год начала подготовки 2018

АНО ВО «Российский новый университет»

Елецкий филиал Автономной некоммерческой организации высшего образования «Российский новый университет»
(Елецкий филиал АНО ВО «Российский новый университет»)

кафедра прикладной экономики и сферы обслуживания

Рабочая программа учебной дисциплины (модуля)

Системы информационной безопасности
(наименование учебной дисциплины (модуля))

09.03.03 Прикладная информатика
(код и направление подготовки/специальности)

Прикладная информатика в экономике
(код и направление подготовки/специальности, в случаях, если программа разработана для разных направлений подготовки/специальностей)

Рабочая программа учебной дисциплины (модуля) рассмотрена и утверждена на заседании кафедры 12 февраля 2018 г., протокол № 6.

Заведующий кафедрой Прикладной экономики и сферы обслуживания
(название кафедры)
к.п.н., доцент Гнездилова Н.А. _____
(ученая степень, ученое звание, фамилия и инициалы, подпись заведующего кафедрой)

Елец
2018 год

1. НАИМЕНОВАНИЕ И ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Системы информационной безопасности» являются:

Обеспечение профессионального образования, способствующего социальной, академической мобильности, востребованности на рынке труда, успешной карьере, сотрудничеству.

Формирование у обучающихся систематизированных профессионально значимых знаний по вопросам информатики, связанных с информационной безопасностью, и профессиональных умений и навыков, необходимых бакалавру.

Освоение технологий информационной безопасности, в том числе ознакомление с методами управления информационными ресурсами, обеспечивающими защиту информации в современных ЭВМ, комплексах, системах и сетях, а также изучение законодательной базы и стандартов в области информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП БАКАЛАВРИАТА

Учебная дисциплина «Системы информационной безопасности» относится к вариативной части учебного плана (Б1.В.ДВ.08.02).

Содержание учебной дисциплины тесно связано с логикой и содержанием других изучаемых дисциплин. Для успешного усвоения курса «Системы информационной безопасности» студент должен изучить курсы: «Информационные системы и технологии», «Правовые основы прикладной информатики в экономике».

Дисциплина «Системы информационной безопасности» является необходимой базой для последующего освоения дисциплин профессионального цикла основной образовательной программы таких как: «Информационная безопасность», «Предметно-ориентированные экономические и информационные системы», «Системы электронной коммерции». Компетенции, сформированные в результате освоения содержания дисциплины, необходимы для прохождения преддипломной практики.

Дисциплина изучается на заочной форме обучения на 4 курсе.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОП

В результате освоения дисциплины обучающийся должен овладеть следующими компетенциями:

ПК-9. Способность использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий.

Планируемые результаты освоения компетенций

Компетенция	Показатели (планируемые) результаты обучения
ПК-9 Способность использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий.	**Владеть** - инструментальными средствами подготовки проектной документации В1(ПК-9); - методологией работы со стандартами по разработке программной документации В2(ПК-9); - стандартами, руководящими документами и другими нормативными документами, регулирующими процесс разработки технической документации В3(ПК-9);
	Уметь - разрабатывать основную техническую документацию на проектирование и разработку программного обеспечения У1(ПК-9). - вести процесс разработки и согласования проектной документации (технического задания) У3(ПК-9); - составлять техническую документацию проектов автоматизации прикладных процессов У4(ПК-9).
	Знать - состав технической документации, подготавливаемой на всех стадиях

	проектирования информационных систем З1(ПК-9); - основные принципы и методы стандартизации программного обеспечения З3(ПК-9); - техническую документацию проектов информатизации прикладных процессов З4(ПК-9).

4. 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

Дисциплина предполагает изучение 4 тем. Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 часов).

Общий объем учебной дисциплины

№	Форма обучения	Семестр/ сессия, курс	Общая трудоемкость		в том числе контактная работа с преподавателем					СР	Контроль
			в з.е.	в часах	Всего	Л	Сем	КоР	зачет		
1.	Заочная	2 сессия, 4 курс	1	36	4	4				32	
		1 сессия, 5 курс	2	72	10		8	1,7	0,3	58,3	3,7
	Итого		3	108	14	4	8	1,7	0,3	58,3	3,7

Распределение учебного времени по темам и видам учебных занятий
заочная форма

№	Наименование разделов, тем учебных занятий	Всего часов	Контактная работа с преподавателем					Сам.работа	Контроль	Формируемые результаты обучения
			Всего	Лекции	Сем	Кор	Зач			
	Модуль 1. Введение в безопасность информации современного предприятия									
1	Основные принципы построения систем информационной безопасности.	5	1	1	2			4		В3(ПК-9) З1(ПК-9) З3(ПК-9)
2	Общие характеристики защищаемого объекта.	5	1	1	2			4		В3(ПК-9) З1(ПК-9) З3(ПК-9)
3	Планирование защитных мероприятий по видам угроз. Обеспечение информационной безопасности выделенного объекта с учетом особенностей операционной системы.	5	1	1	2			4		В2(ПК-9) В3(ПК-9) У3(ПК-9) У1(ПК-9) З3(ПК-9)

4	Разработка модели системы информационной безопасности на основе матричной модели.	5	1	1	2			4		В1(ПК-9) У3(ПК-9) З1(ПК-9) З3(ПК-9)
5	***Промежуточная аттестация (Зачет)***		2			1,7	0,3	14		
6	**Всего по дисциплине**	**108**	**14**	**4**	**8**	**1,7**	**0,3**	**58,3**	**3,7**	**108**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ СТРУКТУРИРОВАННОЕ ПО ТЕМАМ

№ п/п	Наименование раздела, темы учебной дисциплины	Содержание раздела, темы
1	2	3
1.___	Основные принципы построения систем информационной безопасности.	Комплексный подход и системность при обеспечении информационной безопасности. Сущность задачи управления информационной безопасностью. Документированная информация как объект информационных правоотношений. ***Литература:*** Обязательная: 1-2. Дополнительная: 1-3.
2.___	Общие характеристики защищаемого объекта	Выявление каналов утечки информации. Анализ защищенности выделенного объекта. Разработка модели угроз. Разработка модели нарушителя. ***Литература:*** Обязательная: 1-2. Дополнительная: 1-3.
3.___	Планирование защитных мероприятий по видам угроз. Обеспечение информационной безопасности выделенного объекта с учетом особенностей операционной системы.	Мероприятия по защите информации. Механизмы безопасности ОС Linux и Windows. Основные атаки на ОС Linux и Windows и меры противодействия им. ***Литература:*** Обязательная: 1-2. Дополнительная: 1-3.
4.___	Разработка модели системы информационной безопасности на основе матричной модели	Общее описание матричной модели системы информационной безопасности. Варианты решений для элементов матрицы в соответствии с техническим заданием. ***Литература:*** Обязательная: 1-2. Дополнительная: 1-3.

Планы практических занятий

Тема 1. *Основные принципы построения систем информационной безопасности.*

1. Комплексный подход и системность при обеспечении информационной безопасности.

2. Сущность задачи управления информационной безопасностью.

Тема 2. *Общие характеристики защищаемого объекта.*

1. Выявление каналов утечки информации.

2. Анализ защищенности выделенного объекта.

3. Разработка модели угроз.

4. Разработка модели нарушителя.

Тема 3. *Планирование защитных мероприятий по видам угроз. Обеспечение информационной безопасности выделенного объекта с учетом особенностей операционной системы.*

1. Мероприятия по защите информации.

2. Механизмы безопасности ОС Linux и Windows.

3. Основные атаки на ОС Linux и Windows и меры противодействия им.

Тема 4. *Разработка модели системы информационной безопасности на основе матричной модели.*

1. Общее описание матричной модели системы информационной безопасности.

2. Варианты решений для элементов матрицы в соответствии с техническим заданием.

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Контроль самостоятельной работы студента осуществляется в форме:

изучения:

- первоисточников,
- дат и событий,
- терминологии.

ответов:

- на вопросы для самопроверки,

подготовки:

- сообщений,
- рефератов,
- презентаций.

решений:

- заданий,
- тестов.

6.1. Задания для приобретения, закрепления и углубления знаний.

6.1.1 Основные категории учебной дисциплины для самостоятельного изучения:

Администратор защиты – субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Аутентификация – проверка принадлежности субъекту доступа предъявляемого им идентификатора, подтверждение подлинности.

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Верификация – процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

Дискреционное управление доступом – разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Диспетчер доступа (ядро защиты) – технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

Доступ к информации – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Защита от несанкционированного доступа – предотвращение или существенное затруднение несанкционированного доступа.

Защищенное средство вычислительной техники (защищенная автоматизированная система) – средство вычислительной техники (автоматизированная система), в котором

реализован комплекс средств защиты.

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Класс защищенности средств вычислительной техники, автоматизированной системы – определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

Комплекс средств защиты (КСЗ) – совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Конфиденциальная информация – информация, требующая защиты.

Концепция диспетчера доступа – концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам.

Мандатное управление доступом – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Матрица доступа – таблица, отображающая правила разграничения доступа.

Метка конфиденциальности (метка) – элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

Многоуровневая защита – защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Модель защиты – абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

Модель нарушителя правил разграничения доступа – абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Нарушитель правил разграничения доступа – субъект доступа, осуществляющий несанкционированный доступ к информации.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Пароль – идентификатор субъекта доступа, который является его секретом.

Показатель защищенности средств вычислительной техники – характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Санкционированный доступ к информации – доступ к информации, не нарушающий правила разграничения доступа.

Сертификат защиты (Сертификат) – документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

Сертификация уровня защиты (Сертификация) – процесс установления соответствия

средствами вычислительной техники или автоматизированной системы набору определенных требований по защите.

Система защиты информации от несанкционированного доступа (СЗИ НСД) – комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Система защиты секретной информации (СЗСИ) – комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.

Система разграничения доступа (СРД) – совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Средство защиты от несанкционированного доступа – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Уровень полномочий субъекта доступа – совокупность прав доступа субъекта доступа.

Целостность информации – способность средствами вычислительной техники или автоматизированной системы обеспечить неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

6.2 Задания для повторения и углубления приобретаемых знаний.

Задание 6.2.1. З1(ПК-9) *Основные принципы построения систем информационной безопасности.*

1. Какие принципы создание систем информационной безопасности вам известны?
2. Какие существуют подходы к оценке безопасности информационных систем?
3. Назовите признаки безопасности современных информационных систем.
4. Что такое политика безопасности?
5. В чем сущность программы информационной безопасности?
6. Перечислите цели программы информационной безопасности верхнего уровня.
7. Перечислите цели программы информационной безопасности нижнего уровня.

Задание 6.2.2. З2(ПК-9) *Основные принципы построения систем информационной безопасности.*

1.Назовите модели представления информационной защиты.

2.Перечислите требования к математической модели представления информационной защиты.

3.Перечислите основные этапы построения модели информационной безопасности.

4.Сформулируйте основные требования к системе информационной безопасности.

5.Назовите объективные трудности, с которыми можно столкнуться при моделировании системы информационной защиты.

Задание 6.2.3. З1(ПК-9) *Основные принципы построения систем информационной безопасности.*

1.В чем сущность управления рисками при реализации информационной безопасности.

2.Опишите методы снижения рисков при реализации информационной безопасности.

3.Какие существуют методы оценки экономического эффекта от затрат на информационную безопасность?

4.По каким параметрам можно судить о степени защищенности информационной системы?

Задание 6.2.4 З1(ПК-9) *Общие характеристики защищаемого объекта*.

1. Назовите основные характеристики защищаемого объекта.
2. Что включают в себя физические условия функционирования объекта?
3. Какие рабочие процессы анализируются в целях информационной безопасности?
4. Что входит в правила, регламентирующие работу и процедуры защищаемого объекта?
5. Как учитываются требования государственных органов и руководства к объекту при разработке системы информационной безопасности?

Задание 6.2.5 З2(ПК-9) *Общие характеристики защищаемого объекта*.

1.Охарактеризуйте этапы методики определения угроз.

2.Что включает в себя список элементов информации для целей информационной безопасности?

3.Из каких источников может осуществляться сбор информации об угрозе?

4.Каким образом составляется матрица нежелательных последствий?

5.Что представляет собой дерево отказов?

6.Каким образом определяются жизненно важные области защищаемого объекта?

Задание 6.2.6 З2(ПК-9) *Планирование защитных мероприятий по видам угроз. Обеспечение информационной безопасности выделенного объекта с учетом особенностей операционной системы.*

1.Какие организационные мероприятия входят в план информационной безопасности?

2.Каким образом производится блокирование каналов возможной утечки информации ограниченного доступа?

3.Что входит в техническую защиту информации ограниченного доступа?

4.Охарактеризуйте методы обнаружения устройств съема информации.

5.Что включают в себя организационно-технические мероприятия обеспечения информационной безопасности?

Задание 6.2.7 З3(ПК-9) *Планирование защитных мероприятий по видам угроз. Обеспечение информационной безопасности выделенного объекта с учетом особенностей операционной системы.*

1.Какие средства служат для разграничения доступа к информации в автоматизированных системах?

2.Какие средства обеспечивают защиту информации при передаче ее по каналам связи?

3.Охарактеризуйте средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем?

4.Какие средства обеспечивают защиту от воздействия программ-вирусов?

5.С помощью чего в информационных системах обеспечивается безопасность хранения, транспортировки носителей информации и защиту их от копирования?

Задание 6.2.8 З3(ПК-9) *Планирование защитных мероприятий по видам угроз. Обеспечение информационной безопасности выделенного объекта с учетом особенностей операционной системы*.

1. Каковы традиционные способы защиты, используемые в Linux и Windows?
2. Как осуществляется защита операционных систем с помощью паролей?
3. Оцените возможности систем Linux и Windows с точки зрения защиты данных.
4. Какие средства защиты графического дисплея предусматриваются в системе Linux?
5. Охарактеризуйте средства сетевой защиты в Linux и Windows.

Задание 6.2.9 З2(ПК-9) *Разработка модели системы информационной безопасности на основе матричной модели.*

1. Охарактеризуйте матричную модель как метод разграничения доступа к объектам.

2. Какими правилами описывается поведение матричной модели защиты информации?
3. Что такое матрица доступа?
4. Что представляет собой модель Лэмпсона?
5. В чем сущность модели Харрисона – Руззо – Ульмана?

Задание 6.2.10 З3(ПК-9) *Разработка модели системы информационной безопасности на основе матричной модели.*

1. Как производится оценка качества системы защиты информации на основе анализа профиля безопасности?
2. Опишите структурную схему формирования системы защиты информации с помощью матрицы?
3. Какие существуют недостатки применения матриц доступа?
4. Каким образом реализована матричная модель организации доступа в системе Linux?

Задание 6.2.11 З1(ПК-9) *Разработка модели системы информационной безопасности на основе матричной модели.*

1. Охарактеризуйте основные этапы создания систем защиты информации?
2. Каким образом производится описание содержания элементов матрицы с целью создания системы защиты информации?
3. Как можно оценить эффективность создаваемой или уже функционирующей системы информационной безопасности?
4. Каковы возможности использования программ для оценки эффективности систем защиты информации?

6.3. Задания, направленные на формирование профессиональных умений.

Задание 6.3.1. У1(ПК-9)

Подготовьте реферат на тему «Подходы к обеспечению информационной безопасности объектов».

Задание 6.3.2. У2(ПК-9)

Составьте презентацию «Принципы системного подхода к защите информации».

Задание 6.3.3. У3(ПК-9)

Подготовьте эссе на тему «Комплексные системы информационной безопасности предприятия и организации».

Задание 6.3.4. У2(ПК-9)

Подготовьте реферат на тему: «Методы нарушения конфиденциальности, целостности и доступности информации».

Задание 6.3.5. У2(ПК-9)

Составьте презентацию «Политика информационной безопасности».

Задание 6.3.6. У3(ПК-9)

Подготовьте реферат на тему «Использование аутентификации в информационных системах».

Задание 6.3.7. У1(ПК-9)

Составьте презентацию «Программно-аппаратные методы и средства обеспечения безопасности».

Задание 6.3.8. У3(ПК-9)

Подготовьте эссе на тему «Методы моделирования информационной безопасности предприятия или организации».

Задание 6.3.9. У3(ПК-9)

Подготовьте реферат на тему «Проектирование системы защиты информации».

6.4. Задания, направленные на формирование профессиональных навыков, владений

Задание 6.4.1. В1(ПК-9)

Определите в каких формах представлена информация на вашем домашнем

компьютере. Опишите, как обеспечивается информационная безопасность вашего компьютера и отвечает ли современным требованиям развития систем безопасности.

Задание 6.4.2. В2(ПК-9)

Определите и классифицируйте угрозы безопасности вашего домашнего компьютера.

Задание 6.4.3. В3(ПК-9)

Предложите схему удаленного администрирования сети филиала. Выбор схемы и соответствующего ПО обоснуйте.

Задание 6.4.4 В1(ПК-9)

Опишите каким образом осуществлено разграничение доступа к информационным ресурсам на вашем компьютере, в случае отсутствия его обоснуйте.

Задание 6.4.5 В1(ПК-9)

Опишите антивирусные программы, которые вы использовали ранее и используете в данный момент. Ваш выбор обоснуйте.

Задание 6.4.6 В3(ПК-9)

Приведите примеры, когда вам приходилось восстанавливать удаленную информацию. Опишите и обоснуйте логическую разбивку вашего жесткого диска.

Задание 6.4.7 В2(ПК-9)

Определите, какие организационные меры используются в учебном процессе университета.

Задание 6.4.8 В1(ПК-9)

Определите какими нормативными документами ограничен круг задач, решаемых вами с использованием вашего домашнего компьютера.

Задание 6.4.9 В2(ПК-9)

Составьте примерный план концепции информационной безопасности университета.

Задание 6.4.10 В3(ПК-9)

Опишите механизмы обеспечения информационной безопасности университета.

Задание 6.4.11 В2(ПК-9)

Разработайте организационные мероприятия по реализации информационной безопасности университета.

Задание 6.4.12 В1(ПК-9)

Разработайте программно-технические мероприятия по реализации информационной безопасности университета.

Задание 6.4.13 В1(ПК-9)

Оцените эффективность мероприятий по реализации информационной безопасности университета.

Соотношение заданий с формируемыми показателями обучения

Формируемая компетенция	***Показатели сформированности компетенции***	***Задания, направленные на: - приобретение новых знаний, углубления и закрепления ранее приобретенных знаний; - формирование профессиональных умений и навыков***
ПК-9 Способность использовать нормативно-правовые документы, международные и отечественные стандарты в	**Владеть:** - инструментальными средствами подготовки проектной документации В1(ПК-9); - методологией работы со стандартами по разработке программной документации В2(ПК-9); - стандартами, руководящими документами и другими нормативными документами, регулирующими процесс разработки технической документации В3(ПК-9).	**Задание 6.4.3** В3(ПК-9) **Задание 6.4.6** В3(ПК-9) **Задание 6.4.9** В2(ПК-9) **Задание 6.4.10** В3(ПК-9) **Задание 6.4.13** В1(ПК-9)

области информационных систем и технологий..	**Уметь:** - разрабатывать основную техническую документацию на проектирование и разработку программного обеспечения У1(ПК-9). - вести процесс разработки и согласования проектной документации (технического задания) У3(ПК-9).	**Задание 6.3.6.** У4(ПК-9) **Задание 6.3.7.** У1(ПК-9) **Задание 6.3.8.** У4(ПК-9) **Задание 6.3.9.** У3(ПК-9)
	Знать: - состав технической документации, подготавливаемой на всех стадиях проектирования информационных систем З1(ПК-9); - основные принципы и методы стандартизации программного обеспечения З3(ПК-9).	**Задание 6.2.3.** З1(ПК-9) **Задание 6.2.8** З4(ПК-9) **Задание 6.2.10** З3(ПК-9) **Задание 6.2.11** З1(ПК-9)

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Средства оценивания в ходе текущего контроля:

7.1.1 Задания для оценки знаний

7.1.1.1 Тестовые задания (ПК-9)

Вопрос № 1: К какому уровню политики информационной безопасности относятся вопросы доступа к тому или иному сервису?

1. нижний
2. средний
3. верхний
4. промежуточный

Вопрос № 2: Выделите утверждение, верное в отношении защиты информационных систем?

1. уровень защищенности системы определяется уровнем защищенности ее самого «сильного» звена
2. уровень защищенности системы определяется суммой уровней защищенности ее звеньев
3. уровень защищенности системы определяется уровнем защищенности ее самого «слабого» звена
4. уровень защищенности системы не зависит напрямую от защищенности ее отдельных звеньев

Вопрос № 3: При отсутствии в системе барьеров, «перекрывающих» выявленные уязвимости, степень сопротивляемости механизма защиты принимается равной…

1. 0
2. 1
3. 2
4. -1

Вопрос № 4: В чем заключается идеология открытых систем информационной безопасности?

1. в открытости программных кодов средств защиты от производителей разных стран
2. в открытости информации о стоимости реализации конкретной системы защиты
3. в строгом соблюдении совокупности профилей, протоколов и стандартов
4. в строгом соответствии систем информационной безопасности законодательству страны, котором они созданы

Вопрос № 5: Какой ключ используется для шифрования данных в ассиметричном криптографическом алгоритме?

1. закрытый
2. открытый
3. прямой
4. обратный

Вопрос № 6: Как называется подход, при котором информационная безопасность реализуется решением совокупности локальных задач по единой программе?

1. частный
2. комплексный
3. интегральный
4. дифференциальный

Вопрос № 7: Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется…

1. опасностью
2. предостережением
3. намерением
4. угрозой

Вопрос № 8: Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется…

1. политикой информации
2. защитой информации
3. политикой безопасности
4. организацией безопасности

Вопрос № 9: Как подразделяются вирусы в зависимости от деструктивных возможностей?

1. сетевые, файловые, загрузочные, комбинированные
2. безвредные, неопасные, опасные, очень опасные
3. резидентные, нерезидентные
4. полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

Вопрос № 10: Распознавание каждого участника процесса информационного взаимодействия перед тем, как к нему будут применены какие бы то ни было понятия информационной безопасности – это…

1. политика
2. идентификация
3. аутентификация
4. авторизация

Вопрос № 11: Обеспечение уверенности в том, что участник процесса обмена информацией определен верно, т.е. действительно является тем, чей идентификатор он предъявил – это…

1. политика
2. идентификация
3. аутентификация
4. авторизация

Вопрос № 12: Создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа – это…

1. политика
2. идентификация
3. аутентификация

4. контроль доступа

Вопрос № 13: Формирование профиля прав для конкретного участника процесса информационного обмена из набора правил контроля доступа – это…

1. авторизация
2.контроль доступа
3. аутентификация
4.политика

Вопрос №14: Обеспечение соответствия возможных потерь от нарушения информационной безопасности затратам на их построение – это…

1. реагирование на инциденты
2. управление конфигурацией
3. управление пользователями
4. управление рисками

Вопрос № 15: Поддержание среды информационного обмена в минимально допустимом работоспособном состоянии и соответствие требованиям информационной безопасности в условиях деструктивны внешних или внутренних воздействий – это…

1. управление рисками
2. обеспечение устойчивости
3. управление конфигурацией
4. реагирование на инциденты

Вопрос № 16: Совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности – это…

1. реагирование на инциденты
2. управление конфигурацией
3. управление пользователями
4. управление рисками

Вопрос № 17: Какой считается информация, по классификации информационных объектов, если без нее можно работать, но очень короткое время?

1. критической
2.очень важной
3.важной
4. полезной

Вопрос № 18: Какой считается информация, по классификации информационных объектов, если без нее можно работать, но ее использование экономит ресурсы?

1. критической
2.очень важной
3.важной
4. полезной

Вопрос № 19: Какой считается по классификации информационных объектов устаревшая или неиспользуемая информация, не влияющая на работу субъекта?

1. важной
2. полезной
3. несущественной
4. вредной

Вопрос № 20: Устройство, хранящее некий уникальный параметр, на основе которого выдается корректный ответ на запрос системы об аутентификации – это…

1. токен
2. брелок
3. карточка

4. мастер-ключ

Вопрос № 21: Основной документ, на основе которого проводится политика информационной безопасности – это…

1. программа информационной безопасности
2. регламент информационной безопасности
3. кодекс информационной безопасности
4. инструкция по информационной безопасности

Вопрос № 22: Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право – это…

1. управление доступом
2. конфиденциальность
3. аутентичность
4. целостность

Вопрос № 23: Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем – это…

1. защита от сбоев в электропитании
2. защита от сбоев устройств для хранения информации
3. защита от сбоев серверов, рабочих станций и локальных компьютеров
4. защита от утечек информации электромагнитных излучений

Вопрос № 24: Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных - это…

1. защита от сбоев серверов, рабочих станций и локальных компьютеров
2. защита от утечек информации электромагнитных излучений
3. защита от сбоев в электропитании
4. защита от сбоев устройств для хранения информации

Вопрос № 25: Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений – это…

1. защита от сбоев серверов, рабочих станций и локальных компьютеров
2. защита от утечек информации электромагнитных излучений
3. защита от сбоев в электропитании
4. защита от сбоев устройств для хранения информации

Вопрос № 26: Обеспечение достоверности и полноты информации и методов ее обработки – это…

1. целостность
2. доступность
3. конфиденциальность
4. защищенность

Вопрос № 27: Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это:

1. идентификация
2. аутентификация
3. регистрация
4. авторизация

Ответы:
1) 1
2) 3
3) 1
4) 3

5) 2
6) 2
7) 4
8) 3
9) 2
10) 2
11) 3
12) 4
13) 1
14) 4
15) 2
16) 1
17) 2
18) 4
19) 3
20) 1
21) 1
22) 2
23) 3
24) 4
25) 2
26) 1
27) 2

№	*Показатели сформированности компетенции*	*ФОС текущего контроля (тестовые задания)*
1.	З1(ПК-9).	1-27
2.	З2(ПК-9).	1-27
3.	З3(ПК-9).	1-27
4.	З1(ПК-9).	1-27
5.	З3(ПК-9).	1-27
6.	З4(ПК-9).	1-27

7.1.2 Задания для оценки умений

7.1.2.1 Примерные темы сообщений (ПК-9)

Сообщения (устная форма) позволяет глубже ознакомиться с отдельными, наиболее важными и интересными процессами, осмыслить, увидеть их сложность и особенности.

1. Информация как объект права собственности.
2. Основные законодательные акты и нормативные документы, касающиеся информационной безопасности в России.
3. Российское законодательство в области охраны авторских прав.
4. Виды тайн.
5. Информационные войны.
6. Классификации угроз информационной безопасности.
7. Случайные угрозы информационной безопасности.
8. Внешние угрозы информационной безопасности.
9. Внутренние (инсайдерские) угрозы информационной безопасности.
10. Физическая защита информационных систем.
11. Программно-технические методы обеспечения информационной безопасности.
12. Регистрация и контроль действий пользователей
13. Криптографические методы защиты информации.
14. Шифрование.
15. Основные методы шифрования.

16. Стандарты шифрования.
17. Вредоносные программы.
18. Информационная безопасность в Интернете.
19. Стратегия злоумышленника при несанкционированном доступе.
20. Электронная цифровая подпись.
21. Критерии оценки безопасности компьютерных систем Министерства обороны США.
22. Европейские критерии безопасности информационных технологий.
23. Функционирование КСЗИ
24. Создание организационной структуры КСЗИ
25. Принципы построения КСЗИ.

№	*Показатели сформированности компетенции*	*ФОС текущего контроля (тематика сообщений)*
1.	У1(ПК-9)	1-25
2.	У2(ПК-9)	1-25
3.	У4(ПК-9)	1-25
4.	У1(ПК-9)	1-25
5.	У3(ПК-9)	1-25
6.	У3(ПК-9)	1-25

7.1.2.2 Темы рефератов (ПК-9)

№	Тема	Опорные слова для раскрытия темы
1.	Источники возникновения и последствия реализации угроз информационной безопасности	Источники возникновения и последствия реализации угроз информационной безопасности. Классификация источников угроз. Антропогенные источники угроз. Техногенные источники угроз. Стихийные источники угроз. Человеческий фактор как антропогенный источник угроз. Внешние источники угроз. Внутренние источники угроз. Последствия воздействия угроз и виды угрожающих воздействий. Классификация угроз по степени тяжести последствий и возможного ущерба.
2.	Криптографические системы защиты данных	Основные задачи криптографии. Криптографические средства защиты. Принципы работы криптосистемы. Управление криптографическими ключами. Симметричная (секретная) методология. Асимметричная (открытая) методология. Алгоритмы шифрования Симметричные алгоритмы. Асимметричные алгоритмы. Хеш-функции. Механизмы аутентификации. Электронные подписи и временные метки. Стойкость шифра.
3.	Настройка безопасности ОС Windows	Виды опасностей и средства защиты операционной системы Windows. Классификация источников опасностей. Виды антивирусов и сравнение их эффективности. Сравнение эффективности фаерволов. Сравнение эффективности руткитов. Установка и настройка программ защиты операционной системы Windows. Встроенная защита Windows. Установка антивируса. Установка фаервола.
4.	Модели информационной безопасности	Модели безопасности и их применение. Модель дискреционного доступа (DAC). Модель безопасности Белла – Ла Падулы. Ролевая модель контроля доступа (RBAC). Системы разграничения доступа. Предназначения моделей безопасности.
5.	Исследование уровня безопасности операционной системы Linux	Основные понятия компьютерной безопасности. Локальная и сетевая безопасность Linux. Пользователи и пароли. Особенности файловой системы Linux. Права доступа. Атрибуты файлов . Механизм квот. Библиотека PAM. Брандмауэр. Удаленное управление. Средства усиления безопасности в Linux. Linux ACLs. LIDS. AIDE. Техника безопасности.
6.	Защита баз данных	Понятие защиты информации. Защита ПК от несанкционированного доступа. Защита информации в базах данных. Реализация защиты в некоторых СУБД. Архитектура защиты Microsoft AccessMS SQL Server. Организация защиты. Вопросы безопасности доступа. Управление доступом. Тип подключения к SQL Server. Роли.

		Безопасность данных в Oracle 7. Ограничение доступа. Использование пакетов. Юридическая защита авторских прав на базы данных.
7.	Программно технические средства обнаружения сетевых атак	Классификация сетевых атак. Классификация по уровню модели OSI. Классификация по типу. Классификация по местоположению злоумышленника и атакуемого объекта. Анализ угроз сетевой безопасности. Проблема безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей. Технологии обнаружения атак. Методы анализа сетевой информации. Классификация систем обнаружения атак IDS. Компоненты и архитектура IDS. Методы реагирования.
8.	Радиоэлектронные каналы утечки информации	Радиоэлектронный канал. Структура радиоэлектронного канала утечки информации. Виды утечки информации. Антенные устройства. Классификация помех.
9.	Компьютерные вирусы. Классификация	Файловые вирусы. Загрузочные, комбинированные вирусы и вирусы-спутники. Вирусы в пакетных файлах, шифрующиеся и полиморфные вирусы, стелс-вирусы и макрокомандные вирусы. Вредоносные программы других типов: троянские программы, логические бомбы и программы-черви. Вирусы в системе документооборота. Новые и экзотические вирусы.
10.	Программные закладки и защита от них	Клавиатурные шпионы. Имитаторы (приглашения для аутентификации). Троянские кони. Внедрение, выявление программных закладок и защита от них.
11.	Аппаратно-программные средства защиты информации	Системы идентификации и аутентификации пользователей. Методы обеспечения информационной безопасности. Системы шифрования данных, передаваемых по сетям. Системы аутентификации электронных данных. Средства управления криптографическими ключами.
12.	Разработка системы информационной безопасности	Рекомендации по разработке концепции информационной безопасности. Разработка политики ИБ и выбор решений по обеспечению политики ИБ. Административный уровень ИБ. Организационный уровень ИБ. Технический уровень ИБ. Создание системы информационной безопасности.
13.	Уровни информационной защиты	Законодательный уровень. Административный уровень (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами). Процедурный уровень (меры безопасности, ориентированные на людей). Программно-технический уровень.
14.	Концепция информационной безопасности	Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности. Угрозы конфиденциальной информации. Действия, приводящие к неправомерному овладении конфиденциальной информацией.
15.	Защита информации от утечки по техническим каналам	Защита информации от утечки по визуально оптическим каналам. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным каналам. Защита информации от утечки по материально-вещественным каналам
16.	Противодействие несанкционированному доступу к источникам конфиденциальной информации	Способы несанкционированного доступа. Технические средства несанкционированного доступа к информации. Защита от наблюдения и фотографирования. Защита от подслушивания. Противодействие незаконному подключению к линиям связи. Противодействие контактному подключению. Противодействие бесконтактному подключению. Защита о т перехвата
17	Объектно-ориентированный подход к информационной безопасности	Необходимость применения объектно-ориентированного подхода к информационной безопасности. Основные понятия объектно-ориентированного подхода. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения
18.	Основные критерии и классификации угроз	Основные понятия об угрозах. Наиболее распространенные угрозы доступности. Примеры угроз доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности.
19	Защита информации от утечки по	Защита от утечки за счет микрофонного эффекта. Защита от утечки за

	электромагнитным каналам	счет электромагнитного излучения. Защита от утечки за счет паразитной генерации. Защита от утечки по цепям питания. Защита от утечки по цепям заземления. Защита от утечки за счет взаимного влияния проводов и линий связи. Защита от утечки за счет высокочастотного навязывания. Защита от утечки в волоконно-оптическим линиях и системах связи
20	Стандарты в области информационной безопасности	Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Рекомендации X.800. Стандарт ISO/IEC 15408 «Общие критерии оценки безопасности. Руководящие документы Гостехкомиссии России.
21	Административный уровень информационной безопасности	Основные понятия административного уровня информационной безопасности. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Понятие об управлении рисками.
22	Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.
23	Основные принципы криптографической защиты информации	Понятие криптографии. Понятия о симметричных и асимметричных криптосистемах. Понятие криптоанализа. Аппаратно-программные криптографические средства защиты информации.
24	Асимметричные криптосистемы	Концепция криптосистемы с открытым ключом. Однонаправленные функции. Криптосистема шифрования данных RSA. Процедуры шифрования и расшифрования в криптосистеме. RSA. Пример использования алгоритма RSA. Безопасность и быстродействие криптосистемы RSA. Аутентификация данных и электронная цифровая подпись. Алгоритм цифровой подписи RSA.
25	Симметричные криптосистемы	Понятие о симметричной криптосистеме. Шифры перестановки. Шифрующие таблицы. Система шифрования Цезаря. Аффинная система подстановок Цезаря. Система Цезаря с ключевым словом. Шифры сложной замены. Одноразовая система шифрования. Шифрование методом гаммирования. Стандарт шифрования данных DES.
26	Межсетевые экраны	Межсетевые экраны прикладного уровня. Межсетевые экраны с пакетной фильтрацией. Гибридные межсетевые экраны. Пример конфигурирования межсетевого экрана.
27	Аутефекация и управление сертификатами	Цифровые подписи. Управление ключами и сертификация ключей. Концепция доверия в информационной системе. Иерархическая модель доверия. Сетевая модель доверия. Аутентификация с использованием протоколов открытого ключа.

№	*Показатели сформированности компетенции*	*ФОС текущего контроля (тематика рефератов)*
1.	У1(ПК-9)	1-27
2.	У2(ПК-9)	1-27
3.	У4(ПК-9)	1-27
4.	У1(ПК-9)	1-27
5.	У3(ПК-9)	1-27
6.	У3(ПК-9)	1-27

7.1.2.3. Примерная тематика презентаций (ПК-9)

Презентация – набор слайдов в Power Point. Выступление по презентации не требуется и оценивается дополнительно.

Преподаватель каждый раз выбирает самостоятельно количество слайдов (в зависимости от количества учебных часов по дисциплине) от 10 слайдов и до 30 по одной проблематике.

Название документа – ФИО студента (Иванов И.П.ppt);

Первый слайд – тема презентации, далее – сам материал. План, актуальность темы, введение, заключение и список литературы не являются составной частью презентации и

делаются студентом по собственному желанию.

Презентация в обязательном порядке включает следующие элементы:

- картинки и фото;
- графические элементы;
- классификации;
- таблицы;
- логические цепочки;
- схемы;
- выводы.

Ссылка при цитировании на источник в презентации обязательна. Все данные должны быть сопровождены годами.

1. Презентация на тему «Администрирование информационных систем Шифрование»
   - Средства защиты информационных систем.
   - Шифрование.
   - Сертификаты сервера.
   - Сертификаты клиента.
   - Сертификаты подписывания кода.
   - Ключи сертификатов.
   - Криптографические средства защиты данных.
   - Бюро сертификатов.
2. Презентация на тему «Виды угроз в информационной системе».
   - Основные определения и критерии классификации угроз.
   - Виды угроз, возникающие в ИС.
   - Ошибочные действия пользователей и персонала.
   - Ошибки в программном обеспечении.
   - Компьютерные вирусы и другие вредоносные программы.
   - Человеческий фактор.
   - Основные задачи защиты.
   - Уровни защиты
3. Презентация на тему «Модель угроз безопасности персональных данных при их обработке в информационных системах».
   - Основные элементы информационной системы персональных данных.
   - Виды угроз безопасности персональных данных.
   - Виды несанкционированных действий, осуществляемых с персональными данными.
   - Угрозы несанкционированного доступа к информации.
   - Уязвимости системного программного обеспечения.
   - Уязвимости прикладного программного обеспечения.
4. Презентация на тему «Обеспечение безопасности ОС семейства Linux».
   - Обеспечение безопасности рабочей станции.
   - Обеспечение безопасности сервера.
   - Защита окружения Linux.
   - Парольная защита.
   - Защита BIOS и загрузчика системы.
5. Презентация на тему «Обеспечение безопасности корпоративных информационных систем».
   - Понятие информационной безопасности.
   - Угрозы информационной безопасности.
   - Обеспечение безопасности информационных систем.
   - Меры и средства программно-технического уровня.
   - Организационно-экономическое обеспечение безопасности.
   - Правовое обеспечение безопасности.

6. Презентация на тему «Каналы утечки информации»
   - Документация.
   - Персонал.
   - Технические средства.
   - Интернет как канал утечки.
   - Предотвращение утечки интеллектуальных прав.

№	*Показатели сформированности компетенции*	*ФОС итогового контроля (тематика презентаций)*
1.	З1(ПК-9).	1-6
2.	З2(ПК-9).	1-6
3.	З3(ПК-9).	1-6
4.	З1(ПК-9).	1-6
5.	З3(ПК-9).	1-6
6.	З4(ПК-9).	1-6

7.1.3 Задания для оценки навыков, владений, опыта деятельности

7.2.3.1 Задачи по дисциплине (ПК-9)

Задача 1.

В операционной системе Windows XP настроить политику учетных записей установив следующие параметры:

· максимальный срок действия пароля 45 дней;
· минимальная длина пароля 8 символов;
· минимальный срок действия пароля 5 дней;
· пароль должен отвечать требованиям сложности;
· пароли не должны повторяться;
· хранимые пароли должны быть зашифрованы.

Задача 2.

В операционной системе Windows XP настроить политику блокировки учетных записей установив следующие параметры:

· блокировка учетной записи на 60 минут после 5 попыток ввода неправильного пароля.
· сбор счетчика попыток через 30 минут.

Задача 3.

В операционной системе семейства Linux произвести настройку протокола безопасных соединений – SSH.

Задача 4.

В операционной системе Windows Server настроить аудит доменных служб Active Directory.

Задача 5.

Провести настройку RAID массива с целью повышения безопасности данных посредством одновременной записи на два разных диска.

Задача 6.

Провести настройку брандмауэра в Windows 7 для обеспечения повышенного уровня защиты.

№	*Показатели сформированности компетенции*	*ФОС итогового контроля (тематика презентаций)*
1.	В1(ПК-9).	1-6
2.	В2(ПК-9).	1-6
3.	В3(ПК-9).	1-6
4.	В1(ПК-9).	1-6
5.	В2(ПК-9).	1-6

6.	В3(ПК-9).	1-6

7.2 ФОС для промежуточной аттестации

7.2.1 Задания для оценки знаний

Вопросы к зачету (ПК-9)

1. Комплексный подход и системность при обеспечении информационной безопасности.
2. Сущность задачи управления информационной безопасностью.
3. Выявление каналов утечки информации.
4. Анализ защищенности выделенного объекта.
5. Разработка модели угроз.
6. Разработка модели нарушителя.
7. Механизмы безопасности ОС Linux и Windows.
8. Основные атаки на ОС Linux и меры противодействия им.
9. Общее описание матричной модели системы информационной безопасности.
10. Понятие и назначение модели безопасности.
11. Административные меры защиты.
12. Программно-технические меры защиты.
13. Уровни политики безопасности.
14. Модель дискреционного доступа.
15. Ролевая модель контроля доступа.
16. Матрица доступа и ее представления.
17. Системы разграничения доступа.
18. Задачи системы информационной безопасности.
19. Меры противодействия угрозам безопасности.
20. Основные принципы построения систем защиты.

№	*Показатели сформированности компетенции*	*ФОС промежуточного контроля (вопросы к зачету)*
1.	З1(ПК-9)	1-19
2.	З2(ПК-9)	1-19
3.	З3(ПК-9)	1-19
4.	З1(ПК-9)	1-6, 9-19
5.	З3(ПК-9)	1-6, 9-19

7.2.2 Задания для оценки умений

В качестве фондов оценочных средств для оценки умений обучающегося используются задания, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.2)

7.2.3 Задания для оценки навыков, владений, опыта деятельности

В качестве фондов оценочных средств для оценки навыков, владений, опыта деятельности обучающегося используются задания, рекомендованные для выполнения в часы самостоятельной работы (раздел 6.3).

8. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Литература

а) Основная

1. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

б) Дополнительная

1. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 c. — 978-5-4487-0299-0. — Режим доступа: http://www.iprbookshop.ru/77318.html

2. Семененко В.А. Информационная безопасность: Учебное пособие. – М.: МГИУ, 2006. (Гриф)

3. Информационная безопасность: учебно-методич.комплекс/ автор-сост. Е.Е. Шиловская. – М.: Изд-во РАГС, 2009.

9. ПЕРЕЧЕНЬ КОМПЛЕКТОВ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО ПРИ ИЗУЧЕНИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

При изучении учебной дисциплины (в том числе в интерактивной форме) предполагается применение современных информационных технологий. Комплект программного обеспечения для их использования включает в себя: операционная система Microsoft Windows 7 Pro, офисный пакет программ Microsoft Office Professional Plus 2010, офисный пакет программ Microsoft Office Professional Plus 2007, антивирусная программа Dr. Web Desktop Security Suite, архиватор 7-zip, аудиопроигрыватель AIMP, просмотр изображений FastStone Image Viewer, ПО для чтения файлов формата PDF Adobe Acrobat Reader, ПО для сканирования документов NAPS2, ПО для записи видео и проведения видеотрансляций OBS Studio, ПО для удалённого администрирования Aspia, правовой справочник Гарант Аэро, онлайн-версия КонсультантПлюс: Студент, электронно-библиотечная система IPRBooks, электронно-библиотечная система Юрайт, математические вычисления Mathcad 14 University, версия 1С для использования типовых конфигураций в учебных целях: 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях, моделирование бизнес-процессов CA ERwin Process Modeler 7.3, версия 1С для обучения программированию: 1С: Предприятие 8.2 Версия для обучения программированию

10. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Российская государственная публичная библиотека http://elibrary.rsl.ru/
2. Электронно-библиотечная система (ЭБС), Издательство Юстицинформ// http://e.lanbook.com/books/
3. Библиотека Российского государственного гуманитарного университета http://liber.rsuh.ru/
4. Сайт Института развития информационного общества http://www.iis.ru
5. Сайт научно-аналитического журнала «Информационное общество» http://www.infosoc.iis.ru
6. Энциклопедия информационного общества http://wiki.iis.ru
7. Образовательная платформа ЮРАЙТ https://urait.ru
8. ЭБС IPRbooks (АйПиАрбукс) http://www.iprbookshop.ru

11. ОБУЧЕНИЕ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Изучение данной учебной дисциплины обучающимися с ограниченными возможностями здоровья осуществляется в соответствии с Приказом Министерства образования и науки РФ от 9 ноября 2015 г. № 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн, «Положением о порядке обучения студентов – инвалидов и лиц с ограниченными возможностями здоровья», утвержденным приказом ректора от 6 ноября 2015 года №60/о, «Положением о службе инклюзивного образования и психологической помощи» АНО ВО «Российский новый университет» от 20 мая 2016 года № 187/о.

Предоставление специальных технических средств обучения коллективного и индивидуального пользования, подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится преподавателями с учетом их индивидуальных психофизиологических особенностей и специфики приема передачи учебной информации.

С обучающимися по индивидуальному плану и индивидуальному графику проводятся индивидуальные занятия и консультации.

12. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля успеваемости и промежуточной аттестации

Ауд.305 (компьютерный класс № 3)

Специализированная мебель:

- столы студенческие;
- стулья студенческие;
- стол для преподавателя;
- стул для преподавателя;
- столы компьютерные;
- кресла компьютерные;
- шкаф для хранения раздаточного материала;
- доска (меловая);
- маркерная доска (переносная).

Технические средства обучения:

- проектор (портативный);
- ПК для преподавателя с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду вуза;
- ПК для обучающихся с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду;

год начала подготовки 2018

- веб-камера;
- экран (переносной);
- колонки;
- микрофон.

Специализированное оборудование:
- наглядные пособия (плакаты), информационный стенд

Автор (составитель): к.п.н., доцент Гнездилова Н.А. _____
Подпись

год начала подготовки 2018

Аннотация рабочей программы учебной дисциплины
СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Код и направление подготовки: **09.03.03 «Прикладная информатика»**
Направленность (профиль): **«Прикладная информатика в экономике»**

Цели освоения дисциплины

Обеспечение профессионального образования, способствующего социальной, академической мобильности, востребованности на рынке труда, успешной карьере, сотрудничеству.

Формирование у обучающихся систематизированных профессионально значимых знаний по вопросам информатики, связанных с информационной безопасностью, и профессиональных умений и навыков, необходимых бакалавру.

Освоение технологий информационной безопасности, в том числе ознакомление с методами управления информационными ресурсами, обеспечивающими защиту информации в современных ЭВМ, комплексах, системах и сетях, а также изучение законодательной базы и стандартов в области информационной безопасности.

Место дисциплины в структуре ОП бакалавриата.

Учебная дисциплина «Системы информационной безопасности» относится к вариативной части учебного плана (Б1.В.ДВ.08.02).

Содержание учебной дисциплины тесно связано с логикой и содержанием других изучаемых дисциплин. Для успешного усвоения курса «Системы информационной безопасности» студент должен изучить курсы: «Информационные системы и технологии», «Правовые основы прикладной информатики в экономике».

Дисциплина «Системы информационной безопасности» является необходимой базой для последующего освоения дисциплин профессионального цикла основной образовательной программы таких как: «Информационная безопасность», «Предметно-ориентированные экономические и информационные системы», «Системы электронной коммерции».

Дисциплина изучается на заочной форме обучения на 4 курсе в 7 и 8 семестрах.

Требования к уровню освоения содержания курса:

В результате освоения дисциплины обучающийся должен овладеть следующими компетенциями:

ПК-9. Способность использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий

Содержание учебной дисциплины.

1. Основные принципы построения систем информационной безопасности
2. Общие характеристики защищаемого объекта.
3. Планирование защитных мероприятий по видам угроз. Обеспечение информационной безопасности выделенного объекта с учетом особенностей операционной системы.
4. Разработка модели системы информационной безопасности на основе матричной модели.

Лист внесения изменений в рабочую программу учебной дисциплины «Системы информационной безопасности»

Рабочая программа рассмотрена и одобрена на 2021/2022 учебный год.
Протокол № 10 заседания кафедры ПЭ от «11» июня 2021 г.

1. Актуализация перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины на 2021-2022 учебный год.

1.1.Пункт 8.1. Основная литература

1. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 c. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html
2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

1.2.Пункт 8.2.Дополнительная литература

1. Фомин Д.В. Информационная безопасность [Электронный ресурс] : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 125 c. — 978-5-4487-0299-0. — Режим доступа: http://www.iprbookshop.ru/77318.html
2. Семененко В.А. Информационная безопасность: Учебное пособие. – М.: МГИУ, 2006. (Гриф)
3. Информационная безопасность: учебно-методич.комплекс/ автор-сост. Е.Е. Шиловская. – М.: Изд-во РАГС, 2009.

Зав. кафедрой ____/Преснякова Д.В./