

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный гуманитарно-педагогический университет имени В.М. Шукшина»
(АГПУ имени В.М. Шукшина)

Кафедра математики, физики, информатики

Утверждаю
проректор по учебной работе
М.В. Довыдова
«26» августа 2022 г.



ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.06.05 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки

**44.03.05 Педагогическое образование
(с двумя профилями подготовки)**

Профиль подготовки

Технология и Информатика

Квалификация

бакалавр

Форма обучения

очная

Составитель:

доктор физ.-мат. наук, профессор

П.В. Захаров

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УЧЕБНОМ ПРОЦЕССЕ

на заседании кафедры математики, физики, информатики

(протокол от 22 июня 2022 г. № 9)

Заведующий кафедрой
математики, физики, информатики _____



Т.А. Гусева

1. Цель и задачи дисциплины

Целью изучения данного курса является формирование у студентов понимания основ компьютерной безопасности, основных видов информационных угроз и средств защиты от них.

Задачи изучения дисциплины:

- усвоить основные понятия информационной безопасности;
- изучить угрозы информационной безопасности;
- познакомить с инженерно-техническими и программно-аппаратными методами и средствами защиты информации;
- изучить методы и средства защиты информации от несанкционированного доступа в компьютерные системы;
- изучить методы и приемы аутентификация пользователей;
- дать представление о криптографических методах информационной безопасности;
- познакомить с возможностями компьютерных вирусов;
- познакомить с возможностями антивирусных пакетов;
- привить навыки работы с антивирусными пакетами.

2. Место дисциплины в структуре ОПОП

Дисциплина «Методы и средства защиты информации» (Б1.О.06.05) относится к профессиональному циклу дисциплин и входит в состав вариативной части ОПОП. Областью профессиональной деятельности бакалавров, на которую ориентирует дисциплина «Методы и средства защиты информации» является процесс управления информацией с помощью информационных технологий.

Для освоения дисциплины «Методы и средства защиты информации» обучающиеся используют знания и умения, сформированные при изучении дисциплины «Операционные системы, сети и интернет-технологии».

Дисциплина «Методы и средства защиты информации» является необходимой основой для изучения дисциплины «Информационные системы».

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих **компетенций**:

- Способен проектировать и реализовывать программу основного и среднего общего образования в предметной области Информатика (ПК-2).

В результате изучения дисциплины студент должен

знать:

- ПК 2.1 - знание основы методики преподавания, основные принципы деятельностного подхода, виды и приемы современных педагогических технологий в области информатики (З.1);

- ПК 2.2 - знание рабочей программы и методики обучения по информатике (З.2);

уметь:

- ПК 2.3 - умение планировать и проводить учебные занятия по информатике (У.1);

- ПК 2.4 - умение использовать методы и средства педагогического мониторинга, позволяющие оценить степень сформированности у детей качеств, необходимых для дальнейшего обучения и развития по информатике (У.2);

владеть:

ПК 2.5 - владение формами и методами обучения, в том числе выходящими за рамки учебных занятий: проектная

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 3 зачетных единицы.

Вид учебной работы	5 семестр
Аудиторные занятия (всего)	40
В том числе:	
Лекции (Л)	14
Лабораторные работы (ЛР)(практическая подготовка)	26
Практические занятия (ПЗ)	
Самостоятельная работа (всего)	68
В том числе:	
Контрольная работа	10
Тестирование	10
Реферат	21
Подготовка к зачету с оценкой	27
Вид промежуточной аттестации:	Зачет с оценкой
Общая трудоемкость часы	108
зачетные единицы	3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Содержание разделов дисциплины

№ п/п	Наименование раздела (модуля) дисциплины	Содержание
1.	Основные понятия информационной безопасности	Основные понятия. Служебная тайна, коммерческая тайна, персональные данные. Утечки информации. Несанкционированный доступ к информации. Эффективность защиты информации. Шифрование информации. Хеширование информации. Политика безопасности. Угрозы информационной безопасности. Уязвимость информации. Умышленные и случайные угрозы информационной безопасности. Возможные каналы утечки информации. Основные методы и средства защиты информации.

2	Инженерно-технические и программно-аппаратные методы и средства обеспечения информационной безопасности	Основные и вспомогательные аппаратные средства защиты информации. Основные и вспомогательные программные средства защиты информации. Преимущества и недостатки программных средств защиты информации. Требования к системам защиты информации. Основные требования к комплексной системе защиты информации. Основные категории требований к защищённости компьютерных систем: политика, подотчетность, гарантии. «Оранжевая книга» как стандарт безопасности. Защищенность информации в руководящих документах России.
3	Методы и средства защиты информации от несанкционированного доступа в компьютерные системы	Основные и вспомогательные способы несанкционированного доступа к информации в компьютерные системы. Системы разграничения доступа (СРД) субъектов к объектам. Основные направления защиты средств вычислительной техники. Основные функции СРД. Идентификация и аутентификация субъектов как основное средство СРД. Авторизация и шифрование информации. Протоколы идентификации пользователя. Учетная запись в регистрационной базе данных. Аутентификация пользователей в компьютерных системах. Три группы способов аутентификации пользователей. Аутентификация пользователей с использованием паролей и модели рукопожатия. Требования к паролю учетной записи. Правила использования паролей. Одноразовые пароли. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью. Процедура настройки на характеристики регистрируемого пользователя. Процедура аутентификации в двух вариантах. Аутентификация пользователей при удалённом доступе. Протокол аутентификации Kerberos на серверах.
4.	Защита информации от несанкционированного доступа в операционных системах.	Пароли в BIOS Setup – достоинства и недостатки. Дискреционное управление доступом. Мандатное управление доступом. Системы безопасности защищенных версий операционной системы Windows. Привилегии для групп и отдельных пользователей. Учетные записи «администратор» и «гость». Аудит событий безопасности в защищенных операционных системах Windows. События регистрируемые в типовом журнале аудита. Системные события, как правило, регистрируемые в журнале аудита. Защита информации в операционной системе Linux. Алгоритм хеширования.
5	Криптографические методы информационной безопасности	Симметричные и асимметричные криптосистемы. Принцип построения асимметричных криптосистем. Использование симметричных и асимметричных криптосистем. Применение электронной цифровой подписи. Защита документов MS Office от несанкционированного доступа.

6	Защита систем от компьютерных вирусов	Классификация вирусов. Возможности загрузочных и файловых вирусов. Особенности макровирусов. Методы обнаружения и удаления, их достоинства и недостатки. Приёмы используемые в закладках для усложнения обнаружения их присутствия в компьютерных системах. Некопируемая метка, как метод защиты инсталляционных дисков. Настройка устанавливаемого программного обеспечения на характеристики компьютера. Антивирусные пакеты, их возможности и недостатки.
---	---------------------------------------	--

Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Лабор. зан.	СРС	В т.ч. использов. интеракт. форм (ч.)	Всего
1	Основные понятия информационной безопасности	2		10	Интерактивное лекционное занятие с демонстрацией фрагментов учебных фильмов (2ч)	12
2	Инженерно-технические и программно-аппаратные методы и средства обеспечения информационной безопасности	2		10		12
	Методы и средства защиты информации от несанкционированного доступа в компьютерные системы	4	6	10	Использование ЭОР (4ч)	20
4	Защита информации от несанкционированного доступа в операционных системах.	2	6	10	Использование ЭОР (2ч)	18
5	Криптографические методы информационной безопасности	2	6	10	Использование ЭОР (2ч)	18

6	Защита систем от компьютерных вирусов	2	8	18	Использование ЭОР (2ч)	28
	Итого	14	26	68		108
	Интерактивные часы				12	

6.ЛАБОРАТОРНЫЙ ПРАКТИКУМ

№ п/п	раздел дисциплины	Наименование лабораторных работ	Всего
1	Несанкционированный доступ	Методы и средства защиты информации от несанкционированного доступа в компьютерные системы	6
2	Защита систем от компьютерных вирусов	Изучение механизмов защиты ПК от вирусов и вредоносных программ	6
3.	Криптографические методы информационной безопасности	Кодирование информации	6
4.	Защита систем от компьютерных вирусов	Шифрование информации	8

7. ПРИМЕРНАЯ ТЕМАТИКА РЕФЕРАТОВ

1. Защита информации в Windows XP,7,8.
2. Назначение и возможности базовой системы ввода/вывода.
3. Классификация и назначение вредоносных программ.
4. Назначение и возможности работы в безопасном режиме.
5. Прямое редактирование CMOS памяти.
6. Алгоритм работы и возможности антивируса Касперского.
7. Алгоритм работы и возможности антивируса Данилова.
8. Алгоритм работы и возможности антивируса NOD32.
9. Алгоритм работы и возможности антивируса Panda.
10. Алгоритм работы и возможности антивируса Avira.
11. Возможности и работа в защищенном режиме Windows XP,7,8.
12. Возможности защиты объектов в MS Office.
13. Алгоритм работы и возможности Reg Cleaner.
14. Защита информации в Linux.
15. Администрирование в Windows XP,7,8.
16. Защита информации в Unix.
17. Алгоритм работы и возможности MacAfee.

18. Сравнительный анализ антивирусных пакетов.
19. Возможности брандмауэра.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А. В. Артемов. — Электрон. текстовые данные. — Орел : Межрегиональная Академия безопасности и выживания (МАБИБ), 2014. — 256 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/33430.html>
2. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] / А. Е. Фаронов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 154 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52160.html>

Дополнительная литература

3. Клейменов С.А. Информационная безопасность и защита информации: Учебное пособие/ С.А.Клейменов, В.П.Мельников, А.М.Петраков: - М.: Academia, 2008 г.-336 с.
4. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. Учебное пособие. – М.: ACADEMIA, 2006 г. – 254с.
5. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. Учебное пособие. – М.: ACADEMIA, 2006 г. – 255с.
6. Шмаков Н.В. Организация программного обеспечения: Учебное пособие.- Бийск: НИЦ БПГУ, 2006 г.-100с.
7. Столингс В. Операционные системы: Внутреннее устройство и принципы проектирования. 4-е изд.- М.: Вильямс, 2002 г.-848с.
8. Гульев И.А. Компьютерные вирусы. Взгляд изнутри. М.: ДМК, 1999 г.- 303с.

в) программное обеспечение

1. Работа на компьютере проводится с использованием лицензионных версий операционной системы Microsoft Windows XP Prof.
2. Для работы в библиотеке используется общеузовское лицензионное программное обеспечение «Ирбис-64», в составе которого входят АРМ «Каталогизатор», АРМ «Читатель», АРМ «Администратор», АРМ «Комплектатор», Web-Ирбис (CZ39.50)
3. Лицензионная программа АУП (Шахты) – комплекс «Электронные ведомости»

г) базы данных, информационно-справочные и поисковые системы

1. Российское образование [Электронный ресурс] : федеральный портал – режим доступа: <http://www.edu.ru>
2. Российский общеобразовательный портал [Электронный ресурс] – режим доступа: <http://www.school.edu.ru>
3. Единое окно доступа к образовательным ресурсам [Электронный ресурс] – режим доступа: <http://www.window.edu.ru>
4. Единая коллекция цифровых образовательных ресурсов [Электронный ресурс] – режим доступа: <http://www.school-collection.edu.ru>
5. Федеральный центр информационно-образовательных ресурсов (ФЦИОР) [Электронный ресурс] – режим доступа: <http://www.fcior.edu.ru>
6. Электронно-библиотечная система IPRbooks [Электронный ресурс] – режим доступа: <http://www.iprbookshop.ru>

д) перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Организация самостоятельной работы студентов в учреждении высшего образования [Текст]: методические рекомендации / Сост. Е.Б. Манузина, Е.Э. Норина; Алтайская гос. Академия обр-я им. В.М. Шукшина. – Бийск: ФГБОУ ВПО «АГАО», 2014. – 84 с.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные аудитории для проведения занятий лекционного типа:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player), мультимедиа проектор, экран для представления учебной информации большой аудитории обучающихся.

Учебные аудитории для проведения практических занятий:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player), мультимедиа проектор, экран для представления учебной информации большой аудитории обучающихся.

Учебные аудитории для проведения групповых и индивидуальных консультаций:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player), мультимедиа проектор, экран для представления учебной информации большой аудитории обучающихся.

Учебные аудитории для проведения текущего контроля и промежуточной аттестации:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Помещения для самостоятельной работы:

Аудитория, укомплектованная специализированной мебелью, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (лицензионное программное обеспечение: Windows XP, Office2003, Ирбис; Свободно распространяемое программное обеспечение: 7Zip, Adobe Flash Player, Google Chrome, VLC media Player) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Читальный зал, оснащенный автоматизированными и обычными рабочими местами, с компьютерами, оснащенными комплектом лицензированного программного обеспечения (Лицензионное программное обеспечение: Windows

XP, Office2003, Kaspersky. Свободно распространяемое программное обеспечение: Google Chrome, 7Zip), копировальной машиной, принтерами, сканерами, с наличием автоматизированных рабочих мест для пользователей с проблемами зрения: специальное программное обеспечение, тифлофлешплееры, электронная лупа, читающая машина. Для обучающихся инвалидов и лиц с ОВЗ специализированные сервисы и информационные ресурсы при помощи программно-аппаратных комплексов:

- тифло-флеш-плееров Victor Reader Stream с удобной системой навигации;
- АРМ с проводными гарнитурами Jabra UC VOICE 550 Duo и Windows-приложением для преобразования речи в текст VOCO. Professional .;
- электронного видео-увеличителя Ruby.;
- сканирующего и читающего устройства Eye-Pal Vision;
- специализированного программного обеспечения Easy Converter для создания цифровых говорящих книг в формате DAIZY.

Помещение для хранения и профилактического обслуживания учебного оборудования:

Аудитория, укомплектованная специализированной мебелью: шкаф для хранения учебных наглядных пособий, обеспечивающих тематические иллюстрации; стол, стул, компьютер, принтер, учебно-методические пособия.

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Методические рекомендации по организации изучения дисциплины для преподавателей

Дисциплина разработана таким образом, чтобы у студентов сформировалось цельное представление о структуре информационной безопасности, функциональном назначении и возможностях её компонентов.

При разработке курса основное внимание уделялось методологическому подходу к пониманию основ использования различных компонентов информационной безопасности.

Необходимо четко соблюдать дифференцированный подход при преподавании этой дисциплины, так как уровень подготовки и интеллектуальный уровень студентов сильно разнятся.

Для успешного усвоения курса большое внимание необходимо уделить систематической работе студентов, для этого необходим постоянный контроль выполнения, как лабораторных работ, так и опросы по теоретическому материалу.

Проверяя лабораторные работы и рефераты, преподаватель должен не просто оценить – поставить оценку – констатируя результат, а наводящими вопросами должен подтолкнуть студента либо к решению задачи выбранным методом, либо другим методом. Любая проверка, контроль должны быть не констатацией полученного рейтинга, но и посылком к улучшению результата.

Рекомендуется соблюдать предложенную последовательность тем при преподавании дисциплины, хотя при другом временном распределении лабораторных часов, возможна небольшая корректировка последовательности тем.

Дисциплина включает лекции, практические занятия и самостоятельную работу бакалавров по освоению дисциплины. В ходе лекций раскрываются базовые положения данной дисциплины. Важной частью освоения данной дисциплины является самостоятельная работа студентов с первоисточниками (поиск необходимой информации, разработка докладов, презентаций). Результаты этой

работы студенты могут использовать как на лекциях, так и на практических (семинарских) занятиях, носящих интерактивный характер, а также в ответах на итоговом зачете. Практическим заданием, которое студенты выполняют на протяжении всего изучения данной дисциплины, являются подготовка к презентации доклада по заранее выбранной теме. Все эти материалы являются обязательными составляющими для получения допуска к экзамену.

Методические рекомендации по организации изучения дисциплины для студентов

Рекомендации к составлению доклада. Назначение доклада заключается в кратком изложении основного содержания и передаче новой проблемной информации, взятой и скомпонованной из первоисточников. В докладе нет той обстоятельности изложения, которая характерна, например, для научной статьи. В нем нет развернутых доказательств, рассуждений, сравнений, сопоставлений и обсуждений результатов, оценок, так как это – действенное средство убеждения читателя, а назначение реферата передать что-то, а не убеждать в чем-то.

Реферат отличается и от аннотации, которая отвечает на вопрос, *о чем говорится в первичном документе (статье, книге)*, и дает общее представление о нем, его сжатую характеристику обычно в виде перечня основных проблем. Реферат дает ответ на вопрос, *что нового, существенного содержится в первичном документе*, и передает основное содержание документа, новую проблемную информацию, содержащуюся в нем.

Доклад не предназначен для замены первоисточника. Он только помогает читателю отобрать критериальную информацию и дает основные сведения о содержании первичных документов.

Объем доклада определяется важностью темы, целью, но не должен выходить из временных рамок от 15 до 30 минут.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

1. Назначение фонда оценочных средств. Фонд оценочных средств разработан для проведения промежуточной аттестации обучающихся по дисциплине «Методы и средства защиты информации» (Б1.В.02) и входит в состав основной образовательной программы 44.03.05 Педагогическое образование (с двумя профилями подготовки), реализуемой при подготовке обучающихся в федеральном государственном бюджетном образовательном учреждении высшего образования «Алтайский государственный гуманитарно-педагогический университет имени В.М. Шукшина».

2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

- Способен проектировать и реализовывать программу основного и среднего общего образования в предметной области Информатика (ПК-2).

В результате изучения дисциплины обучающийся должен:

знать:

ПК-2.1 Знать основы методики преподавания, основные принципы деятельностного подхода, виды и приемы современных педагогических технологий в области информатики

ПК-2.2 Знать рабочую программа и методику обучения по информатике

уметь:

ПК-2.3 Уметь планировать и проводить учебные занятия по информатике

ПК-2.4 Уметь использовать методы и средства педагогического мониторинга, позволяющие оценить степень сформированности у детей качеств, необходимых для дальнейшего обучения и развития по информатике

владеть:

ПК-2.5 Владеть формами и методами обучения, в том числе выходящими за рамки учебных занятий: проектная деятельность, лабораторные эксперименты, практические занятия и т.п.

Доклад оценивается по 100-балльной шкале.

Уровни	Показатели
Пороговый 60-74%	В докладе излагается информация по выбранной теме, но источников мало и среди них есть устаревшие данные. Студент отвечает на вопросы с трудом и не на все.
Базовый 75-86%	В докладе излагается информация по выбранной теме на базе современных источников. Студент уверенно отвечает на вопросы, а на некоторые потом делает дополнительное сообщение
Повышенный 87-100%	В докладе соблюдаются четкое построение от постановки задачи до выводов. Используются современные источники. Студент владеет навыками интерпретации информации из источников.

Вопросы к зачету

1. Классификация объектов защиты информации.
2. Характеристика информации как объекта права собственности.
3. Характеристика информации как коммерческой тайны.
4. Классификация угроз безопасности в ЭВМ.
5. Обзор современных методов защиты информации в ЭВМ.
6. Ограничение доступа как метод защиты информации в ЭВМ.
7. Контроль доступа к аппаратуре как метод защиты информации в ЭВМ.
8. Разграничение и контроль доступа к информации как метод защиты информации в ЭВМ.
9. Идентификация и установление подлинности личности.
10. Идентификация и установление подлинности технических средств.
11. Идентификация и установление подлинности документов.
12. Идентификация и установление подлинности информации.
13. Методы шифрования информации в ЭВМ.
14. Шифрование информации с открытым ключом.
15. Методы обнаружения вирусов.
16. Удаление вирусов из компьютера.

17. Восстановление системы поврежденной вирусами ОС.
18. Краткая характеристика антивирусного пакета Doctor Web.
19. Краткая характеристика антивирусного пакета Касперского.
20. Краткая характеристика антивирусного пакета Panda.
21. Краткая характеристика антивирусного пакета Avira.
22. Краткая характеристика антивирусного пакета Nod32.
23. Краткая характеристика антивирусного пакета Aidstest.
24. Организационные мероприятия по защите информации.
25. Законодательные меры по защите информации.

Пример контрольной работы

Заполните таблицу ниже, указав разновидности конкретного вида вирусов, механизмы порчи информации и средства борьбы с ними

№	Название группы вирусов	Разновидности	Механизм порчи информации	Рекомендуемые средства защиты
1	Черви			
2	Трояны			

Фрагмент тестового задания

1. Защита информации от утечки это деятельность по предотвращению:
 - a. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
 - b. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
 - c. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
 - d. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;**
 - e. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
2. Защита информации это:
 - a. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
 - b. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
 - c. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
 - d. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

е. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

3. Естественные угрозы безопасности информации вызваны:
- а. деятельностью человека;
 - б. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 - с. ***воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;***
 - д. корыстными устремлениями злоумышленников;
 - е. ошибками при действиях персонала.
4. Искусственные угрозы безопасности информации вызваны:
- а. деятельностью человека;***
 - б. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
 - с. воздействиями объективных физических процессов или стихийных природных явлений, независимых от человека;
 - д. корыстными устремлениями злоумышленников;
 - е. ошибками при действиях персонала.
5. К посторонним лицам нарушителям информационной безопасности относятся:
- а. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
 - б. персонал, обслуживающий технические средства;
 - с. технический персонал, обслуживающий здание;
 - д. пользователи;
 - е. сотрудники службы безопасности.
 - ф. представители конкурирующих организаций.***
 - г. лица, нарушившие пропускной режим;

Методические материалы, определяющие процедуры оценивания (зачет, зачет с оценкой)

Цель процедуры:

Целью промежуточной аттестации по дисциплине (модулю) является оценка уровня усвоения обучающимися знаний, приобретения умений, навыков и сформированности компетенций в результате изучения учебной дисциплины (части дисциплины – для многосеместровых дисциплин).

Субъекты, на которых направлена процедура:

Процедура оценивания должна охватывать всех без исключения обучающихся, осваивающих дисциплину (модуль). В случае, если обучающийся не проходил процедуру без уважительных причин, то он считается имеющим академическую задолженность.

Период проведения процедуры:

Процедура оценивания проводится по окончании изучения дисциплины (модуля).

Требования к помещениям и материально-техническим средствам для проведения процедуры:

Требования к аудитории для проведения процедуры и необходимости применения специализированных материально-технических средств определяются преподавателем.

Требования к кадровому обеспечению проведения процедуры:

Процедуру проводит преподаватель, ведущий дисциплину (модуль), как правило, проводящий занятия лекционного типа.

Требования к банку оценочных средств:

До начала проведения процедуры преподавателем подготавливается необходимый банк оценочных материалов для оценки знаний, умений, навыков. Банк оценочных материалов может включать вопросы открытого и закрытого типа, перечень тем, выносимых на опрос, типовые задания. Из банка оценочных материалов формируются печатные бланки индивидуальных заданий. Количество вопросов, их вид (открытые или закрытые) в бланке индивидуального задания определяется преподавателем самостоятельно.

Описание проведения процедуры:

Каждому обучающемуся, принимающему участие в процедуре преподавателем выдается вопрос. После получения вопроса и подготовки ответов обучающийся должен в меру имеющихся знаний, умений, навыков, сформированности компетенции дать развернутые ответы на поставленные в задании открытые вопросы и ответить на вопросы закрытого типа в установленное преподавателем время. Продолжительность проведения процедуры определяется преподавателем самостоятельно, исходя из сложности индивидуальных заданий, количества вопросов, объема оцениваемого учебного материала, общей трудоемкости изучаемой дисциплины (модуля) и других факторов.

Результаты процедуры:

Результаты проведения процедуры в обязательном порядке проставляются преподавателем в зачетные книжки обучающихся и электронные ведомости, и представляются в деканат факультета, за которым закреплена образовательная программа.

По результатам проведения процедуры оценивания преподавателем делается вывод о результатах промежуточной аттестации по дисциплине.

По результатам проведения процедуры оценивания обучающиеся, показавшие неудовлетворительные результаты считаются имеющими академическую задолженность, которую обязаны ликвидировать в соответствии с составляемым индивидуальным графиком. В случае, если обучающийся своевременно не ликвидировал имеющуюся академическую задолженность он подлежит отчислению из вуза, как не справившийся с образовательной программой.