Государственное бюджетное образовательное учреждение
высшего образования Московской области
«Университет «Дубна»
(государственный университет «Дубна»)

Филиал «Протвино»
Кафедра «Информационные технологии»

УТВЕРЖДАЮ
Директор
_____/Евсиков А.А./
подпись *Фамилия И.О.*
«27» 06 2022 г.

Рабочая программа дисциплины (модуля)

Защита информации
наименование дисциплины (модуля)

Направление подготовки (специальность)
09.03.01 Информатика и вычислительная техника
код и наименование направления подготовки (специальности)

Уровень высшего образования
бакалавриат
бакалавриат, магистратура, специалитет

Направленность (профиль) программы (специализация)
«Программное обеспечение вычислительной техники и автоматизированных систем»

Форма обучения
очная
очная, очно-заочная, заочная

Протвино, 2022

Преподаватель (преподаватели):
Кривцов П.Н., ст.преп., кафедра информационных технологий
Фамилия И.О., должность, ученая степень, ученое звание, кафедра; подпись

Рабочая программа разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) высшего образования
09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки (специальности))

Программа рассмотрена на заседании кафедры информационных технологий
(название кафедры)
Протокол заседания № 11 от «24» июня 2022 г.

Заведующий кафедрой _____ Нурматова Е.В.
(Фамилия И.О., подпись)

СОГЛАСОВАНО

Заведующий выпускающей кафедрой[1] _____
(Фамилия И.О., подпись)
«____» _____ 20___ г.

Эксперт (рецензент):

_____
(Ф.И.О., ученая степень, ученое звание, место работы, должность; если текст рецензии не прикладывается – подпись эксперта (рецензента), заверенная по месту работы)

[1] Для обеспечивающих кафедр.

2

Оглавление

1 Цели и задачи освоения дисциплины (модуля)

Дисциплина «Защита информации» **имеет целью** сформировать у обучающихся общепрофессиональные ОПК-3, ОПК-8 компетенции в соответствии с требованиями ФГОС ВО по направлению подготовки бакалавров 09.03.01 «Информатика и вычислительная техника» с учетом направленности бакалаврской программы – «Программное обеспечение вычислительной техники и автоматизированных систем».

Студенты **получают навыки** применения методов, способов и средств получения, хранения, переработки информации, навыков работы с компьютером как со средством управления информацией, навыков проведения исследований в выбранной области с использованием информационных технологий с учетом отечественного и зарубежного опыта. В задачи дисциплины входит теоретическая и практическая подготовка студентов к новым условиям работы в информационном обществе

Задачи изучения дисциплины можно сформулировать следующим образом:

- изучить законодательные и нормативные документы, регламентирующие защиту информации;
- изучить технические каналы утечки информации;
- изучить технические средства защиты компьютерной информации;
- изучить организационные меры и программно-аппаратные методы защиты компьютерной информации;
- изучить симметричные и асимметричные криптоалгоритмы;
- изучить компьютерные технологии, связанные с реализацией цифровой подписи и протоколов аутентификации.

Специфика курса учитывает особенности информационных технологий для студентов с ограниченными возможностями здоровья. Преподавание данного курса происходит с использованием адаптированной компьютерной техники.

Объектами профессиональной деятельности в рамках изучаемой дисциплины (модуля) являются:

- автоматизированные системы обработки информации и управления;
- программное обеспечение вычислительной техники и информационных систем.

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Защита информации» Б1.О.15 относится к части образовательной программы, формируемой участниками образовательных отношений, к дисциплинам (модулям) по выбору обучающихся.

Дисциплина преподаётся в VII семестре, на IV курсе.

Приступая к изучению дисциплины «Защита информации», студент имеет знания и навыки по дисциплинам: «Архитектура вычислительных систем», «Базы данных», «Операционные системы», «Структуры и алгоритмы обработки данных», «Объектно-ориентированное программирование».

На знания данной дисциплины опираются в той или иной степени дисциплины, связанные с обработкой информации.

Освоение материала дисциплины позволит студенту быть подготовленным к последующей профессиональной деятельности.

3 Планируемые результаты обучения по дисциплине (модулю)

Формируемые компетенции *(код и наименование)*	**Индикаторы достижения компетенций** *(код и формулировка)*	**Планируемые результаты обучения по дисциплине (модулю)**
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	Б-ОПК-3.1: Демонстрирует навыки решения стандартных задач обработки информации с применением информационно-коммуникационных технологий	Владеет анализом проблемной ситуации как системой
		Умеет выявлять составляющие проблемной ситуации и связи между ними
	Б-ОПК-3.2: Учитывает угрозы и обеспечивает информационную безопасность на программно-аппаратном уровне	Знает, как осуществлять критический анализ и синтез информации, полученной из разных источников. Умеет оценивать их на предмет обеспечения безопасности и защиты информации
		Владеет навыками решения нестандартных задач в сфере защиты информации с учетом основных требований информационной безопасности
		Знает основные методы оценки и предотвращения рисков разных сценариев решения профессиональных задач
		Владеет техническими средствами и методами защиты информации
ОПК-8: Способен разрабатывать алгоритмы и программы, пригодные для практического применения	ОПК-8.1 Выбирает инструментальные средства, языки программирования и технологии обработки данных на начальном этапе разработки программного продукта	Знает принципы обоснованного выбора инструментальных средств и языков программирования
		Умеет применять технологии обработки данных на начальном этапе разработки программного продукта
	ОПК-8.2 Разрабатывает алгоритмы и программные коды программных модулей для практического применения	Знает алгоритмы и программные модули, используемые в области защиты информации
		Умеет разрабатывать алгоритмы и программы для задач информационной безопасности
	ОПК-8.3 Тестирует работоспособность программ и программных компонентов	Владеет методиками тестирования работоспособности программного обеспечения
	ОПК-8.4: Применяет языки программирования и современные программные среды разработки информационных систем для решения прикладных задач различных классов	Решает прикладные задачи защиты информации с применением современных языков программирования и средств разработки

Результат обучения сформулирован с учетом следующих профессиональных стандартов:

- 06.001 «Программист», обобщённая трудовая функция C5 - Интеграция программных модулей и компонент и проверка работоспособности выпусков программного продукта; трудовая функция C/02.5 - Осуществление интеграции программных модулей и компонент и верификации выпусков программного продукта; обобщённая трудовая функция D6 - Разработка требований и проектирование программного обеспечения; трудовая функция D/01.6 - Анализ требований к программному обеспечению;
- 06.011 «Администратор баз данных», обобщённая трудовая функция B5 - Оптимизация функционирования БД; трудовая функция B/01.5- Мониторинг работы БД, сбор статистической информации о работе БД.

4 Объем дисциплины (модуля)

Объем дисциплины (модуля) составляет 2 зачетные единицы, всего 72 академических часов.

40 часов составляет контактная работа обучающегося с преподавателем, в том числе:

- 20 часов – лекционные занятия;
- 20 часов – практические занятия.

32 часов составляет самостоятельная работа обучающегося.

Промежуточный контроль (зачет с оценкой).

5 Содержание дисциплины (модуля)

_____очная____ форма обучения

Наименование и краткое содержание разделов и тем дисциплины (модуля) Форма промежуточной аттестации по дисциплине (модулю)	Всего (часы)	В том числе:											
		Контактная работа (работа во взаимодействии с преподавателем), часы из них[1]									Самостоятельная работа обучающегося, часы, из них		
		Лекционные занятия	Семинарские занятия	Практические занятия	Лабораторные занятия	…	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости (коллоквиумы, практические контрольные занятия и др.)*	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п.	**Всего**
VII семестр													
Цель и задачи курса. Информация и необходимость её защиты. Федеральный Закон РФ “Об информации, информатизации и защите информации	4	2		2						4		8	8
Классификация каналов утечки информации, источники образования технических каналов утечки, ТСПИ и ВТСС, электромагнитные каналы утечки информации, электрические каналы утечки информации.	4	2		2						4			
Пассивные методы защиты информации, активные методы защиты информации, пространственное и линейное зашумление.	12	2		2						4			
Источники угроз и воздействий на информацию, основные угрозы безопасности ИС, модель потенциального нарушителя, организационные меры защиты информационных ресурсов.	4	2		2						4			
Несанкционированный доступ к информации; виды вредоносных программ, обеспечение безопас-	4	2		2						4			

[1] Перечень видов учебных занятий уточняется в соответствии с учебным планом.

ности ИС, основные направления обеспечения защиты от НСД.													
Понятие криптографии, общие принципы безопасности передачи информации, требования к алгоритмам шифрования, виды угроз электронным документам, простейшие шифры.	12	2		2						4		8	8
Сеть Фейстеля, криптоалгоритмы DES, AES, ГОСТ28147-89	4	2		2						4			
Основные требования к алгоритмам асимметричного шифрования, основные способы использования алгоритмов с открытым ключом, алгоритм обмена ключами Диффи-Хеллмана, алгоритм RSA, электронная подпись на базе алгоритма RSA. алгоритм ЭльГамаля.	12	2		2						4		8	8
Односторонние функции, требования к хэш- функции, хэш- функция MD5. хэш- функция SHA. функция хэширования ГОСТ Р 34.11-94.	4	2		2						4			
Требования к ЭЦП, прямая и арбитражная цифровые подписи, стандарт DSS. Российский стандарт цифровой подписи ГОСТ Р 34.10.	12	2		2						4		8	8
Промежуточная аттестация зачёт с оценкой *(указывается форма проведения)***		X									X		
Итого	**72**	20		20						40		32	32

При реализации дисциплины (модуля) организуется практическая подготовка путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка при изучении дисциплины реализуется:

- непосредственно в университете (филиале);
- в структурном подразделении университета (филиала), предназначенном для проведения практической подготовки.

6 Перечень учебно-методического обеспечения по дисциплине (модулю)

Для обеспечения реализации программы дисциплины (модуля) разработаны:

– методические материалы к практическим (семинарским) занятиям;
– методические материалы по организации самостоятельной работы обучающихся;
– методические материалы по организации изучения дисциплины (модуля) с применением электронного обучения, дистанционных образовательных технологий;
– методические рекомендации для обучающихся с ограниченными возможностями здоровья и инвалидов по освоению программы дисциплины (модуля).

Методические материалы по дисциплине (модулю) и образовательной программе в целом представлены на официальном сайте образовательной организации (раздел «Сведения об образовательной организации» – Образование – Образовательные программы).

7 Фонды оценочных средств по дисциплине (модулю)

Для аттестации обучающихся на соответствие их персональных достижений поэтапным требованиям образовательной программы по дисциплине (модулю) разработаны фонды оценочных средств, позволяющие оценить результаты обучения (знания, умения, навыки) и сформированные (формируемые) компетенции.

Эти фонды включают теоретические вопросы, типовые практические задания, контрольные работы, домашние работы, тесты и иные оценочные материалы, используемые при проведении процедур текущего контроля успеваемости и промежуточной аттестации.

Фонды оценочных средств представлены в приложении к рабочей программе.

При необходимости обучающиеся с ограниченными возможностями здоровья и инвалиды обеспечиваются оценочными материалами в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа,
– в форме аудиофайла.

Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,
– в форме аудиофайла.

8 Ресурсное обеспечение

Перечень литературы

Основная учебная литература

1. Защита информации: Учебное пособие [Электронный ресурс] / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2018. - 392 с.: - (Высшее образование: Бакалавриат; Магистратура). ISBN 978-5-369-01378-6 // ЭБС "Znanium.com". - URL: http://znanium.com/catalog/product/937469 (дата обращения: 14.05.2022). Режим доступа: ограниченный по логину и паролю
2. Борисов М.А. Основы программно-аппаратной защиты информации : учебное пособие / М.А. Борисов, И.В. Заводцев, И.В. Чижов. - 4-е изд.,перераб.и доп. - М. : Ленанд, 2016. - 416 с. : ил. - (Основы защиты информации. №1.). - ISBN 978-5-9710-2667-9
3. Криптографическая защита информации [Электронный ресурс]: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — М. : РИОР : ИНФРА-М, 2018. — 321 с. — (Высшее образование). ISBN 978-5-369-01716-6 // ЭБС "Znanium.com". - URL:http://znanium.com/catalog/product/901659 (дата обращения: 14.05.2022). Режим доступа: ограниченный по логину и паролю

Дополнительная учебная литература

1. Хорев П.Б. Программно-аппаратная защита информации [Электронный ресурс]: учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). ISBN 978-5-16-107812-9, // ЭБС "Znanium.com". - URL: http://znanium.com/catalog/product/1025261 (дата обращения: 14.05.2022). Режим доступа: ограниченный по логину и паролю
2. Кияев, В. Безопасность информационных систем : учебное пособие [Электронный ресурс] / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. // ЭБС "Университетская библиотека онлайн". - URL: http://biblioclub.ru/index.php?page=book&id=429032 (дата обращения: 14.05.2022). - Режим доступа: ограниченный по логину и паролю
3. Проскурин, В.Г. Защита программ и данных: учебное пособие / В.Г. Проскурин. – М.: Издательский центр «Академия», 2012. – 208 с.: ил. (Сер. Бакалавриат). 978-5-7695-9288-1
4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие [Электронный ресурс] / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2018. - 592 с.: ил. - (Высшее образование: Бакалавриат). ISBN 978-5-8199-0730-6 // ЭБС "Znanium.com". - URL: http://znanium.com/catalog/product/937502 (дата обращения: 14.05.2022). Режим доступа: ограниченный по логину и паролю

- **Периодические издания**

1. Информационные технологии и вычислительные системы: научный журнал / Учредитель Федеральное государственное учреждение "Федеральный исследовательский центр "Информатика и управление" РАН; гл. ред. Попков Ю.С. - М.: ФГУ Федеральный исследовательский центр "Информатика и управление" РАН. – Журнал выходит 2 раза в полуг. – Основан в 1995 г. - ISSN 2071-8632. – Текст : электронный. Полные электронные версии статей журнала доступны по подписке на сайте научной электронной библиотеки «eLIBRARY.RU»: https://www.elibrary.ru/title_about_new.asp?id=8746
2. Информация и безопасность: научный журнал / Учредители: Воронежский государственный технический университет; гл. ред. Остапенко А.Г. – Воронеж: Воронежский государственный технический университет. – Журнал выходит 2 раза в полуг. - Основан в 1998 году. - ISSN 1682-7813. – Текст : электронный. Полные электронные версии статей журнала доступны на сайте научной электронной библиотеки «eLIBRARY.RU»: http://elibrary.ru/contents.asp?titleid=8748
3. Информатика и системы управления: научное издание / Учредитель: Амурский государственный университет; гл. ред. Е.Л. Еремин. – Благовещенск: Амурский государствен-

ный университет. – журнал выходит 2 раза в полуг. - Основан в 2001 г. – ISSN: 1814-2400. - Текст : электронный. Полные электронные версии статей журнала доступны на сайте научной электронной библиотеки «eLIBRARY.RU»: https://www.elibrary.ru/contents.asp?titleid=9793

4. Открытые системы СУБД / Учредитель: ООО «Издательство «Открытые системы»; гл. ред. Д. Волков. – М.: Издательство «Открытые системы». – журнал выходит 2 раза в полуг. - Основан в 1993 году. – ISSN: 1028-7493. - – Текст : электронный. – Полные электронные версии статей представлены на сайте журнала: https://www.osp.ru/os/archive
5. Программные продукты и системы: международный научно-практический журнал / Учредитель: Куприянов В.П.; гл. ред. Савин Г.И. - Тверь: Центрпрограммсистем. – журнал выходит 2 раза в полуг. - Основан в 1988 году. – ISSN: 0236-235X. – Текст : электронный. – Полные электронные версии статей представлены на сайте журнала: http://swsys.ru/
6. Российские нанотехнологии: научный журнал / Учредитель: НИЦ "Курчатовский институт"; гл. ред. Ковальчук М.В. – М.: Общество с ограниченной ответственностью Парк-медиа – Журнал выходит 6 раз в год. – Основан в 2006 году. - ISSN 1993-4068. – Текст : электронный. – Полные электронные версии статей представлены на сайте журнала: https://nanorf.elpub.ru/jour/issue/viewIssue/16/15#
7. Системный администратор / Учредитель: "Издательский дом "Положевец и партнеры"; гл. ред. Г. Положевец. – М.: Общество с ограниченной ответственностью "Издательский дом "Положевец и партнеры". – Журнал выходит 12 раз в год. - Основан в 2002 году. - ISSN 1813-5579. – Текст : электронный. Полные электронные версии статей журнала доступны по подписке на сайте научной электронной библиотеки «eLIBRARY.RU»: https://elibrary.ru/title_about.asp?id=9973

- **Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

Электронно-библиотечные системы и базы данных

1. ЭБС «Znanium.com»: http://znanium.com/
2. ЭБС «Лань»: https://e.lanbook.com/
3. ЭБС «Юрайт»: https://biblio-online.ru/
4. ЭБС «Университетская библиотека онлайн»: http://biblioclub.ru/
5. Научная электронная библиотека (РУНЭБ) «eLIBRARY.RU»: http://elibrary.ru
6. Национальная электронная библиотека (НЭБ): http://нэб.рф/
7. Базы данных российских журналов компании «East View»: https://dlib.eastview.com/

Научные поисковые системы

1. ArXiv.org - научно-поисковая система, специализируется в областях: компьютерных наук, астрофизики, физики, математики, квантовой биологии. http://arxiv.org/
2. Google Scholar - поисковая система по научной литературе. Включает статьи крупных научных издательств, архивы препринтов, публикации на сайтах университетов, научных обществ и других научных организаций. https://scholar.google.ru/
3. WorldWideScience.org - глобальная научная поисковая система, которая осуществляет поиск информации по национальным и международным научным базам данных и порталам. http://worldwidescience.org/
4. SciGuide - навигатор по зарубежным научным электронным ресурсам открытого доступа. http://www.prometeus.nsc.ru/sciguide/page0601.ssi

Профессиональные ресурсы сети «Интернет»

1. Федеральная информационная система «Единое окно доступа к информационным ресурсам»: http://window.edu.ru/.
2. Проект Инициативного Народного Фронта Образования - ИНФО-проект. Школа программирования Coding Craft http://codingcraft.ru/.
3. Портал Life-prog http://life-prog.ru/.
4. OpenNet www.opennet.ru.
5. Алгоритмы, методы, программы algolist.manual.ru.
6. Сервер министерства высшего образования www.informika.ru.

- **Перечень информационных технологий, используемых при осуществлении образовательного процесса, включая программное обеспечение, информационные справочные системы** *(при необходимости)*

Проведение лекционных занятий предполагает использование комплектов слайдов и программных презентаций по рассматриваемым темам.

Проведение практических занятий по дисциплине предполагается использование специализированных аудиторий, оснащенных персональными компьютерами, объединенными в локальную сеть и имеющих доступ к ресурсам глобальной сети Интернет.

Для выполнения заданий самостоятельной подготовки обучающиеся обеспечиваются литературой, а также в определённом порядке могут получать доступ к информационным ресурсам Интернета.

Дисциплина обеспечена необходимым программным обеспечением, которое находится в свободном доступе (программы Open office, свободная лицензия, код доступа не требуется).

В филиале «Протвино» государственного университета «Дубна» созданы условия для обучения людей с ограниченными возможностями: использование специальных образовательных программ и методов обучения, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающим обучающимся необходимую техническую помощь, обеспечение доступа в здания организации.

Имеется универсальное средство для подъема и перемещения инвалидных колясок – пандус-платформа складной.

Компьютерные классы оборудованы столами для инвалидов с ДЦП, также здесь оборудованы рабочие места для лиц с ОВЗ: установлены специальный программно-технологический комплекс позволяющий работать на них студентам с нарушением опорно-двигательного аппарата, слабовидящим и слабослышащим. Имеются гарнитуры компактные, беспроводная клавиатура с большими кнопками, беспроводной компьютерный джостик с двумя выносными кнопками, беспроводной ресирвер, беспроводная выносная большая кнопка, портативное устройство для чтения печатных материалов.

Специальные учебники, учебные пособия и дидактические материалы, в том числе в формате печатных материалов (крупный шрифт или аудиофайлы) имеются в ЭБС, на которые подписан филиал.

Наличие на сайте справочной информации о расписании учебных занятий в адаптированной форме доступной для обучающихся с ограниченными возможностями здоровья, являющихся слепыми или слабовидящими.

- **Описание материально-технической базы**

Компьютерный класс (15 ПК) (оборудование в собственности)

Обучающиеся из числа инвалидов и лиц с ограниченными возможностями здоровья могут использовать специализированное программное и материально-техническое обеспечение:

- обучающиеся с нарушениями опорно-двигательного аппарата при необходимости могут использовать адаптивные технические средства: специально оборудованные джойстики, увеличенные выносные кнопки, клавиатуры с большими клавишами.
- обучающиеся с ограничениями по зрению могут прослушать доступный аудиоматериал или прочитать тексты, увеличив шрифт на экране монитора компьютера. Рекомендуется использовать экранную лупу и другие визуальные вспомогательные средства, чтобы изменить шрифт текста, межстрочный интервал, синхронизацию с речью и т.д., программы экранного доступа (скринридеры для прочтения текстовой информации через синтезированную речь) и/или включить функцию «экранного диктора» на персональном компьютере с операционной системой Windows 7, 8, 10.
- обучающиеся с ограничениями по слуху могут воспользоваться компьютерной аудиогарнитурой при прослушивании необходимой информации и портативной индукционной системой серии «ИСТОК».

При необходимости обучающиеся с ограниченными возможностями здоровья и инвалиды обеспечиваются печатными и (или) электронными образовательными ресурсами (образовательная программа, учебные пособия и др.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла.

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Приложение к рабочей программе дисциплины

Фонды оценочных средств

В результате освоения дисциплины «Защита информации» программы бакалавров по направлению подготовки 09.03.01 «Информатика и вычислительная техника» с учетом направленности бакалаврской программы – «Программное обеспечение вычислительной техники и автоматизированных систем» выпускник должен обладать следующими компетенциями:

Общепрофессиональные компетенции:

Компетенция 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

код и формулировка компетенции

Описание показателей и критериев оценивания компетенций, а также шкал оценивания

Компетенция 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

ИНДИКАТОР ДОСТИЖЕНИЯ КОМПЕТЕНЦИИ (код и наименование)	**КРИТЕРИИ ОЦЕНИВАНИЯ ШКАЛА оценивания**				
	1	**2**	**3**	**4**	**5**
Б-ОПК-3.1. Демонстрирует навыки решения стандартных задач обработки информации с применением информационно-коммуникационных технологий	Отсутствие умений	Демонстрирует частичное умение анализировать проблемную ситуацию как систему, выявляя ее составляющие и связи между ними Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение анализировать проблемную ситуацию как систему, выявляя ее составляющие и связи между ними Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое умение анализировать проблемную ситуацию как систему, выявляя ее составляющие и связи между ними Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение анализировать проблемную ситуацию как систему, выявляя ее составляющие и связи между ними Не допускает ошибок.
Владеть анализом проблемной ситуации как системой Уметь выявлять составляющие проблемной ситуации и связи между ними					

Б-ОПК-3.2. Учитывает угрозы и обеспечивает информационную безопасность на программно-аппаратном уровне	Отсутствие умений	Демонстрирует частичное умение учитывать угрозы и обеспечивает информационную безопасность на программно-аппаратном уровне Допускает множественные грубые ошибки.	Демонстрирует удовлетворительное умение учитывать угрозы и обеспечивает информационную безопасность на программно-аппаратном уровне Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивое умение учитывать угрозы и обеспечивает информационную безопасность на программно-аппаратном уровне Допускает отдельные негрубые ошибки.	Демонстрирует устойчивое умение учитывать угрозы и обеспечивает информационную безопасность на программно-аппаратном уровне Не допускает ошибок.
Знать, как осуществлять критический анализ и синтез информации, полученной из разных источников. Уметь оценивать их на предмет обеспечения безопасности и защиты информации Знать основные методы оценки и предотвращения рисков разных сценариев решения профессиональных задач Владеть навыками решения нестандартных задач в сфере защиты информации с учетом основных требований информационной безопасности Владеть техническими средствами и методами защиты информации					

Компетенция ОПК-8 – способен разрабатывать алгоритмы и программы, пригодные для практического применения

ИНДИКАТОР ДОСТИЖЕНИЯ КОМПЕТЕНЦИИ (код и наименование)	**КРИТЕРИИ ОЦЕНИВАНИЯ ШКАЛА оценивания**				
	1	**2**	**3**	**4**	**5**
Б-ОПК-8.1: Выбирает инструментальные средства, языки программирования и технологии обработки данных на начальном этапе разработки программного продукта	Отсутствие знаний и умений	Демонстрирует частичные знания и умения принципов обоснованного выбора инструментальных средств и языков программирования; умений применять технологии обработки данных на начальном этапе	Демонстрирует удовлетворительные умения принципов обоснованного выбора инструментальных средств и языков программирования; умений применять технологии обработки данных на начальном этапе	Демонстрирует достаточно устойчивые умения принципов обоснованного выбора инструментальных средств и языков программирования; умений применять технологии обработки данных на начальном этапе раз-	Демонстрирует устойчивые знания и умения принципов обоснованного выбора инструментальных средств и языков программирования; умений применять технологии обработки данных на начальном этапе

		разработки программного продукта Допускает множественные грубые ошибки.	разработки программного продукта Допускает достаточно серьезные ошибки	работки программного продукта Допускает отдельные негрубые ошибки.	разработки программного продукта Не допускает ошибок.
Б-ОПК-8.2: Разрабатывает алгоритмы и программные коды программных модулей для практического применения.	Отсутствие знаний и умений	Демонстрирует частичные знания и умения разрабатывать алгоритмы и программы для задач информационной безопасности; существующих алгоритмов и программных модулей, используемых в области защиты информации Допускает множественные грубые ошибки.	Демонстрирует удовлетворительные умения разрабатывать алгоритмы и программы для задач информационной безопасности; существующих алгоритмов и программных модулей, используемых в области защиты информации Допускает достаточно серьезные ошибки	Демонстрирует достаточно устойчивые умения разрабатывать алгоритмы и программы для задач информационной безопасности; существующих алгоритмов и программных модулей, используемых в области защиты информации Допускает отдельные негрубые ошибки.	Демонстрирует устойчивые знания и умения разрабатывать алгоритмы и программы для задач информационной безопасности; существующих алгоритмов и программных модулей, используемых в области защиты информации Не допускает ошибок.
Б-ОПК-8.3: Тестирует работоспособность программ и программных компонентов.	Отсутствие владений	Демонстрирует частичные навыки владения решения	Демонстрирует удовлетворительные навыки владения	Демонстрирует достаточно устойчивые навыки владения	Демонстрирует устойчивые навыки владения решения

Б-ОПК-8.4: Применяет языки программирования и современные программные среды разработки информационных систем для решения прикладных задач различных классов.		прикладных задач защиты информации с применением современных языков программирования и средств разработки Допускает множественные грубые ошибки.	решения прикладных задач защиты информации с применением современных языков программирования и средств разработки Допускает достаточно серьезные ошибки	решения прикладных задач защиты информации с применением современных языков программирования и средств разработки Допускает отдельные негрубые ошибки.	прикладных задач защиты информации с применением современных языков программирования и средств разработки Не допускает ошибок.

При балльно-рейтинговой системе все знания, умения и навыки, приобретаемые студентами в результате изучения дисциплины, оцениваются в баллах.

Оценка качества работы в рейтинговой системе является накопительной и используется для оценивания системной работы студентов в течение всего периода обучения.

По итогам работы в семестре студент может получить максимально **70** баллов. Итоговой формой контроля в VIII семестре является экзамен. На экзамене студент может набрать максимально **30** баллов.

В течение VIII семестра студент может заработать баллы за следующие виды работ:

№	Вид работы	Сумма баллов
1	Работа на практических занятиях	20
2	Устный опрос на практическом/семинарском занятии (УО-1.1)	10
3	Устный опрос на практическом/семинарском занятии (УО-1.2)	10
4	Устный опрос на практическом/семинарском занятии (УО-1.3)	10
5	Тест по теоретическому материалу дисциплины (ПР-1)	12
6	Аудиторные занятия (посещение)	8
	Итого:	70

Если к моменту окончания семестра студент набирает от **51** до **70** баллов, то он получает допуск к экзамену.

Если студент к моменту окончания семестра набирает от **61** до **70** баллов, то он может получить автоматическую оценку «удовлетворительно». При желании повысить свою оценку, студент имеет право отказаться от автоматической оценки и сдать экзамен.

Если студент не набрал минимального числа баллов (**51** балл), то он не получает допуск к экзамену.

Соответствие рейтинговых баллов и академических оценок

Общая сумма баллов за семестр	Итоговая оценка
86-100	Отлично
71-85	Хорошо
51-70	Допуск к экзамену
в том числе: 61-70	Возможность получения автоматической оценки «удовлетворительно»
51-60	Только допуск к экзамену

0-50 *	Неудовлетворительно (студент не допущен к экзамену)

Текущий контроль успеваемости осуществляется в процессе выполнения практических и самостоятельных работ в соответствии с ниже приведенным графиком.

График выполнения самостоятельных работ студентами в VIII семестре

Виды работ	Недели учебного процесса																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
УО-1.1	ВЗ		ЗЗ														
УО-1.2				ВЗ		ЗЗ											
УО-1.3							ВЗ		ЗЗ								
ПР-1										ВЗ/ ЗЗ							

ВЗ – выдача задания
ЗЗ – защита задания

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

– в печатной форме,
– в печатной форме увеличенным шрифтом,
– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

При необходимости обучающемуся инвалиду и лицу с ОВЗ предоставляется дополнительное время для подготовки ответа на зачете или экзамене. У обучающегося инвалида и лица с ОВЗ имеется возможность выбора формы контроля на практических занятиях, зачетах, экзаменах, подходящая конкретно для него

Методические указания к практическим занятиям

1) Изучение криптографических методов подстановки и замены.
2) Двухключевые системы защиты информации (криптосистемы с открытым ключом)
3) Использование генераторов псевдослучайных чисел для формирования цифровых ключей
4) Изучение методов гаммирования.
5) Зашифрование информации многоалфавиным шифром по алгоритму Виженера
6) Расшифрование информации многоалфавиным шифром по алгоритму Виженера
7) Вычисление открытого и закрытого ключей асимметричного алгоритма RSA методом решения Диофантовых уравнений
8) Зашифрование информации по асимметричному алгоритму RSA
9) Расшифрование информации по асимметричному алгоритму RSA
10) Генерация ЭЦП на основе алгоритма RSA.Оформление результатов работы

Методическое обеспечение инновационных форм учебных занятий

Разбор конкретных ситуаций применения методов обеспечения информационной безопасности

Инновационные формы проведения учебных занятий

Семестр	Вид учебных занятий[2]	Используемые инновационные формы проведения учебных занятий	Количество академ. часов
VII	Лекционные занятия	Разбор конкретных ситуаций при рассмотрении способов и методов защиты информационной безопасности	16
VII	Практические занятия	Разбор конкретных ситуаций при рассмотрении способов и методов защиты информационной безопасности	8
		Всего:	24

Методические указания для самостоятельной работы обучающихся и прочее

№ п/п	*№ раздела дисциплины*	*Содержание самостоятельной работы*	*Трудоемкость*
1	1-3	УО-1.1. Основы построения моделей и методов оценки защищенности вычислительных систем	8
2	4-6	УО-1.2. Основы информационной безопасности систем и сетей передачи данных	8
3	7-8	УО-1.3. Требования и этапы составления схемы проверки системы защиты информации, включая организационные, технические, аппаратно-программные и криптографические средства защиты.	8
4	1-10	ПР-1.4. Теоретический материал по всем разделам дисциплины	8

Перечень обязательных видов учебной работы студента:

- *посещение лекционных занятий;*
- *ответы на теоретические вопросы на практических занятиях;*
- *решение практических задач и заданий на практических занятиях;*

В случае использования инновационных форм проведения учебных занятий приводится перечень инновационных форм проведения учебных занятий (по видам учебных занятий).

Список вопросов к экзамену

1. Активные методы защиты информации.
2. Алгоритм RSA
3. Алгоритм обмена ключами Диффи-Хеллмана.
4. Алгоритм симметричного шифрования Rijndael. Нелинейное преобразование.
5. Алгоритм Эль Гамаля.
6. Информация и необходимость ее защиты.
7. Источники угроз и воздействий на информацию.
8. Модель потенциального нарушителя.
9. Обеспечение безопасности автоматизированных систем.
10. Основные направления обеспечения защиты от НСД.
11. Основные способы использования алгоритмов с открытым ключом.
12. Основные требования к алгоритмам асимметричного шифрования.
13. Основные угрозы безопасности АС.
14. Пассивные методы защиты информации.
15. Пространственное и линейное зашумление.

[2] Перечень видов учебных занятий уточняется в соответствии с учебным планом.

16. Российский стандарт цифровой подписи ГОСТ Р 34.10-94.
17. Стандарт цифровой подписи DSS.
18. Требования к электронной цифровой подписи.
19. Функция хеширования ГОСТ Р 34.11-94.
20. Хеш-функция MD5.
21. Хеш-функция SHA.
22. Электрические каналы утечки информации.
23. Электромагнитные каналы утечки информации.
24. Электронная цифровая подпись на базе алгоритма RSA.

Варианты вопросов к устному опросу по теме 1-3 (УО-1.1)

1. Какие угрозы существуют электронным документам, при обмене информацией между пользователями.
2. Сформулируйте основную задачу защиты данных.
3. Перечислите возможные угрозы защищаемым сведениям.
4. Какие виды уязвимостей компьютерных систем вы знаете?

Варианты вопросов к устному опросу по теме 4-6 (УО-1.2)

1. Перечислите области использования криптографических методов защиты информации.
2. Перечислите задачи, решаемые современной криптографией.
3. Сформулируйте классификацию криптографических систем защиты информации.
4. Перечислите определения: алфавит, текст, криптограмма, криптоалгоритм, криптографическая система, шифр, зашифрование, расшифрование.

Варианты вопросов к устному опросу по теме 7-8 (УО-1.3)

1. Перечислите асимметричные алгоритмы, используемые в современной практике защиты информации.
2. Напишите порядок вычисления закрытого ключа пользователя в криптоалгоритме RSA.
3. Напишите порядок вычисления общего секретного ключа пользователя в алгоритме Диффи-Хеллмана.
4. Напишите порядок зашифрования данных в алгоритме Эль Гамаля.

Варианты тестов (ПР-1)

1) Какие существуют основные уровни обеспечения защиты информации?
   а) Законодательный
   б) Организационно-административный
   в) Программно-технический (аппаратный)
   г) Физический
   д) Вероятностный
   е) Распределительный

2) Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?
   а) Доступность
   б) Целостность
   в) Конфиденциальность
   г) Управляемость
   д) Сложность

3) Какое определение информации дано в Законе РФ "Об информации, информатизации и защите информации"?
   а) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления

б) Получение сведений из глобальной информационной сети
в) Систематизированные данные об экономике
г) Это результаты компьютерных решений определенных задач

4) Какие угрозы безопасности информации являются преднамеренными?
а) Взрыв в результате теракта
б) Поджог
в) Забастовка
г) Ошибки персонала
д) Неумышленное повреждение каналов связи
е) Некомпетентное использование средств защиты
ж) Утрата паролей, ключей, пропусков
з) Хищение носителей информации
и) Незаконное получение паролей

5) Что такое коммерческая тайна?
а) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам
б) Информация, к которой нет доступа на законном основании
в) Информации, обладатель которой принимает меры к охране ее конфиденциальности
г) Информация, содержащая в учредительных документах
д) Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов

6) Какие правовые документы решают вопросы информационной безопасности?
а) Уголовный кодекс РФ
б) Конституция РФ
в) Закон "Об информации, информатизации и защите информации"
г) Закон РФ "О государственной тайне"
д) Закон РФ "О коммерческой тайне"
е) Закон РФ "О лицензировании отдельных видов деятельности"
ж) Закон РФ "Об образовании"
з) Закон РФ " Об электронной цифровой подписи "

7) Что относится к средствам подотчетности согласно «Оранжевой книге»?
а) Идентификация и аутентификация
б) Предоставление доверенного пути
в) Анализ регистрации информации
г) Копирование файлов
д) Администрирование системы

8) Что относится к средствам сетевых механизмов безопасности согласно «Рекомендациям X.800»?
а) Шифрование
б) Электронная цифровая подпись
в) Механизмы контроля целостности данных
г) Механизмы аутентификации
д) Механизмы дополнения трафика
е) Механизмы управления маршрутизацией
ж) Механизмы нотаризации
з) Настройка ip адресов системы

9) Каковы меры управления персоналом для обеспечения информационной безопасности?
а) Описание должности (должностных обязанностей)
б) Разделение обязанностей
в) Минимизация привилегий
г) Обучение
д) Подбор кадров
е) Подбор программно-технических средств
ж) Аттестация персонала

10) Что относится к основным способам физической защиты?
а) Физическое управление доступом
б) Противопожарные меры
в) Защита поддерживающей инфраструктуры
г) Защита от перехвата данных
д) Защита мобильных систем
е) Проведение производственной зарядки
ж) Проведение соревнований по профессиональному мастерству

11) Что относится к средствам физической защиты информации?

а) Пропускная система на предприятиях
б) Ограждения на предприятиях
в) Документирование
г) Системы видео наблюдения на предприятиях
д) Резервное копирование
е) Средства защиты от пожаров
ж) Средства защиты от жары, холода, влаги, магнетизма
з) Индивидуальные средства защиты
и) Противорадиационные средства защиты
к) Анализ требований к защищаемому сервису
л) Информатизация защищаемого сервиса, установленного на предприятии

12) Какие имеются основные направления обеспечения информационной безопасности, связанные с человеческим фактором?
а) Разделение обязанностей
б) Минимизация привилегий
в) Описание должности (должностные инструкции)
г) Обучение персонала информационной безопасности
д) Планирование требований к защищаемому серверу
е) Информатизация защищаемого сервиса, установленного на предприятии
ж) Противорадиационные средства защиты
з) Индивидуальные средства защиты

13) Какие имеются методы и средства поиска и уничтожения известных вирусов?
а) Метод сканирования и сравнения с уникальным фрагментом программного кода, находящимся в базе данных кодов известных компьютерных вирусов.
б) Метод проведения математических вычислений по заранее известным алгоритмам
в) Метод сравнения количества значений равных 0 с количеством значений равных 1
г) Метод сравнения контрольных служебных значений файлов

14) Какие имеются методы и средства поиска и уничтожения неизвестных вирусов

а) Метод контроля целостности системы (обнаружение изменений)
б) Метод проведения математических вычислений по заранее известным алгоритмам
в) Метод выявления создателей вирусов
г) Метод проверки наличия служебных символов в файле

15) Что относится к идентификации и/или аутентификации людей на основе их физиологических характеристик?
а) Анализ особенностей голоса
б) Распознавание речи
в) Отпечатки пальцев
г) Сканирование радужной оболочки глаза
д) Анализ знаний по информационной безопасности

16) Что относится к идентификации и/или аутентификации людей на основе их поведенческих характеристик?
а) Анализ динамики подписи (ручной)
б) Анализ стиля работы с клавиатурой
в) Анализ отпечатков пальцев
г) Анализ административных указаний по информационной безопасности
д) Отпечатки пальцев

17) Что такое открытый ключ электронной цифровой подписи?
а) Уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.
б) Последовательность символов, изготавливаемая любым пользователем информационной системы по своему усмотрению, предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе
в) Ключ электронной цифровой подписи, который стал известен в результате разведывательных, хакерских или других операций
г) Ключ электронной цифровой подписи, которым шифруют заголовки электронных документов для установления подлинности владельца

18) Что такое доступность информации?
а) Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия
б) Свойство системы, обеспечивать беспрепятственный доступ к информации любых субъектов
в) Свойство системы, обеспечивать закрытый доступ к информации любых субъектов
г) Свойство информации, заключающееся в легкости ее несанкционированного получения и дальнейшего распространения (несанкционированного копирования)

19) Что такое целостность информации?
а) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)
б) Свойство информации, заключающееся в возможности ее изменения любым субъектом
в) Свойство информации, заключающееся в возможности изменения только единственным пользователем
г) Свойство информации, заключающееся в ее существовании в виде единого набора файлов

20) Какие угрозы безопасности информации являются непреднамеренными?
а) Взрыв в результате теракта
б) Поджог
в) Забастовка
г) Ошибки персонала
д) Неумышленное повреждение каналов связи
е) Некомпетентное использование средств защиты
ж) Утрата паролей, ключей, пропусков
з)Хищение носителей информации

21) Что относится к правовым мерам защиты информации?

а) Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения
б) Действия правоохранительных органов для защиты информационных ресурсов
в) Организационно-административные меры для защиты информационных ресурсов
г) Действия администраторов сети защиты информационных ресурсов

22) Что такое лицензия?
а) Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю
б) Перечень документов, которыми организация пользуется для засекречивания информации
в) Осуществление любых видов деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю
г) Разрешение на осуществление любого вида деятельности выданное юридическому лицу или индивидуальному предпринимателю
д) Документы, подтверждающие уровень защиты информации

23) Что такое сертификация?
а) Подтверждение соответствия продукции или услуг установленным требованиям или стандартам
б) Процесс подготовки к изготовлению программно-технических средств защиты информации
в) Документы, по которым происходит процесс засекречивания программно-технических средств
г) Административное управление информационной безопасностью

24) Какой основной документ по информационной безопасности Гостехкомиссии при Президенте РФ?
а) Руководящие документы по защите от несанкционированного доступа
б) Руководство по защите баз данных
в) Устав предприятия по защите информации

25) Что понимается под средством физического управления доступом?
а) Механические, электронно-механические устройства и сооружения, специально предназначенные для созданияфизических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к защищаемой информации
б) Силовые действия охраны организации против потенциальных нарушителей
в) Указания в инструкциях на мероприятия по подержанию физической формы сотрудников
г) Программные меры защиты, предназначенные для создания препятствий потенциальным нарушителям
д) Информационное обеспечение секретных задач

26) Каковы основные принципы построения систем физической защиты?
а) Принцип системности
б) Принцип непрерывности защиты
в) Принцип разумной достаточности
г) Гибкость управления и применения
д) Простота применения защитных мер и средств
е) Установка препятствий по мере сложности преодоления
ж) Установка обязательной связи звуковой и телевизионной сигнализации

27) Что такое несанкционированный доступ (нсд)?
а) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

б) Создание резервных копий в организации
в) Правила и положения, выработанные в организации для обхода парольной защиты
г) Вход в систему без согласования с руководителем организации
д) Удаление не нужной информации

28) Что такое идентификация?
а) Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации
б) Указание на правильность выполненных операций по защите информации
в) Определение файлов, которые изменены в информационной системе несанкционированно
г) Выполнение процедуры засекречивания файлов
д) Процесс периодического копирования информации

29) Что относится к идентификации и/или аутентификации людей на основе их поведенческих характеристик?
а) Специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы
б) Методы защиты информации с помощью контрольных сумм
в) Методы защиты информации организационньми мероприятиями
г) Методы защиты информации с использование пароля
д) Физические методы передачи данных

30) Что такое симметричный метод шифрования?
а) Криптографический метод защиты информации, где для шифрования и дешифрования используется один и тот же ключ, сохранение которого в секрете обеспечивает надежность защиты
б) Метод защиты информации, где для шифрования используется открытый ключ, для дешифрования используется закрытый ключ
в) Преобразование, которое позволяет пользователям проверить авторство и подлинность
г) Метод защиты информации, где шифрование и дешифрование производят набором симметричных ключей

31) Что такое электронная цифровая подпись?
а) Реквизит электронного документа, предназначенный длязащиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе
б) Набор цифр персонально закрепленных за пользователями, неразрешенных к использованию любыми другими пользователями
в) Индивидуальный код, известный ограниченному кругу пользователей и зашифрованный симметричным ключом
г) Возможность зашифровывать сообщения индивидуальным (собственным) ключом
д) Электронный документ, достоверность которого подтверждена удостоверяющим центром

32) Что такое закрытый ключ электронной цифровой подписи?
а) Уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
б) Ключ электронной цифровой подписи, который зашифрован с помощью единственного симметричного ключа владельца
в) Ключ электронной цифровой подписи, который хранится отдельно от других закрытый ключей
г) Ключ электронной цифровой подписи, которым шифруют заголовки электронных документов для установления подлинности владельца

33) Что такое Хэш-функция?
а) Труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков
б) Уникальный метод шифрования и дешифрования информации
в) Выполнение предварительных операций перед шифрованием и дешифрованием
г) Функция распределения файлов по названиям и принадлежности к определенным документам

34) Что такое конфиденциальность информации?
а) Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ кданной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней
б) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)
в) Свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора
г) Свойство информации, заключающееся в ее шифрования
д) Свойство информации, заключающееся в ее принадлежности к определенному набору

35) Что относится к угрозам информационной безопасности?

а) Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию
б) Классификация информации
в) Стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.)
г) Сбои и отказы оборудования (технических средств) АС
д) Ошибки эксплуатации (пользователей, операторов и другого персонала)
е) Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)
ж) Последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.)
з) Иерархическое расположение данных

36) Какие имеются виды правовой ответственности за нарушение законов в области информационной безопасности?
а) Уголовная
б) Административно-правовая
в) Гражданско-правовая
г) Дисциплинарная
д) Материальная
е) Условная
ж) Договорная

37) Что такое государственная тайна?
а) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ
б) Сведения о состоянии окружающей среды
в) Все сведения, которые хранятся в государственных базах данных
г) Сведения о состоянии здоровья президента РФ
д) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне

38) Какие документы относятся к основным международным документы по информационной безопасности?
а) Критерии оценки доверенных компьютерных систем (Оранжевая книга)
б) Рекомендации X.800
в) Критерии оценки безопасности информационных технологий (Стандарт ISO/IEC 15408)
г) Рекомендации X.400
д) Международный закон по информационной безопасности

39) Что включает в себя политика безопасности согласно «Оранжевой книге»?
а) Произвольное управление доступом
б) Безопасность повторного использования объектов
в) Метки безопасности
г) Принудительное управление доступом
д) Переговоры между организациями

40) Что такое политика информационной безопасности организации
а) Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию
б) Уничтожение, модификация, копирование информации в организации
в) Набор административных документов, утвержденных в организации
г) Совокупность механизмов компьютерных систем
д) Инструкции администраторам по настройке информационных систем

41) Что входит в задачи службы безопасности организации?
а) Выявление лиц, проявляющих интерес к коммерческой тайне предприятия
б) Разработка системы защиты секретных документов
в) Определение уязвимых участков на предприятии, аварии или сбои в работе которых могут нанести урон предприятию
г) Планирование, обоснование и организация мероприятий по защите информации
д) Взаимодействие с Управлением внутренних дел
е) Определение сведений, составляющих коммерческую тайну
ж) Арест нарушителей информационной безопасности

42) Какие действия являются реагированием на нарушение режима информационной безопасности организации?
а) Локализация и уменьшение вреда
б) Выявление нарушителя
в) Предупреждение повторных нарушений
г) Судебное рассмотрение
д) Проведение общего собрания организации

43) Что относится к основным организационным мероприятиям, направленным на поддержание работоспособности информационных систем?
а) Резервное копирование
б) Поддержка программного обеспечения
в) Документирование
г) Регламентные работы
д) Усложнение управления техническими средствами
е) Выполнение нескольких операций одним оперативно-техническим персоналом

44) Что такое аутентификация?
а) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).
б) Нахождение файлов, которые изменены в информационной системе несанкционированно
в) Проверка количества переданной и принятой информации
г) Определение файлов, из которых удалена служебная информация
д) Определение файлов, из которых удалена служебная информация

45) Какими способами обеспечиваются основные уровни антивирусной защиты?
а) Поиск и уничтожение известных вирусов
б) Поиск и уничтожение неизвестных вирусов
в) Блокировка проявления вирусов
г) Определения адреса отправителя вирусов
д) Выявление создателей вирусов

46) На каких методах основана блокировка проявления вирусов
а) На методах перехвата характерных для вирусов функций
б) На методах вероятностного проявления кодов разрушения файлов
в) На методах проверок и сравнениях с контрольной копией

47) Какие меры позволяют повысить надежность парольной защиты?
а) Наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.)
б) Управление сроком действия паролей, их периодическая смена
в) Ограничение доступа к файлу паролей
г) Ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы") обучение пользователей
д) Выбор простого пароля (имя подруги, название спортивной команды)

48) Какие методы применяются в криптографических методах защиты информации?
а) Подстановка
б) Перестановка
в) Аналитическое преобразование
г) Комбинированное преобразование
д) Замена контрольными суммами
е) Замена только цифр

49) Что такое асимметричный метод шифрования?
а) Метод защиты информации, где для шифрования и дешифрования информации используются различные ключи
б) Метод защиты информации, где для шифрования и дешифрования информации используются больше трех ключей
в) Метод защиты информации, где для шифрования и дешифрования информации используют астрономические методы
г) Метод защиты информации, где шифрование и дешифрование информации осуществляют без ключа

50) Что такое лицензия?
а) Специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю
б) Перечень документов, которыми организация пользуется для засекречивания информации
в) Осуществление любых видов деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю
г) Разрешение на осуществление любого вида деятельности выданное юридическому лицу или индивидуальному предпринимателю
д) Документы, подтверждающие уровень защиты информации

Процедура промежуточной аттестации проходит в соответствии с «Положением балльно-рейтинговой системе оценки и текущем контроле успеваемости студентов», а также «Положением о промежуточной аттестации» университета «Дубна».

Адаптированная рабочая программа учебной дисциплины (модуля) разработана в отношении разнонозологической учебной группы обучающихся, имеющих документально подтвержденные нарушения слуха, зрения, опорно-двигательного аппарата, соматические заболевания и поддающиеся коррекции нервно-психические нарушения или сочетанные нарушения.

Содержание зачётного билета

1 вопрос – фундаментальная теория (знать + уметь)

2 вопрос – практическая комплексная задача (уметь + владеть)

Пример составления экзаменационного билета:

1 вопрос. Угрозы и уязвимости компьютерной системы

2 вопрос. Построить цифровой ключ, используя биквадратичный генератор псевдослучайных числе, имея порождающее число 2316.