием примерного списка аудиторных и домашних заданий.

Изучение дисциплины «Защита информации» включает лекционные и лабораторные занятия. Лекции разбиты на основные разделы, каждый раздел может содержать несколько тем.

Курс сопровождают лабораторные работы. При подготовке к лабораторным работам студентам необходимо самостоятельно изучить рекомендуемую литературу, ответить на контрольные вопросы. В течение семестра каждый студент должен подготовить хотя бы один доклад на темы, предложенные преподавателем.

При подготовке к занятиям необходимо использовать литературу, имеющуюся в достаточном количестве в библиотеке вуза. В список рекомендуемой литературы входит основная и дополнительная литература. Список литературы приведен в карте обеспечения дисциплины учебно-методической литературой.

Текущий контроль усвоения знаний по дисциплине предполагает использование разных форм контроля, в том числе тестирование. Итоговый контроль может осуществляться в форме теста и экзамена. Вопросы к экзамену и образцы тестовых заданий приведены.

Методические указания по организации самостоятельной работы студентов

В курсе «Защита информации» предусмотрен значительный объём самостоятельной работы студентов, который включает изучение лекционного материала, учебной литературы, обучающих Интернет-ресурсов; подготовку к выполнению лабораторного практикума, самоконтроль знаний в форме компьютерного тестирования; выполнение программированных заданий. Для приобщения обучаемых к поиску, к исследовательской работе, для развития их творческого потенциала следует

по возможности избегать прямого руководства работой обучающихся при выполнении ими тех или иных заданий, чаще выступать в роли консультанта, эксперта, коллеги-исследователя.

Подготовка к выполнению лабораторных работ

Лабораторный практикум способствуют повышению качества знаний студентов, это творческие задания, углубляющие знания студентов в их профессиональной деятельности.

Цель лабораторного практикума − обеспечить текущий контроль над знаниями студентов и предоставить возможность:

− студентам - систематизировать и расширить знания, самостоятельно освоить пропущенный материал;

− преподавателю - оценить степень готовности студента к сдаче экзамена по дисциплине.

Для выполнения лабораторных работ по дисциплине «Защита информации» необходим персональный компьютер с вышеперечисленными программами.

На лабораторных занятиях каждый студент получает индивидуальное задание, направленное на формирование компетенций, определенных данной рабочей программой. Лабораторная работа предусматривает реализацию полученных студентами знаний через организацию учебной работы в различных средах. По каждой лабораторной работе студенты должны получить у преподавателя индивидуальное задание и выполнить его.

Во время выполнения заданий в учебной аудитории студент может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается невыполненной, студент может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Отчет оформляется в тетради или распечатывается на листах формата А4. На титульном листе указывается: фамилия и инициалы, курс, группа и представляется преподавателю на проверку по завершению изучения темы.

Для выполнения лабораторной работы необходимо:

1. Изучить краткие теоретические сведения, необходимые для успешного выполнения конкретной работы.
2. Внимательно изучить все примеры заданий, рассмотренные в лекции и представленные в описании лабораторной работы.
3. Ответить на контрольные вопросы, предложенные в данной лабораторной работе.
4. Выполнить индивидуальные задания в предусмотренной темой программной среде.
5. Оформить отчет о выполненной лабораторной работе.

Отчет должен содержать:

- Название темы.
- Цель работы.
- Условие задачи и описание используемых данных.
- Вывод.

Отчет о лабораторной работе принимает преподаватель во время занятия. В процессе защиты оценивается самостоятельность работы, понимание механизма работы среды, знание используемых в работе параметров, умение анализировать результаты выполнения работы.

Выполнение лабораторного практикума является необходимым условием для допуска к экзамену.

11. Технологическая карта дисциплины

Курс ____*4*____ группа ___*РФ17ДР62ПИ*___ семестр _____*7*_____

Преподаватель – лектор *Козак Людмила Ярославовна*

Преподаватели, ведущие лабораторные занятия *Козак Людмила Ярославовна*

Кафедра_____*информатики и программной инженерии* _____

Наименование дисциплины / курса	Уровень//ступень образования (бакалавриат, специалитет, магистратура)	Статус дисциплины в рабочем учебном плане (А, Б, В, Г)	Количество зачетных единиц / кредитов
Защита информации	бакалавриат	Б1.В.12	5

Смежные дисциплины по учебному плану:

Предшествующие: «Исследование операций», «Основы программирования» «Операционные системы», «Архитектура ЭВМ», «Введение в алгоритмы».

Последующие: написание выпускной квалификационной работы

ВВОДНЫЙ МОДУЛЬ

(входной рейтинг-контроль, проверка «остаточных» знаний по смежным дисциплинам)

Тема, задание или мероприятие входного контроля	Виды текущей аттестации	Аудиторная или внеаудиторная	Мин. кол-во баллов	Макс. количество баллов
	Тестирование	Аудиторная	0	10
Итого:			**0**	**10**

БАЗОВЫЙ МОДУЛЬ

(проверка знаний и умений по дисциплине)

Тема, задание или мероприятие текущего контроля	Виды текущей аттестации	Аудиторная или внеаудиторная	Мин. кол-во баллов	Макс. количество баллов
Текущая работа	Лабораторные работы	Аудиторная	1	5
	Работа на лекциях	Аудиторная	3	5
	Присутствие на занятиях	Аудиторная	1	1
	Решение заданий	Аудиторная	3	5
	Самостоятельная работа	Внеаудиторная	3	5
Промежуточный рейтинг-контроль	Лабораторные работы	Аудиторная	1	5
Итого:			**12**	**21**

ДОПОЛНИТЕЛЬНЫЙ МОДУЛЬ

Тема, задание или мероприятие дополнительного контроля	Виды текущей аттестации	Аудиторная или внеаудиторная	Мин. кол-во баллов	Макс. количество баллов
Промежуточный рейтинг-контроль	Тестирование	Аудиторная	5	10
Итого:			**5**	**10**

ИТОГОВЫЙ МОДУЛЬ

	Тестирование	Аудиторная	10	15
Итого:			**10**	**15**

Необходимый минимум для получения итоговой оценки или допуска к промежуточной аттестации 12 баллов

Составитель _____ Л.Я. Козак, доцент

Зав. кафедрой информатики и программной инженерии _____ Л.А. Тягульская, доцент