

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Романчук Иван Сергеевич
Должность: Ректор
Дата подписания: 24.04.2025 17:16:21
Уникальный программный ключ:
6319edc2b582ffdacea443f01d5779368d0957ac34f5cd074d81181530452479

Приложение к рабочей
программе дисциплины

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Наименование дисциплины	<i>Кибербезопасность</i>
Направление подготовки / Специальность	<i>38.04.01 Экономика</i>
Направленность (профиль) / Специализация	<i>Цифровая экономика ОП ВО</i>
Форма обучения	<i>очная</i>
Разработчик	<i>Зюбан Е.В. доцент кафедры экономической безопасности, системного анализа и контроля</i>

1. Темы дисциплины для самостоятельного освоения обучающимися:
Отсутствуют

2. План самостоятельной работы:

№ п/п	Учебные встречи	Виды самостоятельной работы	Форма отчетности / контроль	Количество баллов	Рекомендуемый бюджет времени на выполнение (ак.ч.)
1.	Международные стандарты информационного обмена. Понятие угрозы.	1. Подготовка к практическому занятию	1. Собеседование	-	1
2.	Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».	1. Подготовка к практическому занятию	1. Собеседование	-	2
3.	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	1. Подготовка к практическому занятию	1. Собеседование	-	2
4.	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	1. Подготовка к практическому занятию	1. Собеседование	-	1
		2. Выполнение расчетных заданий	2. Решение задач	7	24
5.	Концепция информационной безопасности.	1. Подготовка к практическому занятию	1. Собеседование	7	1
6.	Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной	1. Подготовка к практическому занятию	1. Собеседование	-	1

	безопасности страны				
7.	Зачет	Изучение материалов по дисциплине по вопросам к зачету	1. Контрольная работа	-	8
	Итог			14	40

3. Требования и рекомендации по выполнению самостоятельных работ обучающихся, критерии оценивания.

Вид: Подготовка к практическому занятию.

Краткая характеристика: в ходе подготовки к практическим занятиям необходимо повторить лекционный материал по теме учебной встречи, повторно реализовать скрипты примеров решения задач, представленных в лекционном материале и в основной и дополнительной литературе. В качестве формы контроля по подготовке к практическим занятиям применяется собеседование.

Собеседование – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т. п.

Рекомендации для подготовки к собеседованию:

- повторить лекционный материал по теме учебной встречи, повторно реализовать скрипты примеров решения задач, представленных в лекционном материале;
- изучить основную и дополнительную литературу, определенную рабочей программой дисциплины, по теме учебной встречи, повторно реализовать скрипты примеров решения задач, представленных в основной и дополнительной литературе.
- подготовить перечень вопросов преподавателю, вызвавших затруднения при повторении лекционного материала, изучении основной и дополнительной литературы.

Тематика вопросов для подготовки к собеседованию на учебной встрече:

№ п/п	Учебная встреча	Вопросы для подготовки к собеседованию на учебной встрече
1.	Международные стандарты информационного обмена. Понятие угрозы.	1. Что такое международный стандарт информационного обмена? 2. Какие угрозы существуют в информационной среде? 3. Какие международные стандарты разработаны для борьбы с угрозами? 4. Как эти стандарты применяются в реальной практике? 5. Какие меры предпринимаются для обеспечения безопасности информации? 6. Какими инструментами пользуются пользователи для защиты своих данных? 7. Какие организации занимаются разработкой стандартов в этой области? 8. Как международные стандарты влияют на национальные законы? 9. Какие изменения произошли в международных стандартах за последнее время?

		10. Как стандарты помогают в решении проблем, возникающих на международном уровне?
2.	Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».	1. Что такое информационная безопасность в условиях глобальной сети? 2. Какие угрозы существуют в российской информационной среде? 3. Кто является основными нарушителями информационной безопасности в России? 4. Какие меры предпринимает государство для защиты от угроз? 5. Какие методы используются для обнаружения нарушений? 6. Как международные стандарты влияют на информационную безопасность в России? 7. Какие проблемы возникают при взаимодействии с международными сетями? 8. Как противодействуют внешним угрозам в России? 9. Какие стратегические инициативы предпринимает Россия для повышения уровня защиты? 10. Как развиваются международные стандарты в области информационной безопасности?
3.	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	1. Что такое таксономия нарушений информационной безопасности? 2. Какие уровни классификации существуют в таксономии? 3. Какие категории нарушений выделяются в таксономии? 4. Какие причины приводят к возникновению нарушений? 5. Какие типы нарушений встречаются чаще всего? 6. Как классифицируются нарушения по степени тяжести? 7. Какие меры принимают для предотвращения нарушений? 8. Как реагируют на инциденты с нарушениями? 9. Какие методы используются для диагностики и устранения нарушений? 10. Как развивалась таксономия с течением времени? 11. Какие уроки можно извлечь из международного опыта?
4.	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Концепция информационной безопасности.	1. Что подразумевает под собой концепция информационной безопасности на государственном уровне? 2. Какие задачи ставит перед собой государство в обеспечении информационной безопасности? 3. Какие механизмы использует государство для достижения этих задач? 4. Как определяются приоритеты в политике информационной безопасности?

		- Какие инструменты и методы разрабатываются государственными органами для защиты информации? - Какова роль регуляторов в формировании политики информационной безопасности? - Какие нормативные акты регулируют сферу информационной безопасности? - Как государство сотрудничает с частными компаниями и организациями в этом направлении? - Какие вызовы сталкивается государство в обеспечении информационной безопасности? - Как решается проблема дефицита кадров в этой области?
5.	Концепция информационной безопасности.	- Какие основные технологии используются для построения защищённых корпоративных информационных систем (ЭИС)? - Как обеспечивается безопасность данных в корпоративных системах? - Какие меры предпринимания организации для защиты информации? - Как связаны информационные системы с вопросами национальной безопасности? - Какова роль государственных органов в обеспечении безопасности корпоративных систем? - Какие риски существуют для корпоративных систем в части информационной безопасности? - Какие подходы применяются для минимизации этих рисков? - Какие стандарты и нормы регулируют информационную безопасность в России? - Как строится политика информационной безопасности на государственном уровне? - Какие инициативы предпринимаются государством для поддержки компаний в этой области?
6.	Основные технологии построения защищённых ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.	- Что такое международная стандарт информационной безопасности? - Какие угрозы рассматриваются в международных стандартах? - Какие стандарты разработаны для борьбы с угрозами? - Как международные стандарты применяются в России? - Какие меры и методы используются для защиты информации? - Какие риски присутствуют в информационной безопасности? - Какие международные стандарты участвуют в защите информации? - Какие подходы используются для обнаружения угроз?

		9. Как международные стандарты влияют на политику информационной безопасности в России? 10. Какие инициативы государства и частных компаний поддерживают стандарты?
--	--	---

Вид: Выполнение расчетных заданий.

Краткая характеристика: расчетные задания, дифференцированные по следующим уровням:

1. Расчетные задания реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей;
2. Расчетные задания творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

Расчетные задания по теме «Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Концепция информационной безопасности.» представлены комплексом задач по темам, изученным в первой половине семестра:

Задачи

1. Анализ нормативно-правовой базы

Задача: Изучите основные нормативные акты Российской Федерации, регулирующие вопросы информационной безопасности (например, Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации", Указ Президента РФ № 646 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена"). Определите ключевые положения этих документов, касающиеся защиты государственной тайны, персональных данных и других видов конфиденциальной информации.

Задание:

Составьте таблицу с перечислением основных нормативных актов и их ключевых положений.

Приведите примеры конкретных мер, которые должны быть приняты для выполнения требований законодательства.

2. Разработка концепции информационной безопасности организации

Задача: Разработать концепцию информационной безопасности для гипотетической государственной структуры (например, министерства). В рамках этой концепции необходимо определить цели, задачи, принципы и механизмы обеспечения информационной безопасности.

Задание:

Опишите миссию и стратегические цели организации в области информационной безопасности.

Перечислите основные угрозы и риски, которым может подвергаться организация.

Разработайте меры по предотвращению и реагированию на инциденты

информационной безопасности.

Предложите структуру управления информационной безопасностью в организации.

3. Оценка рисков информационной безопасности

Задача: Провести анализ рисков информационной безопасности для государственного учреждения. Необходимо оценить вероятность возникновения различных угроз и возможные последствия для организации.

Задание:

Определите основные виды угроз (например, утечка данных, несанкционированный доступ к системам, кибератаки).

Проведите оценку вероятности каждой угрозы и возможных последствий (финансовых потерь, репутационного ущерба, нарушения работы системы).

Представьте результаты анализа в виде таблицы или диаграммы.

4. Разработка плана действий в случае инцидента

Задача: Составить план действий на случай возникновения инцидента информационной безопасности в государственном учреждении. План должен предусматривать оперативное реагирование, минимизацию ущерба и восстановление нормальной работы.

Задание:

Описать последовательность шагов, которые следует предпринять при обнаружении инцидента.

Назначить ответственных лиц за выполнение каждого этапа плана.

Укажите временные рамки для выполнения каждого действия.

5. Разработка политики информационной безопасности

Задача: Создать проект политики информационной безопасности для государственной организации. Политика должна определять правила использования информационных ресурсов, доступа к ним, а также ответственность сотрудников за нарушение правил.

Задание:

Определите основные разделы политики (общие положения, права и обязанности пользователей, требования к защите информации, порядок обработки инцидентов).

Разработайте конкретные рекомендации по использованию электронной почты, интернета, мобильных устройств и т.д.

Включите раздел об ответственности за нарушение политики.

4. Рекомендации по самоподготовке к промежуточной аттестации по дисциплине.

Форма проведения промежуточной аттестации – контрольная работа.

Краткая характеристика: средство проверки умений применять полученные знания для решения задач определенных типов по дисциплине.

Рекомендации для подготовки:

1. Повторение лекционного материала, самостоятельная реализация скриптов примеров решения задач, представленных в лекционном материале;
2. Чтение основной и дополнительной литературы, самостоятельная реализация скриптов примеров решения задач, представленных в основной и дополнительной литературе;

Контрольная работа состоит из пяти расчетных задач. Типы задач контрольной работы повторяют типы задач, решенных в течение семестра обучающимися самостоятельно и совместно с преподавателем.

Тематика расчетных задач контрольной работы, проводимой в рамках экзамена:

1. Анализ уязвимостей и оценка риска
2. Шифрование и криптография
3. Системы обнаружения вторжений (IDS/IPS)
4. Управление доступом и аутентификацией
5. Безопасность беспроводных сетей
6. Защита от вредоносного ПО
7. Реагирование на инциденты
8. Аудит безопасности
9. Криптографические хеш-функции
10. Цифровые подписи и сертификаты