Приложение к рабочей программе дисциплины

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

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

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
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	-	1
3.	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	1. Подготовка к практическому занятию	1. Собеседование	-	1
4.	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Концепция информационной безопасности.	1. Подготовка к практическому занятию	1. Собеседование	-	1
		2. Выполнение расчетных заданий	2. Решение задач	7	5
5.	Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности	1. Подготовка к практическому занятию	1. Собеседование	-	1

	страны.				
6.	Международные стандарты информационного обмена. Понятие угрозы.	1. Подготовка к практическому занятию	1. Собеседование	-	1
7.	Стратегия безопасности	1. Подготовка к практическому занятию	1. Собеседование	-	4
8.	Жизненный цикл атаки	1. Подготовка к практическому занятию	1. Собеседование	-	6
		2. Выполнение расчетных заданий	2. Решение задач	7	5
9.	Подготовка к зачету	Изучение материалов по дисциплине по вопросам к зачету	-	-	12
	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? 5. Какие инструменты и методы разрабатываются государственными органами для защиты информации? 6. Какова роль регуляторов в формировании политики информационной безопасности? 7. Какие нормативные акты регулируют сферу информационной безопасности? 8. Как государство сотрудничает с частыми компаниями и

		организациями в этом направлении? 9. Какие вызовы сталкивается государство в обеспечении информационной безопасности? 10. Как решается проблема дефицита кадров в этой области?
5.	Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.	1. Какие основные технологии используются для построения защищённых корпоративных информационных систем (ЭИС)? 2. Как обеспечивается безопасность данных в корпоративных системах? 3. Какие меры предпринимания организации для защиты информации? 4. Как связаны информационные системы с вопросами национальной безопасности? 5. Какова роль государственных органов в обеспечении безопасности корпоративных систем? 6. Какие риски существуют для корпоративных систем в части информационной безопасности? 7. Какие подходы применяются для минимизации этих рисков? 8. Какие стандарты и нормы регулируют информационную безопасность в России? 9. Как строится политика информационной безопасности на государственном уровне? 10. Какие инициативы предпринимаются государством для поддержки компаний в этой области?
6.	Международные стандарты информационного обмена. Понятие угрозы.	1. Что такое международная стандарт информационной безопасности? 2. Какие угрозы рассматриваются в международных стандарах? 3. Какие стандарты разработаны для борьбы с угрозами? 4. Как международные стандарты применяются в России? 5. Какие меры и методы используются для защиты

		информации? 6. Какие риски присутствуют в информационной безопасности? 7. Какие международные стандарты участвуют в защите информации? 8. 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?
7.	Стратегия безопасности	1. Что такое стратегия безопасности? 2. Какие цели и задачи стратегия безопасности определяет? 3. Какие подходы и методы используются для разработки стратегии безопасности? 4. Как стратегия безопасности интегируется с другими аспектами управления проектами? 5. Какие угрозы и риски стратегия безопасности рассматривает? 6. Какие инструменты и технологии применяются для реализации стратегии безопасности? 7. Как стратегия безопасности влияет на эффективность проектов? 8. Какие меры принимаются для защиты информации? 9. Как стратегия безопасности помогает решать задачи и проблемы? 10. Какие задачи и задачи стратегия безопасности решает на протяжении времени?
8.	Жизненный цикл атаки	1. Что такое жизненный цикл атаки? 2. Какие этапы жизненного цикла атаки включают? 3. Какие факторы влияют на каждый этап жизненного цикла атаки? 4. Как различать жизненные циклы атак? 5. Какие механизмы защиты

		информации используются на каждом этапе жизненного цикла атаки? 6. Какие угрозы возникают на каждом этапе жизненного цикла атаки? 7. Как защищать информацию на каждом этапе жизненного цикла атаки? 8. Какие подходы и методы применяются для обнаружения атак? 9. Какие меры и стратегии применяются для нейтрализации атак? 10. Какие барьеры и ограничения возникают при защите информации?

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.

Расчетные задания по теме «Современные технологии в контексте управления проектами» представлены комплексом задач по темам, изученным во второй половине семестра:

Задание 1: Классификация типов атак

Описание задачи: На основе изучения материалов курса, классифицируйте различные типы атак, описав их особенности и методы реализации. Примеры атак включают:

- Атака типа "отказ в обслуживании" (DoS)
- Фишинговые атаки
- SQL-инъекции
- XSS-атаки

Задание:

- Создайте таблицу, содержащую описание каждого типа атаки, включая ее цель, используемые инструменты и потенциальные последствия.
- Для каждой атаки предложите хотя бы два метода предотвращения или смягчения последствий.

Задание 2: Моделирование жизненного цикла атаки

Описание задачи: Построение модели жизненного цикла типичной атаки на информационную систему. Эта модель должна отражать все этапы атаки от разведки до эксплуатации уязвимостей и постэксплуатации.

Задание:

- Нарисуйте схему жизненного цикла атаки, указывая каждый этап и его характеристики.
- Для каждого этапа укажите типичные действия злоумышленника и возможные контрмеры со стороны защитников.

Задание 3: Разведка и сбор информации

Описание задачи: Проанализируйте процесс разведки и сбора информации перед проведением атаки. Рассмотрите как пассивные, так и активные методы разведки.

Задание:

- Опишите не менее трех методов пассивной разведки (например, использование поисковых систем, OSINT) и три метода активной разведки (например, сканирование портов, зондирующие запросы).
- Приведите пример ситуации, когда каждая из перечисленных техник могла бы быть использована злоумышленником.

Задание 4: Эксплуатация уязвимости

Описание задачи: Рассмотрите различные способы эксплуатации уязвимостей в информационных системах. Особое внимание уделите вопросам использования эксплойтов и автоматизации процесса поиска уязвимостей.

Задание:

- Выберите одну известную уязвимость (например, Heartbleed, Shellshock) и опишите, каким образом она может быть использована злоумышленниками.
- Подберите подходящий эксплойт для данной уязвимости и объясните, как он работает.
- Предложите меры по устранению данной уязвимости и защите системы.

Задание 5: Постэксплуатационные действия

Описание задачи: После успешной эксплуатации уязвимости злоумышленники часто стремятся сохранить доступ к системе и расширить свои возможности. Проанализируйте возможные постэксплуатационные действия и методы их обнаружения.

Задание:

- Перечислите не менее пяти постэксплуатационных действий (например, установка

бэкдоров, кража данных, изменение конфигураций).
- Для каждого действия предложите способ его обнаружения и нейтрализации.
- Разработайте стратегию мониторинга и логирования событий, которая поможет выявить подозрительную активность.

Задание 6: Анализ инцидента

Описание задачи: Предположим, что ваша система была атакована. Вам нужно провести анализ инцидента, чтобы понять, какие шаги предпринял злоумышленник и как можно предотвратить подобные атаки в будущем.

Задание:

- На основании предоставленных логов и другой доступной информации восстановите хронологию атаки.
- Определите слабые места в системе, которые позволили злоумышленнику проникнуть внутрь.
- Сформулируйте рекомендации по улучшению безопасности системы.

Задание 7: Разработка стратегии защиты

Описание задачи: Разработайте общую стратегию защиты информационной системы, основываясь на знаниях о жизненном цикле атаки и методах противодействия.

Задание:

- Составьте список мер, направленных на защиту системы на каждом этапе жизненного цикла атаки.
- Объясните, почему выбранные меры являются эффективными и как они помогают снизить риск успешных атак.
- Оцените затраты на реализацию предложенных мер и сравните их с возможными потерями от успешных атак.

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