Министерство просвещения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ульяновский государственный педагогический университет
имени И.Н. Ульянова»
(ФГБОУ ВО «УлГПУ им. И.Н. Ульянова»)

Факультет физико-математического и технологического образования
Кафедра информатики

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ С.Н. Титов
25 июня 2021 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИКЕ

Программа учебной дисциплины Предметно-методического модуля

основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки),

направленность (профиль) образовательной программы
Математика. Экономика

(очная форма обучения)

Составитель: Шубович В.Г., к.п.н., профессор кафедры информатики

Рассмотрено и одобрено на заседании ученого совета факультета физико-математического и технологического образования, протокол от 21.06.2021 №7

Ульяновск, 2021

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D77C644FC1E54000000006381D0002
Владелец: Титов Сергей Николаевич
Действителен: с 19.07.2021 до 19.07.2022

Место дисциплины в структуре образовательной программы

Дисциплина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОНОМИКЕ» включена в обязательную часть Блока 1 Дисциплины (модули) основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), направленность (профиль) образовательной программы «Математика. Экономика», очной формы обучения.

Дисциплина опирается на результаты обучения, сформированные в рамках школьного курса «Информатика и ИКТ» или соответствующих дисциплин среднего профессионального образования, а также ряда дисциплин учебного плана: Педагогика, Психология, Информационно-коммуникационные технологии и медиаинформационная грамотность.

Результаты изучения дисциплины являются теоретической и методологической основой для изучения дисциплины: Производственная (научно-исследовательская работа) Преддипломная практика.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Целью освоения дисциплины является:

содействие становлению будущего педагога путем формирования целостного представления об информационной безопасности для использования в решении педагогических задач.

В результате освоения дисциплины обучающийся должен овладеть следующими результатами обучения по дисциплине:

Компетенция и индикаторы ее достижения в дисциплине	Образовательные результаты дисциплины (этапы формирования дисциплины)		
	знает	умеет	владеет
Способен организовывать совместную и индивидуальную учебную и воспитательную деятельность обучающихся, в том числе с особыми образовательными потребностями, в соответствии с требованиями федеральных государственных образовательных стандартов (ОПК-3)	ОР-1 теоретические информационной безопасности;	ОР-2 использовать элементы информационной безопасности для обеспечения устойчивого функционирования информационных систем и сетей;	ОР-3 навыками применения информационной безопасности для эффективного ориентирования в современном информационном пространстве;

2. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся*:*

Номер семестра	Учебные занятия						Форма промежуточной аттестации
	Всего		Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	
	Трудоемк.						
	Зач. ед.	Часы					
10	2	72	12	-	20	40	зачет
Итого:	2	72	12	-	20	40	зачет

3. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

3.1. Указание тем (разделов) и отведенного на них количества академических часов и видов учебных занятий:

Наименование раздела и тем	Количество часов по формам организации обучения			
	Лекц. занятия	Лаб. занятия	Практ. занятия	Самост. работа
10 семестр				
Тема 1.Основные понятия и анализ угроз информационной безопасности.	2			4
Тема 2. Криптографическая защита информации.	2	4		6
Тема 3. Идентификация, аутентификация и управление доступом.	2	4		5
Тема 4. Обеспечение безопасности операционных систем.	2	4		5
Тема 5. Обеспечение безопасности инфокоммуникационных сетей.	2	4		10
Тема 6. Управление информационной безопасностью.	2	4		10
ИТОГО 10 семестр:	12	20		40
Всего:	12	20		40

3.2. Краткое описание содержания тем (разделов) дисциплины

Тема 1. Основные понятия и анализ угроз информационной безопасности.

Основные понятия информационной безопасности и защиты информации. Анализ угроз информационной безопасности. Анализ угроз корпоративных сетей. Атаки на сети. Обеспечение информационной безопасности компьютерных сетей.

Тема 2. Криптографическая защита информации.

Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Электронная

цифровая подпись. Инфраструктура управления открытыми ключами PKI.

Тема 3. Идентификация, аутентификация и управление доступом.

Аутентификация, авторизация и администрирование действий пользователей. Биометрическая аутентификация пользователя. Управление идентификацией и доступом.

Тема 4. Обеспечение безопасности операционных систем.

Обеспечение безопасности ОС семейства Windows. Обеспечение безопасности ОС семейства Linux.

Тема 5. Обеспечение безопасности инфокоммуникационных сетей.

Протоколы защищенных каналов. Технологии межсетевого экранирования. Технологии виртуальных защищенных сетей VPN. Защита удаленного доступа.

Тема 6. Управление информационной безопасностью.

Задачи управления информационной безопасностью. Функционирование системы управления информационной безопасностью информационной системы образовательного учреждения. Аудит и мониторинг безопасности информационной системы.

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов является особой формой организации учебного процесса, представляющая собой планируемую, познавательно, организационно и методически направляемую деятельность студентов, ориентированную на достижение конкретного результата, осуществляемую без прямой помощи преподавателя. Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, а также выполнение учебных заданий, подготовку к предстоящим занятиям и экзамену. Она предусматривает, как правило, разработку рефератов, написание докладов, выполнение творческих, индивидуальных заданий в соответствии с учебной программой (тематическим планом изучения дисциплины). Тема для такого выступления может быть предложена преподавателем или избрана самим студентом, но материал выступления не должен дублировать лекционный материал. Реферативный материал служит дополнительной информацией для работы на практических занятиях. Основная цель данного вида работы состоит в обучении студентов методам самостоятельной работы с учебным материалом. Для полноты усвоения тем, вынесенных в практические занятия, требуется работа с первоисточниками. Курс предусматривает самостоятельную работу студентов со специальной литературой. Следует отметить, что самостоятельная работа студентов результативна лишь тогда, когда она выполняется систематически, планомерно и целенаправленно.

Задания для самостоятельной работы предусматривают использование необходимых терминов и понятий по проблематике курса. Они нацеливают на практическую работу по применению изучаемого материала, поиск библиографического материала и электронных источников информации, иллюстративных материалов. Задания по самостоятельной работе даются по темам, которые требуют дополнительной проработки.

Общий объем самостоятельной работы студентов по дисциплине включает аудиторную и внеаудиторную самостоятельную работу студентов в течение семестра.

Аудиторная самостоятельная работа осуществляется в форме выполнения тестовых заданий, кейс-задач, письменных проверочных работ по дисциплине. Аудиторная самостоятельная работа обеспечена базой тестовых материалов, кейс-задач по разделам дисциплины.

Внеаудиторная самостоятельная работа осуществляется в формах:

- подготовки к устным докладам (мини-выступлениям);
- подготовка к защите реферата;
- подготовки к защите индивидуальных лабораторных работ.

Темы рефератов

1. Вредоносные программы.

2. Удаленные сетевые атаки.
3. Технологии межсетевых экранов.
4. Системы обнаружения атак и вторжений.
5. Виртуальные частные сети.
6. Средства перехвата аудиоинформации.
7. Технические каналы утечки информации.
8. Технические средства защиты информации.

Криптографические методы и средства защиты.

Для самостоятельной подготовки к занятиям по дисциплине рекомендуется использовать учебно-методические материалы:

1. Неижмак В.В. Компьютерные технологии в науке, образовании и культуре: методические рекомендации – Ульяновск: ФГБОУ ВО «УлГПУ им. И. Н. Ульянова», 2016. – 28 с.
2. Неижмак В.В. Информационные технологии в современной науке и образовании: методические рекомендации по предмету «Информационные технологии в современной науке и образовании» – Ульяновск: ФГБОУ ВО «УлГПУ им. И. Н. Ульянова», 2016. – 16 с.

5. Примерные оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Организация и проведение аттестации студента

ФГОС ВО в соответствии с принципами Болонского процесса ориентированы преимущественно не на сообщение обучающемуся комплекса теоретических знаний, но на выработку у бакалавра компетенций – динамического набора знаний, умений, навыков и личностных качеств, которые позволят выпускнику стать конкурентоспособным на рынке труда и успешно профессионально реализовываться.

В процессе оценки бакалавров необходимо используются как традиционные, так и инновационные типы, виды и формы контроля. При этом постепенно традиционные средства совершенствуются в русле компетентностного подхода, а инновационные средства адаптированы для повсеместного применения в российской вузовской практике.

Цель проведения аттестации – проверка освоения образовательной программы дисциплины-практикума через сформированность образовательных результатов.

Промежуточная аттестация осуществляется в конце семестра и завершает изучение дисциплины; помогает оценить крупные совокупности знаний и умений, формирование определенных компетенций.

Оценочными средствами текущего оценивания являются: доклад, тесты по теоретическим вопросам дисциплины, защита практических работ и т.п. Контроль усвоения материала ведется регулярно в течение всего семестра на практических (семинарских, лабораторных) занятиях.

№ п/п	**СРЕДСТВА ОЦЕНИВАНИЯ,** используемые для текущего оценивания показателя формирования компетенции	Образовательные результаты дисциплины
	Оценочные средства для текущей аттестации	ОР-1 теоретические информационной безопасности;

	ОС-1 Контрольная работа ОС-2 Обсуждение мини-выступлений. ОС-3 Контрольное мероприятие - защита рефератов. ОС-4 Защита лабораторной работы.	ОР-2 использовать элементы информационной безопасности для обеспечения устойчивого функционирования информационных систем и сетей; ОР-3 навыками применения информационной безопасности для эффективного ориентирования в современном информационном пространстве;
	Оценочные средства для промежуточной аттестации зачет (экзамен) ОС-5 Устное собеседование по теоретическим и практико-ориентированным вопросам (в форме зачета / экзамена)	

Описание оценочных средств и необходимого оборудования (демонстрационного материала), а так же процедуры и критерии оценивания индикаторов достижения компетенций на различных этапах их формирования в процессе освоения образовательной программы представлены в Фонде оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине

ОС-1 Контрольная работа.

Пример контрольной работы (тест из 16 вопросов).
Критерии оценивания: за каждый правильный ответ – 2 балла.

1. Непосредственное использование материалов для обеспечения некоторой механической функции; при этом все основано на взаимном сцеплении и сопротивлении тел. Выберете соответствующий данному определению термин:

a. Механизм
b. Машина
c. Робот

2. Кто является основным ответственным за определение уровня классификации информации?

a. Руководитель среднего звена
b. Высшее руководство
c. Владелец
d. Пользователь

3. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

a. Сотрудники
b. Хакеры
c. Атакующие
d. Контрагенты

4. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует

предпринять руководству?Способен организовывать совместную и индивидуальную учебную и воспитательную деятельность обучающихся, в том числе с особыми образовательными потребностями, в соответствии с требованиями федеральных государственных образовательных стандартов

1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3. Улучшить контроль за безопасностью этой информации
4. Снизить уровень классификации этой информации

5. Что самое главное должно продумать руководство при классификации данных?

a. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
b. Необходимый уровень доступности, целостности и конфиденциальности
c. Оценить уровень риска и отменить контрмеры
d. Управление доступом, которое должно защищать данные

6. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

a. Владельцы данных
b. Пользователи
c. Администраторы
d. Руководство

7. Что такое процедура?

a. Правила использования программного и аппаратного обеспечения в компании
b. Пошаговая инструкция по выполнению задачи
c. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
d. Обязательные действия

8. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

a. Поддержка высшего руководства
b. Эффективные защитные меры и методы их внедрения
c. Актуальные и адекватные политики и процедуры безопасности
d. Проведение тренингов по безопасности для всех сотрудников

9. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

a. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
b. Когда риски не могут быть приняты во внимание по политическим соображениям
c. Когда необходимые защитные меры слишком сложны
d. Когда стоимость контрмер превышает ценность актива и потенциальные потери

10. Что такое политики безопасности?

a. Пошаговые инструкции по выполнению задач безопасности
b. Общие руководящие требования по достижению определенного уровня безопасности
c. Широкие, высокоуровневые заявления руководства
d. Детализированные документы по обработке инцидентов безопасности

11. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

a. Анализ рисковСпособен организовывать совместную и индивидуальную учебную и воспитательную деятельность обучающихся, в том числе с особыми образовательными потребностями, в соответствии с требованиями федеральных государственных образовательных стандартов
b. Анализ затрат / выгоды
c. Выявление уязвимостей и угроз, являющихся причиной риска

12. Что лучше всего описывает цель расчета ALE?

a. Количественно оценить уровень безопасности среды
b. Оценить возможные потери для каждой контрмеры
c. Количественно оценить затраты / выгоды
d. Оценить потенциальные потери от угрозы в год

13. Тактическое планирование – это:

a. Среднесрочное планирование
b. Долгосрочное планирование
c. Ежедневное планирование
d. Планирование на 6 месяцев

14. Что является определением воздействия (exposure) на безопасность?

a. Нечто, приводящее к ущербу от угрозы
b. Любая потенциальная опасность для информации или систем
c. Любой недостаток или отсутствие информационной безопасности
d. Потенциальные потери от угрозы

15. Эффективная программа безопасности требует сбалансированного применения:

1. Технических и нетехнических методов
2. Контрмер и защитных механизмов
3. Физической безопасности и технических средств защиты
4. Процедур безопасности и шифрования

16. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

1. Внедрение управления механизмами безопасности
2. Классификацию данных после внедрения механизмов безопасности
3. Уровень доверия, обеспечиваемый механизмом безопасности
4. Соотношение затрат / выгод

17. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

1. Только военные имеют настоящую безопасность
2. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
3. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
4. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

18. Как рассчитать остаточный риск?

1. Угрозы x Риски x Ценность актива
2. (Угрозы x Ценность актива x Уязвимости) x Риски
3. SLE x Частоту = ALE
4. (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

19. Что из перечисленного не является целью проведения анализа рисков?

1. Делегирование полномочий
2. Количественная оценка воздействия потенциальных угроз
3. Выявление рисков
4. Определение баланса между воздействием риска и стоимостью необходимых контрмер

20 . Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

1. Поддержка
2. Выполнение анализа рисков
3. Определение цели и границ
4. Делегирование поСпособен организовывать совместную и индивидуальную учебную и воспитательную деятельность обучающихся, в том числе с особыми образовательными потребностями, в соответствии с требованиями федеральных государственных образовательных стандартовлномочий

21. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

9. Чтобы убедиться, что проводится справедливая оценка
10. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
11. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
12. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

22. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

a. гаммирования;
b. подстановки;
c. кодирования;
d. перестановки;
e. аналитических преобразований.

23. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

a. гаммирования;
b. подстановки;
c. кодирования;
d. перестановки;
e. аналитических преобразований.

24. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

a. гаммирования;
b. подстановки;
c. кодирования;
d. перестановки;
e. аналитических преобразований.

25. 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.

26. 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;
e. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

27. Естественные угрозы безопасности информации вызваны:

a. деятельностью человека;
b. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
c. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
d. корыстными устремлениями злоумышленников;
e. ошибками при действиях персонала.

28. Искусственные угрозы безопасности информации вызваны:

a. деятельностью человека;
b. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
c. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
d. корыстными устремлениями злоумышленников;
e. ошибками при действиях персонала.

29. К основным непреднамеренным искусственным угрозам АСОИ относится:

a. физическое разрушение системы путем взрыва, поджога и т.п.;
b. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
c. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
d. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
e. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

30. К посторонним лицам нарушителям информационной безопасности относится:

a. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
b. персонал, обслуживающий технические средства;
c. технический персонал, обслуживающий здание;
d. пользователи;
e. сотрудники службы безопасности.
f. представители конкурирующих организаций.
g. лица, нарушившие пропускной режим;

31. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

a. черный пиар;
b. фишинг;
c. нигерийские письма;
d. источник слухов;
e. пустые письма.

ОС-2 Обсуждение мини-выступлений.

Вопросы для самостоятельного изучения обучающимися (темы мини-выступлений)

1. Исторический обзор подходов к обеспечению информационой безопасности.
2. Свободное и проприетарное ПО для защиты информации.

3. Особенности использования программных продуктов для защиты информации в условиях импортозамещения.

ОС-3 Контрольное мероприятие - защита рефератов.

ОС-4 Защита лабораторной работы.

Содержание и защита лабораторной работы

Каждый студент после выполнения и защиты текущих лабораторных работ готовит отчет.

а) структура отчета:

- титульный лист;
- содержание работы

Студент должен продемонстрировать умения и навыки работы с программным обеспечением общего и специального назначения

Перечень тем индивидуальных практических работ:

№ п.п.	№ темы дисциплины	Наименование лабораторной работы
1	2	Применение методов физической защиты устройств хранения данных Криптографическая защита информации. (4 ч.).
2	3	Применение технологии виртуальных машин для проверки используемого ПО и имитации сетевых соединений (4 ч.).
3	4	Использование антивирусного ПО для защиты компьютера. Защита компьютерной сети с использованием межсетевых экранов (4 ч.).
4	5	Использование набора средств PKI. Организация виртуальных частных сетей (4 ч.).
5	6	Устранение результатов воздействия вирусов на компьютеры (4 ч.).

Материалы, используемые для текущего контроля успеваемости обучающихся по дисциплине

Материалы для организации текущей аттестации представлены в п.5 программы.

Материалы, используемые для промежуточного контроля успеваемости обучающихся по дисциплине

ОС-5 Устное собеседование по теоретическим и практико-ориентированным вопросам (в форме зачета / экзамена)

ПРИМЕРНЫЕ ВОПРОСЫ ДЛЯ ЗАЧЕТА

1. Основные понятия информационной безопасности и защиты информации.
2. Анализ угроз информационной безопасности.
3. Анализ угроз корпоративных сетей.
4. Атаки на сети.
5. Обеспечение информационной безопасности компьютерных сетей.
6. Основные понятия криптографической защиты информации.

7. Симметричные криптосистемы шифрования.
8. Асимметричные криптосистемы шифрования.
9. Электронная цифровая подпись.
10. Инфраструктура управления открытыми ключами PKI.
11. Аутентификация, авторизация и администрирование действий пользователей.
12. Биометрическая аутентификация пользователя.
13. Управление идентификацией и доступом.
14. Обеспечение безопасности ОС семейства Windows.
15. Обеспечение безопасности ОС семейства Linux.
16. Протоколы защищенных каналов.
17. Технологии межсетевого экранирования.
18. Технологии виртуальных защищенных сетей VPN.
19. Защита удаленного доступа.
20. Задачи управления информационной безопасностью.
21. Функционирование системы управления информационной безопасностью информационной системы образовательного учреждения.
22. Аудит и мониторинг безопасности информационной системы.

В конце изучения дисциплины подводятся итоги работы студентов на лекционных и лабораторных занятиях путем суммирования заработанных баллов в течение семестра.

Критерии оценивания знаний обучающихся по дисциплине
Формирование балльно-рейтинговой оценки работы обучающихся

		Посещение лекций	Посещение практических занятий	Работа на практических занятиях	Контроль-ная работа	Зачет
10 семестр	Разбалловка по видам работ	6 x 1=6 баллов	10 x 1=10 баллов	10 x 12=120 баллов	32 балла	32 балла
	Суммарный макс. балл	6 баллов max	16 баллов max	136 баллов max	168 баллов max	200 баллов max

Критерии оценивания работы обучающегося по итогам семестра

По итогам изучения, трудоёмкость которой составляет 2 ЗЕ и изучается в 7 семестре, обучающийся набирает определённое количество баллов, которое соответствует «зачтено» или «не зачтено» согласно следующей таблице:

	Баллы (2 ЗЕ)
«зачтено»	более 60
«не зачтено»	60 и менее

6. Методические указания для обучающихся по освоению дисциплины

Успешное изучение курса требует от обучающихся посещения лекций, активной работы на практических занятиях, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

Запись **лекции** – одна из форм активной самостоятельной работы обучающихся, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. В конце лекции преподаватель оставляет время (5 минут) для того, чтобы обучающиеся имели возможность задать

уточняющие вопросы по изучаемому материалу. Из-за недостаточного количества аудиторных часов некоторые темы не удается осветить в полном объеме, поэтому преподаватель, по своему усмотрению, некоторые вопросы выносит на самостоятельную работу студентов, рекомендуя ту или иную литературу. Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. В случае необходимости обращаться к преподавателю за консультацией.

Подготовка к **лабораторным занятиям**.

При подготовке к лабораторным занятиям студент должен изучить теоретический материал по теме занятия (использовать конспект лекций, изучить основную литературу, ознакомиться с дополнительной литературой, при необходимости дополнить конспект, делая в нем соответствующие записи из литературных источников). В случае затруднений, возникающих при освоении теоретического материала, студенту следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале лабораторного занятия преподаватель знакомит студентов с темой, оглашает план проведения занятия, выдает задание. В течение отведенного времени на выполнение работы студент может обратиться к преподавателю за консультацией или разъяснениями. В конце занятия проводится прием выполненных работ, собеседование со студентом.

Результаты выполнения практических зданий оцениваются в баллах, в соответствии с балльно-рейтинговой системой университета.

Планы лабораторных занятий

Лабораторная работа № 1 Применение методов физической защиты устройств хранения данных. Криптографическая защита информации.

Рекомендации к самостоятельной работе

1. Проработать материал по теме лабораторной работы.
2. Изучить материал из информационно-коммуникационной сети интернет по ключевым словам: Методы физической защиты устройств хранения данных, Криптографическая защита.

Содержание работы:

1. Использование методов физической защиты устройств хранения данных.
2. Использование методов криптографической защиты информации.

Форма представления отчета:

Студент должен представить решение предложенных задач в электронном виде.

Лабораторная работа № 2. Применение технологии виртуальных машин для проверки используемого ПО и имитации сетевых соединений.

Рекомендации к самостоятельной работе

1. Проработать материал по теме лабораторной работы.
2. Изучить материал из информационно-коммуникационной сети интернет по ключевым словам: Программное обеспечение для виртуальных машин.

Содержание работы:

1. Поиск и скачивание ПО для развертывания виртуальных машин.
2. Инсталляция ПО и настройка сетевых соединений.

Форма представления отчета:

Студент должен представить решение предложенных задач в электронном виде.

Лабораторная работа № 3 Использование антивирусного ПО для защиты компьютера. Защита компьютерной сети с использованием межсетевых экранов.

Рекомендации к самостоятельной работе

1. Проработать материал по теме лабораторной работы.

2. Изучить материал из информационно-коммуникационной сети интернет по ключевым словам: Антивирусное ПО.

Содержание работы:

1. Использование антивирусного ПО из комплекта ОС.
2. Использование стороннего антивирусного ПО.
3. Использование межсетевых экранов.

Форма представления отчета:

Студент должен представить решение предложенных задач в электронном виде.

Лабораторная работа № 4. Использование набора средств PKI. Организация виртуальных частных сетей.

Рекомендации к самостоятельной работе

1. Проработать материал по теме лабораторной работы.
2. Изучить материал из информационно-коммуникационной сети интернет по ключевым словам: PKI, VPN.

Содержание работы:

1. Использование набора средств PKI для генерации ключей.
2. Использование набора средств PKI для шифрования документов.
3. Использование набора средств PKI для электронной подписи документов.
4. Использование ПО VPN для обеспечения безопасной удаленной работы.

Форма представления отчета:

Студент должен представить решение предложенных задач в электронном виде.

Лабораторная работа № 5. Устранение результатов воздействия вирусов на компьютеры.

Рекомендации к самостоятельной работе

1. Проработать материал по теме лабораторной работы.
2. Изучить материал из информационно-коммуникационной сети интернет по ключевым словам: Устранение результатов воздействия вирусов на компьютеры.

Содержание работы:

1. Устранение результатов воздействия вирусов на компьютеры.
2. Восстановление работоспособности ОС.
3. Восстановление удаленных файлов.

Форма представления отчета:

Студент должен представить решение предложенных задач в электронном виде.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1013711 (дата обращения: 23.03.2021). – Режим доступа: по подписке.
2. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 (дата обращения: 23.03.2021). – Режим доступа: по подписке.

Дополнительная литература

3. Информационные системы в экономике : учебное пособие / под ред. Д. В. Чистова. — Москва : ИНФРА-М, 2019. — 234 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-003511-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1003296 (дата обращения: 23.03.2021). – Режим доступа: по подписке.

Интернет-ресурсы

- Информатика и информационные технологии. Конспект лекций. http:// www.alleng.ru/d/comp/comp63.htm.
- «Информационные технологии». Ежемесячный теоретический и прикладной научно-технический журнал (с приложением)/ [Электронный ресурс]. Режим доступа: http://novtex.ru/IT/index.htm.