МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный педагогический университет»
(ФГБОУ ВО «АлтГПУ»)

УТВЕРЖДАЮ
проректор по образовательной и
международной деятельности

_____С.П. Волохов

ПРЕДМЕТНО- МЕТОДИЧЕСКИЙ МОДУЛЬ ПО ПРОФИЛЮ "ИНФОРМАТИКА"

Информационная безопасность и защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	**Теоретических основ информатики**
Учебный план	zМиИ44.03.05_2022.plx 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Квалификация	**бакалавр**
Форма обучения	**заочная**
Общая трудоемкость	**2 ЗЕТ**

Часов по учебному плану	72	Виды контроля на курсах:
в том числе:		зачеты 5
аудиторные занятия	10	
самостоятельная работа	56	
часов на контроль	4	

Программу составил(и):
старший преподаватель, Москаленко Елена Валерьевна _____

Рабочая программа дисциплины
Информационная безопасность и защита информации

разработана на основании ФГОС ВО - бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (приказ Минобрнауки России от 22.02.2018 г. № 125)

составлена на основании учебного плана 44.03.05 Педагогическое образование (с двумя профилями подготовки) (Уровень: бакалавриат; квалификация: бакалавр), утвержденного Учёным советом ФГБОУ ВО «АлтГПУ» от 25.04.2022, протокол № 9.

Рабочая программа одобрена на заседании кафедры
Теоретических основ информатики

Протокол № 7 от 21.02.2022 20:00:00 г.
Срок действия программы: 2022-2027 уч.г.
Зав. кафедрой Тумбаева Наталья Викторовна

Распределение часов дисциплины по курсам

Курс	**5**		Итого	
Вид занятий	УП	РП		
Лекции	4	4	4	4
Практические	6	6	6	6
Контроль самостоятельной работы	2	2	2	2
Итого ауд.	10	10	10	10
Контактная работа	12	12	12	12
Сам. работа	56	56	56	56
Часы на контроль	4		4	
Итого	72	68	72	68

1.1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1.1	формирование у студентов знаний и умений, которые образуют теоретический и практический фундамент в области теоретических основ информационной безопасности, навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах образовательных учреждений.

1.2. ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.2.1	- знаний о современных тенденциях угроз информационной безопасности, о норма- тивных правовых документах по защите информации, а так же о современных методах и средствах обеспечения информационной безопасности в экономических информационных системах;
1.2.2	- умений выявлять угрозы информационной безопасности, использовать норматив- ные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности;
1.2.3	- навыков владения приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения информационной безопасности в информационных системах.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	К.М.08
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Веб-технологии
2.1.2	Технологии цифрового образования
2.1.3	Теоретические основы информатики
2.1.4	Программное обеспечение
2.1.5	Иностранный язык
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Подготовка к сдаче и сдача государственного экзамена
2.2.3	Учебная практика: практика по получению профессиональных знаний и умений в области математики
2.2.4	Производственная практика: педагогическая практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-1.1: Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета).
ПК-1.2: Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	Общие приемы и правила поиска нормативно- правовых документов в области обеспечения информационной безопасности
3.2	**Уметь:**
3.2.1	использовать нормативные правовые документы, международные и отечественные стандарты в сфере информационной безопасности
3.3	**Владеть:**
3.3.1	Навыками поиска нормативно-правовых документов, стандартами в области информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1.				
1.1	Сущность и понятия информационной безопасности /Лек/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

1.2	Законодательный уровень информационной безопасности /Лек/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Угрозы информационной безопасности /Лек/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.4	Каналы утечки и несанкционированного доступа к конфиденциальной информации /Лек/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.5	Системы защиты информации. Кадровое и ресурсное обеспечение защиты информации /Ср/	5	6	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.6	Инженерно- техническая защита информации /Ср/	5	10	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.7	Настройка параметров безопасности операционной системы Windows /Пр/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.8	Локальная политика безопасности в операционной системе Windows /Пр/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.9	Нормативно-правовой уровень защиты информации /Пр/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.10	Установка и настройка средств защиты информации	5	8	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.11	Шифр Цезаря. Шифрование файлов с помощью программы TrueCrypt /Пр/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.12	Организация защиты документов средствами пакета Microsoft Office	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.13	Электронная подпись /Пр/	5	1	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.14	Настройка параметров безопасности Интернет браузеров /Ср/	5	2	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.15	Средства защиты компьютера от вирусов /Ср/	5	8	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.16	Рекомендации по использованию различных программ в ОУ /Ср/	5	4	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.17	Меры по созданию безопасной информационной системы в образовательном учреждении /Ср/	5	8	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.18	Средства защиты информации /Ср/	5	10	ПК-1.1 ПК-1.2	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Перечень индикаторов достижения компетенций, форм контроля и оценочных средств

ИПК - 2.1. Владеет содержанием предметных областей в соответствии с образовательными программами
Знать: содержание, сущность, закономерности, принципы и особенности изучаемых явлений и процессов, базовые теории в предметных областях.

Уметь: использовать базовые предметные научно-теоретические подходы к сущности, закономерностям, принципам и особенностям изучаемых явлений и процессов.
Владеть: навыками использования базовых предметных научно-теоретических подходов к сущности, закономерностям, принципам и особенностям изучаемых явлений и процессов для решения профессиональных задач.
ИПК - 2.2. Анализирует базовые научно-теоретические подходы к сущности, закономерностям, принципам и особенностям изучаемых явлений и процессов в предметных областях

5.2. Технологическая карта достижения индикаторов

ИПК - 2.1.			
ИПК - 2.2.	Лекционные занятия	Вопросы для самоконтроля	15
ИПК - 2.1.			
ИПК - 2.2.	Лабораторные занятия	Лабораторные работы	45
ИПК - 2.1.			
ИПК - 2.2. Контрольный срез	Тестовые задания Вопросы к коллоквиуму Доклады		20
ИПК - 2.1.			
ИПК - 2.2. Зачет	Вопросы для итогового контроля		20
Всего	100		

5.3. Формы контроля и оценочные средства

Задания для практической работы (полные тексты заданий находятся на кафедре)

1. Настройка параметров безопасности операционной системы Windows 7.

Задание: Ознакомьтесь с основными настройками параметров безопасности операцион- ной системы Windows 7 и выполните работу, сопровождая каждый этап скриншотами. Содержание отчета

1. Титульный лист.
2. Скриншоты работы каждой изученной команды.
3. Комментарии к каждому скриншоту.

2. Локальная политика безопасности в ОС Windows 7

Задание: изучить редактор «Локальная политика безопасности». Осуществить редакти- рование локальной политики. Осуществить редактирование политики блокировки учет- ной записи.

Содержание отчета

1. Титульный лист.
2. Скриншоты работы каждой изученной команды.
3. Комментарии к каждому скриншоту.
4. Ответы на вопросы.

Контрольные вопросы:

1. Каким образом можно открыть оснастку «Локальная политика безопасности»?
2. В каком узле политики можно установить требования к длине, сложности пароля?
3. Какие параметры могут быть установлены для политики блокировки учетных запи- сей?
4. Какие политики можно настраивать в разделе «Политика аудита»?
5. В каком узле можно определить какие пользователи могут управлять аудитом и жур- налом безопасности?

3. Нормативно-правовой уровень защиты информации. Проанализировать содержание нор- мативно-правовых актов согласно своему варианту. К отчету приложить титульный лист, название анализируемого акта, указать дату последней поправки, дату принятия акта, отве- ты на вопросы (при ответе на вопрос необходимо указать ссылку на конкретный пункт ак- та).

4. Построение частной модели угроз.

Задание: Построить частную модель угроз согласно своему варианту. Содержание отчета

1. Титульный лист.
2. Описать структуру организации, с указанием отделов и их функциями, приложить схему структуры организации.
3. Проанализировать и описать угрозы для организации.
4. Построить частную модель угроз, используя таблицу 1. (Для указания рекомендаций по противодействию угроз, используйте в качестве основы прикрепленный документ «Модель_угроз_ИСПДн_3_УЗ»)
5. Сделать выводы (указать актуальные угрозы). Варианты:

1. Образовательная организация
2. Отделение банка
3. Ресторан
4. Жилищно-коммунальное хозяйство
5. Медицинская организация
6. Гостиница
7. Туристическая фирма
8. Коллекторская организация
9. Отдел сотовой связи
10. Строительная компания

5. Шифр Цезаря
Самым древним и самым простым из известных подстановочных шифров является шифр, использовавшийся Юлием Цезарем. В шифре цезаря каждая буква алфавита заменяется
буквой, которая находится на три позиции дальше в этом же алфавите.
Задание: Имеется шифрованный текст, полученный с помощью шифра Цезаря. Величина используемого при этом сдвига неизвестна. Расшифруйте сообщение. (Необходимо соста- вить программу на языке программирования и отчет)

6. Шифрование файлов с помощью программы TrueCrypt. Содержание отчета
1. Титульный лист.
2. Скриншоты работы каждой изученной команды.
3. Комментарии к каждому скриншоту.
4. Ответы на вопросы.
Контрольные вопросы
1. Какие алгоритмы шифрования входят в комплект TrueCrypt?
2. Каковы основные достоинства и недостатки рассмотренного программного продукта?
3. Область применения программы.

7. Организация защиты документов средствами пакета Microsoft Office 2010. Осуществить защиту документа и его отдельных элементов в приложениях Word и Excel.

8. Электронная подпись. Установить Установка СКЗИ КриптоПРО CSP. Сгенерировать ЭЦП на тестовом портале УЦ КриптоПРО. Подпись документов с помощью КриптоПро Office Signature. Подписание документов MSOffice. Подпись документов с помощью КриптоПро PDF. Подпись документов с помощью КриптоАРМ.
Содержание отчета
1. Титульный лист.
2. Скриншоты выполнения работы (порядок установки программ прикреплять не нужно. Необходимо только указать, что была установлена необходимая программа).
3. Ответы на вопросы.
Контрольные вопросы:
1. Что представляет собой электронная цифровая подпись?
2. Для каких целей используется сертификат открытого ключа?
3. В чем заключается отличие «открытого» ключа от «закрытого»?
4. Как происходит формирование ключей?
5. Как происходит генерация ключей и получение сертификата?

2.2. Тестовые задания (полный перечень вопросов находится на кафедре)
Установите соответствие: МАТ
. # Вопрос Ответ
1. Стационарные информационные ресурсы формируются и используются в специализированных информационных организациях с помощью их информационных систем и сетей
2. Передвижные информационные ресурсы формируются государственными и частными информационными организациями как специальные информационные продукты
3. формируются отдельными физическими лицами посредством Интернет
Установите соответствие между следующими понятиями и их определениями: МАТ
. # Вопрос Ответ
1. Угроза намерение нанести объекту существенный ущерб
2. Опасность состояние окружающей среды или объекта, в котором существует возможность причинить объекту существенный ущерб или вред
3. Безопасность состояние объекта, в котором ему не может быть нанесено существенного ущерба или вреда
4. фактор или совокупность факторов, создающих безопасность объекту
Установите соответствия между типами реагирования на несанкционированные действия и их характеристиками:
МАТ
. # Вопрос Ответ
1. пассивные СЗИ не предусматриваются ни сигнализация о несанкционированных действиях, ни воз- действие системы защиты на нарушителя
2. полуактивные СЗИ предусматривается сигнализация о не- санкционированных действиях, но не предусматривается воздействие системы на нарушителя
3. активные СЗИ предусматриваются как сигнализация о несанкционированных действиях, так и воздействие системы на нарушителя.
4. не предусматриваются сигнализация о несанкционированных действиях, предусматривается воздействие системы на нарушителя
Последовательность функций защиты информации: МАТ
. # Вопрос Ответ
1 предупреждение проявления угроз
2 обнаружение проявившихся угроз и предупреждение их воздействия на информацию
3 обнаружение воздействия угроз на защищаемую информацию и локализация этого воздействия

4 ликвидация последствий воздействия угроз
Установите соответствие между классификацией информации и ее видами: МАТ
. # Вопрос Ответ
1. По способу доступа: государственная, коммерческая тайна,персональные данные,
2. По способу организации ресурсов: документ, массив, фонд, архив, банки данных
3. По форме собственности: общероссийское национальное достояние, государственная, федеральная, частная собственность
4. По виду информации: правовая, научно-техническая, политическая, финансово-экономическая, статистическая, персональная
5. По видам носителя: на бумаге, в виде изображения, на машиночитаемом носителе, в электронном виде
6. ручная, механическая, автоматизированная
Установите соответствие между терминами и их определениями: МАТ
. # Вопрос Ответ
1. Правовая защита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту ин- формации на правовой основе
2. Организационная защита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям
3. Инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности.
4. - это комплекс мероприятий, направленных на обеспечение информационной безопасности
Установите соответствие: МАТ
. # Вопрос Ответ
5. - это защита коммерческой, организационной или иной используемой в экономической деятельности информации
Установите соответствие между терминами и их определениями: МАТ
. # Вопрос Ответ
1. идентификация процедура распознавания субъекта по его идентификатору
2. аутентификация процедура проверки подлинности субъекта с данными идентификатора
3. авторизация процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации
4. процедура регистрации субъекта в системе
Установите соответствие между видом шифрования и его характеристикой МАТ
. # Вопрос Ответ
1. симметричное отправитель и получатель информации используют один и тот же ключ
2. асимметричное отправитель и получатель информации используют различные ключи
3. отправитель и получатель информации используют различные ключи, но они могут быть получены один из другого
4. отправитель и получатель информации используют один и тот же ключ, который является открытым
Установите соответствие между терминами и их определениями: МАТ
. # Вопрос Ответ
1.Целостность это гарантия сохранности данными правильных значений, которая обеспечивается запретом неавторизованным пользователям каким-либо образом изменять, модифицировать, разрушать или создавать данные
2. Доступность это гарантия того, что авторизованные пользователи всегда получат доступ к данным
3. Конфиденциальность это гарантия того, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен; та- кие пользователи называются легальными, или авторизованными
Установите соответствие: МАТ
. # Вопрос Ответ
4. состояние объекта, когда ему путем воз- действия на его информационную сферу не может быть нанесен существенный ущерб или вред
Установите соответствие между терминами и их определениями МАТ
. # Вопрос Ответ
1. государственная тайна защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно- розыскной деятельности, распространение которых может нанести ущерб без- опасности РФ
2. коммерческая тайна режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать не- оправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
3. это охраняемые законом конфиденциальные сведения о деятельности государственных органов, доступ к которым ограничен федеральным законом или в силу служебной необходимости, а также ставшие известными в государственных органах
Установите соответствие между уровнем опасности угроз и их характеристиками МАТ
. # Вопрос Ответ
1. низкая опасность если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных
2. средняя опасность если реализация угрозы может привести к негативным последствиям для субъектов

персональных данных
3. высокая опасность если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных
Условно жизненный цикл любого компьютерного вируса можно разделить на пять стадий: MAT
. # Вопрос Ответ
1. 1 проникновение на чужой компьютер
2. 2 активация
3. 3 поиск объектов для заражения
4. 4 подготовка копий
5. 5 внедрение копий

Защищаемые государством сведения, создаваемые в условиях секретности в соответствии с законодательством РФ, называются MC
Ответы Отзыв Оценка
A. Государственной тайной 100
B. Коммерческой тайной 0
C. Научно-юридической информацией 0
К традиционным формам информационных ресурсов, которые классифицируются по способу организации хранения и использования, относятся: MA
Ответы Отзыв Оценка
A. интернет 0
B. банк данных 0
C. фонд документов 33.3
D. массив документов 33.3
E. архив 33.3
Перечислите основные свойства информации: MA
Ответы Отзыв Оценка
A. достоверность 33.3
B. субъективность 0
C. массовость 0
D. понятность 33.3
E. доступность 33.3
Информационные ресурсы по виду информации: MA
Ответы Отзыв Оценка
A. правовая информация 33.3
B. политическая информация 33.3
C. кадастры (земельный, градостроительный, имущественный, лесной, другие) 33.3
D. В канале связи 0
E. открытая информация (без ограничения) 0
Информационные ресурсы по виду носителя: MA
Ответы Отзыв Оценка

Установите соответствие: MAT
. # Вопрос Ответ
A. в виде изображения на экране ЭВМ 33.3
B. в памяти ЭВМ 33.3
C. на бумаге 33.3
D. информация ограниченного доступа 0
E. архив 0
Обеспечение информационной безопасности осуществляется по следующим основным направлениям: MA
Ответы Отзыв Оценка
A. правовая защита 33.3
B. организационная защита 33.3
C. инженерная и программно- техническая защита 33.3
D. государственная защита 0
E. защита интеллектуальной собственности 0
Свойство информации, которое является достаточным для понимания и принятия решений MC
Ответы Отзыв Оценка
A. полнота 100
B. своевременность 0
C. понятность 0
D. доступность 0
Свойство информации, которое отражает истинное положение дел. MC
Ответы Отзыв Оценка
A. достоверность 100

B. полнота 0
C. ценность 0
D. понятность 0
По форме представления информацию можно условно разделить на следующие виды: МС
Ответы Отзыв Оценка

Установите соответствие: МАТ
. # Вопрос Ответ
A. текстовую, числовую, графическую, звуковую и пр. 100
B. математическую, биологическую, медицинскую, психологическую и пр.
0
C. обыденную, производственную, техническую, управленческую 0
D. зрительную, слуховую, тактильную, обонятельную, вкусовую 0
E. научную, социальную, политическую, экономическую, религиозную и пр
0
По способу восприятия информации человеком различают следующие виды информации: МС
Ответы Отзыв Оценка
A. зрительную, слуховую, тактильную, обонятельную, вкусовую 100
B. математическую, биологическую, медицинскую, психологическую и пр.
0
C. обыденную, производственную, техническую, управленческую 0
D. научную, социальную, политическую, экономическую, религиозную и пр.
0
E. текстовую, числовую, графическую, звуковую и пр. 0
Технические каналы утечки информации подразделяются на: МА
Ответы Отзыв Оценка
A. Оптические 25
B. Радиочастотные 25
C. Электрические 25
D. Акустические 25
E. Семантические 0
F. Материально-вещественные 0
Несанкционированный доступ к данным (НСД) может быть: МС
Ответы Отзыв Оценка

Установите соответствие: МАТ
. # Вопрос Ответ
A. пассивным и индуктивным 0
B. изменяющимся и постоянным 0
C. пассивным и активным 100
Радиомикрофоны бывают двух типов: МС
Ответы Отзыв Оценка
A. Акустическими. Вибрационными 100
B. Акустическими. Оптико- электронные 0
C. Акустическими. Радиочастотные 0
К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений ТСПИ: МА
Ответы Отзыв Оценка
A. Излучений элементов ТСПИ 33.3
B. Излучений на частотах работы высокочастотных (ВЧ) генераторов ТСПИ 33.3
C. Излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ТСПИ
33.3
D. Сбоев цепи электропитания и заземления ТСПИ 0
E. Сбоев цепи электропитания ТСПИ 0
Ответы Отзыв Оценка
A. наводки электромагнитных излучений ТСПИ на соединительные линии ВТСС и посторонние про- водники, выходящие за пределы контролируемой зоны
33.3
B. просачивание информационных сигналов в цепи электропитания ТСПИ
33.3
C. просачивание информационных сигналов в цепи заземления ТСПИ 33.3
D. просачивание информационных сигналов через диелектрические материалы в ТСПИ
0
E. наводки создаваемые в информационном канале обработке информации
0
К первому классу относятся каналы от источника информации при НСД к нему: МА

#	Ответы	Отзыв	Оценка

Установите соответствие: МАТ

.	#	Вопрос	Ответ
A.		хищение носителей информации	33.3
B.		подслушивание разговоров	33.3
C.		фотографирование или видеосъемка носителей информации внутри помещения	33.3
D.		снятие информации с устройств электронной памяти	0
E.		подключения к линиям связи	0
F.		изучение выходящей за пределы объекта открытой информации	0

Источниками угроз являются:

Выберите один или несколько ответов: МА

#	Ответы	Отзыв	Оценка
A.	противники		0
B.	документы		0
C.	коррупционеры		33.3
D.	преступники		33.3
E.	конкуренты		33.3
F.	средства массовой информации		0

2.3. Вопросы к зачету

1. Теория защиты информации. Основные направления.
2. Обеспечение информационной безопасности и направления защиты.
3. Комплексность (целевая, инструментальная, структурная, функциональная, временная).
4. Требования к системе защиты информации.
5. Угрозы информации.
6. Виды угроз. Основные нарушения.
7. Характер происхождения угроз.
8. Источники угроз. Предпосылки появления угроз.
9. Система защиты информации.
10. Классы каналов несанкционированного получения информации.
11. Причины нарушения целостности информации:.
12. Методы и модели оценки уязвимости информации.
13. Общая модель воздействия на информацию.
14. Общая модель процесса нарушения физической целостности информации.
15. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
16. Методологические подходы к оценке уязвимости информации.
17. Модель защиты системы с полным перекрытием.
18. Рекомендации по использованию моделей оценки уязвимости информации.
19. Допущения в моделях оценки уязвимости информации.
20. Методы определения требований к защите информации.
21. Факторы, обуславливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
22. Классификация требований к средствам защиты информации.
23. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
24. Требования к защите, обуславливаемые видом защищаемой информации.
25. Требования, обуславливаемые, взаимодействием пользователя с комплексом средств автоматизации.
26. Анализ существующих методик определения требований к защите информации.
27. Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения.
28. Руководящем документе Гостехкомиссии России "Классификация автоматизированных систем и требований по защите информации", выпущенном в 1992 году. Часть 1.
29. Классы защищенности средств вычислительной техники от несанкционированного доступа.
30. Факторы, влияющие на требуемый уровень защиты информации.
31. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты.
32. Методы формирования функций защиты.
33. События, возникающие при формировании функций защиты.
34. Классы задач функций защиты.
35. Класс задач функций защиты 1 — уменьшение степени распознавания объектов
36. Класс задач функций защиты 2 — защита содержания обрабатываемой, хранимой и передаваемой информации.
37. Класс задач функций защиты 3 — защита информации от информационного воздействия.
38. Функции защиты информации.
39. Стратегии защиты информации.

40. Способы и средства защиты информации.
41. Способы "абсолютной системы защиты".
42. Архитектура систем защиты информации. Требования.
43. Общеметодологических принципов архитектуры системы защиты информации.
44. Построение средств защиты информации.
45. Ядро системы защиты.
46. Семирубежная модель защиты.

2.4. Вопросы для самоконтроля:
1. Основные понятия и определения информационной безопасности. Угрозы безопасности информационных систем.
2. Политика информационной безопасности. Отечественные и международные правовые и нормативные акты в области обеспечения информационной безопасности.
3. Основы криптографической защиты информации. Понятие криптосистемы. Понятие шифра, алгоритма и ключа шифрования.
4. Основы криптографической защиты информации. Понятие и примеры симметричных и асимметричных криптографических систем.
5. Шифрование данных методом шифрующих таблиц (одиночная перестановка, одиночная перестановка по ключу).
6. Шифрование данных методом шифрующих таблиц (двойная перестановка).
7. Шифрование и дешифрование данных методом магического квадрата.
8. Шифрование данных с использованием системы Цезаря с ключевым словом.
9. Шифрование данных с использование аффинной системы подстановок Цезаря.
10. Шифрование данных с использованием системы Трисемуса.
11. Шифрование данных на основе алгоритма Плейфера.
12. Шифрование данных с использованием системы Вижинера.
13. Шифрование данных с использованием «двойного квадрата» Уитстона.
14. Шифрование данных на основе алгоритма DES.
15. Шифрование данных на основе алгоритма RSA.
16. Шифрование данных с использованием схемы Эль-Гамаля.
17. Понятие идентификации и аутентификации пользователей. Аутентификация с использованием биометрических данных.
18. Понятие идентификации и аутентификации пользователей. Аутентификация с использованием физического объекта.
19. Понятие идентификации и аутентификации пользователей. Аутентификация пользователей с использованием пароля.
20. Протокол идентификации с нулевой передачей данных.
21. Параллельная схема протокола идентификации с нулевой передачей данных.
22. Понятие электронной цифровой подписи. Однонаправленные хэш-функции.
23. Понятие электронной цифровой подписи. Алгоритмы ЭЦП. Реализация ЭЦП на основе алгоритма RSA.
24. Стеганографические методы защиты информации.
25. Защита информации в компьютерных системах. Задачи по обеспечению безопасности компьютерных систем.
26. Основные угрозы и направления обеспечения безопасности компьютерных систем.
27. Концепция адаптивного управления безопасностью. Технология анализа защищенности.
28. Концепция адаптивного управления безопасностью. Технология обнаружения атак.
29. Жизненный цикл программного обеспечения и безопасность: технологическая и эксплуатационная безопасность программных средств.
30. Защита программ и данных. Парольная защита. Скрытие данных на носителях информации. 31. Безопасность операционной системы: архитектура подсистемы защиты операционной системы.
32. Понятие вредоносного программного обеспечения. Компьютерные вирусы и черви.
33. Понятие вредоносного программного обеспечения. Троянские программы.
34. Понятие вредоносного программного обеспечения. Подозрительные упаковщики. Вредоносные утилиты.
35. Антивирусные средства защиты информации.
36. Протоколы передачи данных HTTP/HTTPS.
37. Понятие межсетевого экрана. Фильтрация на сетевом, сеансом и прикладном уровне.
38. Основы безопасного поведения в сети Интернет.
39. Понятие спама, способы распространения спама. Понятие фишинга. Рекомендации по защите от спама и фишинга.

5.4. Оценка результатов обучения в соответствии с индикаторами достижения компетенций

Неудовл.: не достигнут
Удовл. Пороговый уровень: частично сформированы знания, умения и навыки в области основ проектирования локальных вычислительных сетей, в области сетевых стандартов представления информации и протоколов передачи данных; на базовом уровне сформированы знания и практические навыки, позволяющие проектировать локальные компьютерные сети; обучающийся обладает знаниями только основного материала, но не усвоил его деталей, допускает неточности, демонстрирует недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
Хорошо. Базовый уровень: в достаточном объёме сформированы знания, умения и навыки в области основ

проектирования и создания локальных вычислительных сетей, в области сетевых стандартов представления информации и протоколов передачи данных и принципов их использования для объединения в единое целое разнородных информационных ресурсов; частично сформированы знания и практические навыки, позволяющие проектировать локальные компьютерные сети; обучающийся в достаточной степени знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос или выполнении заданий, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Отлично. Высокий уровень: сформированы в полной мере знания, умения и навыки в области основ проектирования и создания локальных вычислительных сетей, в области сетевых стандартов представления информации и протоколов передачи данных и принципов их использования для объединения в единое целое разнородных информационных ресурсов, а также техническими и программными средствами, обеспечивающими их работу; в полном объёме сформированы знания и практические навыки, позволяющие проектировать локальные компьютерные сети; обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал научной литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Издание	Экз.
Л1.1	В. А. Галатенко	Основы информационной безопасности: учебное пособие — Москва : ИНТУИТ : Ай Пи Ар Медиа, 2020 — URL: http://www.iprbookshop.ru/97562.html	9999
Л1.2	Д. А. Скрипник	Общие вопросы технической защиты информации: учебное пособие — Москва ; Саратов : ИНТУИТ : Ай Пи Ар Медиа, 2020 — URL: http://www.iprbookshop.ru/89451.html	9999
Л1.3	Ю. А. Брюхомицкий	Безопасность информационных технологий: в 2 частях. Часть 1: учебное пособие — Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020 — URL: http://www.iprbookshop.ru/107943.html	9999

6.1.2. Дополнительная литература

	Авторы, составители	Издание	Экз.
Л2.1	А. В. Ревнивых	Информационная безопасность в организациях: учебное пособие — Москва : Ай Пи Ар Медиа, 2021 — URL: https://www.iprbookshop.ru/108227.html	9999
Л2.2	Г. М. Суворова	Информационная безопасность: учебное пособие — Саратов : Вузовское образование, 2019 — URL: https://www.iprbookshop.ru/86938.html	9999
Л2.3	О. И. Солонская	Средства защиты информации: учебное пособие — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021 — URL: https://www.iprbookshop.ru/117115.html	9999

6.3.1 Перечень программного обеспечения

6.3.1.1	Пакет Microsoft Office
6.3.1.2	Операционная система семейства Windows
6.3.1.3	Операционная система семества Linux
6.3.1.4	Интернет браузер
6.3.1.5	Пакет Kaspersky Endpoint Security 10 for Windows

6.3.2 Перечень информационных справочных систем

6.3.2.1	Электронная библиотека НПБ / Алтайский государственный педагогический университет, Научно-педагогическая библиотека
6.3.2.2	eLIBRARY.RU : научная электронная библиотека

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	1. Оборудованные учебные аудитории, в том числе с использованием видеопроектора и подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.
7.2	2. Аудитории для самостоятельной работы с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.
7.3	3. Компьютерный класс с подключением к сети «Интернет» и доступом в электронную информационно-образовательную среду Университета.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

техническими средствами и получить достаточные практические навыки в работе с программными средствами, используемыми при выполнении лабораторных работ по курсу. Особое внимание должно быть уделено изучению типовых задач работы с информацией в компьютерных сетях.
Лабораторные работы выполняются студентов в составе 1 человека по каждому индивидуальному проектному заданию.
Подготовка к следующей лабораторной работе должна производиться в урочное время с использованием электронного учебника.
В течении времени, отведенного по расписанию, студенты получают от преподавателя индивидуальное задание, изучают теоретическую часть, соответствующую выполняемой работе, знакомятся с образцовой задачей и на ее основе выполняют индивидуальное задание по принципу подобия и по «нарастанию» нового материла.
По итогам лабораторных работ готовится отчет.

Методические рекомендации обучающимся с ограниченными возможностями здоровья (ОВЗ)
Специальные условия обучения в АлтГПУ определены «Положением об инклюзивном образовании» (утверждено приказом ректора от 25.12.2015 г. № 312/1п). Данным «Положением» предусмотрено заполнение студентом при зачислении в университет анкеты «Определение потребностей обучающихся в создании специальных условий обучения», в которой указываются потребности лица в организации доступной социально-образовательной среды и помощи в освоении образовательной программы.
Под специальными условиями для получения образования обучающимися с ограниченными возможностями здоровья понимаются условия обучения, воспитания и развития, включающие в себя использование специальных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования.
Построение образовательного процесса ориентировано на учет индивидуальных возрастных, психофизических особенностей обучающихся, в частности предполагается возможность разработки индивидуальных учебных планов.
Реализация индивидуальных учебных планов сопровождается поддержкой тьютора (родителя, взявшего на себя тьюторские функции в процессе обучения, волонтера).
Обучающиеся с ОВЗ, как и все остальные студенты, могут обучаться по индивидуальному учебному плану в установленные сроки с учетом индивидуальных особенностей и специальных образовательных потребностей конкретного обучающегося. Срок получения высшего образования при обучении по индивидуальному учебному плану для лиц с ограниченными возможностями здоровья может быть при необходимости увеличен, но не более чем на год.
При составлении индивидуального графика обучения для лиц с ОВЗ возможны различные варианты проведения занятий:
- проведение индивидуальных или групповых занятий с целью устранения сложностей в усвоении лекционного материала, подготовке к семинарским занятиям, выполнению заданий по самостоятельной работе. Для лиц с ОВЗ, по их просьбе, могут быть адаптированы как сами задания, так и формы их выполнения.
- выполнение под руководством преподавателя индивидуального проектного задания, позволяющего сочетать теоретические знания и практические навыки;
- применение мультимедийных технологий в процессе ознакомительных лекций и семинарских занятий, что позволяет экономить время, затрачиваемое на изложение необходимого материала и увеличить его объем;
- дистанционную форму индивидуальных консультаций, выполнения заданий на базе платформы «Moodle».
Основным достоинством дистанционного обучения для лиц с ОВЗ является то, что оно позволяет полностью индивидуализировать содержание, методы, формы и темпы учебной деятельности инвалида, следить за каждым его действием и операцией при решении конкретных задач; вносить вовремя необходимые коррекции как в деятельность студента-инвалида, так и в деятельность преподавателя. Дистанционное обучение также позволяет обеспечивать возможности коммуникаций не только с преподавателем, но и с другими обучаемыми, сотрудничество в процессе познавательной деятельности (форум, вебинар, skype-консультирование). Эффективной формой проведения онлайн-занятий являются вебинары, которые могут быть использованы для проведения виртуальных лекций с возможностью сетевого взаимодействия всех участников дистанционного обучения.
Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации преподаватели, в соответствии с потребностями студента, отмеченными в анкете, и рекомендациями специалистов дефектологического профиля, разрабатывает фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.
Форма проведения текущей аттестации для студентов с ОВЗ устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости лицам с ОВЗ может быть предоставлено дополнительное время для подготовки к ответу на зачете или экзамене, выполнения задания по самостоятельной работе.
Студент с ограниченными возможностями здоровья обязан:
- выполнять требования образовательных программ, предъявляемые к степени овладения соответствующими знаниями;
- самостоятельно сообщить в соответствующее подразделение по работе со студентами с ОВЗ о наличии у него подтвержденной в установленном порядке ограниченных возможностей здоровья, жизнедеятельности и трудоспособности (инвалидности) необходимости создания для него специальных условий.