Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Основы управления информационной безопасностью

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2025

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности (ИБ), управлять процессом их реализации на объекте защиты.

ПК-3. Способен проводить анализ уязвимостей внедряемой системы защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-10.1 Понимает принципы формирования политики информационной безопасности в соответствии с нормативными требованиями.

ИОПК-10.2 Умеет организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности на защищаемом объекте.

ИОПК-10.3 Демонстрирует навыки формирования и реализации политики информационной безопасности на защищаемом объекте.

ИПК-3.1. Проводит анализ уязвимости средств системы защиты информации.

ИПК-3.2. Устраняет выявленные уязвимости системы защиты информации.

ИПК-3.3. Разрабатывает предложения по совершенствованию системы управления защитой информации.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– контрольные задания.

Текущий контроль по дисциплине проводится путем контроля посещаемости и проверки контрольных заданий. При оценивании необходимо продемонстрировать достижение всех запланированных индикаторов достижения компетенций.

Примерный перечень типовых контрольных заданий:

Тема «Стандарт ГОСТ ИСО/МЭК 27000»
Задание 1. Стандарт ГОСТ ИСО/МЭК 27000. Термины и определения.
Задание 2. Системы менеджмента информационной безопасности. Требования
Задание 3. Свод норм и правил менеджмента информационной безопасности.
Задание 4. Руководство по реализации системы менеджмента ИБ.
Задание 5. Менеджмент информационной безопасности. Измерения.
Задание 6. Руководства по аудиту систем менеджмента информационной безопасности.

Тема «Правовые основы построения системы защиты информации и оценка рисков».
Задание 1. Структура государственной системы защиты информации.
Задание 2. Идентификация рисков работы со сторонними организациями.
Задание 3. Основные документы, определяющие политику РФ в сфере ИБ.
Задание 4. Методика оценки рисков информационной безопасности.

Тема «Мониторинг безопасности и реагирование на инциденты»
Задание 1. Цели аудита состояния информационной безопасности.
Задание 2. Этапы процесса реагирования на инциденты.
Задание 3 Этапы проведения аудита информационной безопасности.
Задание 4. Процедуры идентификация нападающего в процессе реагирования на инцидент

Тема «Разработка политики безопасности предприятия» (проектное задание).
Выполняется группой студентов из 3-4 человек. Требуется выбрать одно из предприятий: государственное образовательное учреждение, адвокатская контора, предприятие в сфере электронной коммерции, предприятие связи, поликлиника, аутсорсинговая компания, страховая компания, банк. После составить модель предприятия - описать хозяйственную деятельности, положения на рынке, конкуренты, контрагенты, клиенты, перечень предоставляемых услуг. Далее построить модель угроз и нарушителя информационной безопасности, оценить уровень защищенности выбранного предприятия, разработать политику безопасности верхнего уровня, политику безопасности среднего уровня по направлениям (менеджмент активов, физическая безопасность, безопасность финансовой деятельности, управление доступом, менеджмент непрерывности бизнеса, менеджмент инцидентов), разработать должностные инструкции для специалиста-пользователя информационными ресурсами предприятия.

Выполнение контрольного задания оценивается в 100 баллов:

0-20 Студент не разбирается в проблематике, не знает методов/способов решения задач предметной области, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в проблематике, плохо знает методы/способы решения задач предметной области, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в проблематике, использует методы/способы решения задач предметной области при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками.

61-80 Студент в целом уверенно разбирается в проблематике, знает и использует методы/способы решения задач предметной области практически самостоятельно, отвечает на вопросы с замечаниями.

81-100 Студент отлично разбирается в проблематике, знает и использует методы/способы решения задач предметной области, отвечает на вопросы уверенно.

Допуском до зачета является выполнение 80% контрольных заданий с оценкой за каждую не менее 50 баллов.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Промежуточная аттестация осуществляется на основе выполнения студентом контрольных заданий и по результатам собеседования с использованием перечня контрольных вопросов по курсу. Вопросы выявляют все запланированные индикаторы достижения компетенций.

Примерный перечень контрольных вопросов по дисциплине:

1. Задачи менеджмента в сфере информационной безопасности.
2. Понятие безопасной информационной инфраструктуры и ее составляющие.
3. Уровни организационной работы в сфере информационной безопасности.
4. Особенности организационной деятельности государства в сфере ИБ.
5. Основополагающие документы, определяющие политику РФ в сфере ИБ.
6. Структура государственной системы защиты информации в РФ.
7. Предпосылки развития менеджмента в сфере ИБ на уровне предприятий.

8. Структура организационной деятельности по обеспечению ИБ предприятия.
9. Структура политики ИБ и процесс ее разработки.
10. Содержание политики ИБ предприятия верхнего и среднего уровня.
11. Задачи департамента информационной безопасности предприятия.
12. Организационная структура департамента ИБ.
13. Направления организационной работы в области ИБ, связанной с персоналом.
14. Меры по организации физической безопасности.
15. Организационные аспекты ИБ при взаимодействии со сторонними организациями.
16. Мероприятия по обеспечению безопасности использования мобильной техники.
17. Этапы процесса реагирования на инциденты
18. Реагирования на инциденты – этап обнаружение нападения.
19. Реагирование на инциденты – локализация и устранение последствий нападения.
20. Реагирование на инциденты – этап идентификации нападающего.
21. Реагирование на инциденты – этап оценки и анализа процесса нападения.
22. Организация и цели аудита состояния ИБ безопасности предприятия.
23. Этапы и стадии аудита информационной безопасности предприятия.
24. Содержание отчета о результатах аудита состояния ИБ предприятия.
25. Основные понятия и определения управления информационными рисками.
26. Процесс управления рисками. Этапы обработки рисков.
27. Определение критерия оценки и приемлемости риска.
28. Методы оценки рисков. Шкалы вероятности угроз и уязвимостей.
29. Стандарты в области управления информационными рисками.

Результаты зачета определяются оценками «зачтено», «не зачтено»:

оценка «зачтено» ставится, если студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении большинства (>80%) контрольных заданий.

оценка «не зачтено» ставится, если студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины и/или не показал требуемые умения и навыки при выполнении контрольных заданий (выполнено менее 80% заданий).

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Примерный перечень контрольных вопросов для проверки остаточных знаний:

1. Задачи менеджмента в сфере информационной безопасности.
2. Понятие безопасной информационной инфраструктуры и ее составляющие.
3. Уровни организационной работы в сфере информационной безопасности.
4. Основополагающие документы, определяющие политику РФ в сфере ИБ.
5. Структура государственной системы защиты информации в РФ.
6. Структура организационной деятельности по обеспечению ИБ предприятия.
7. Структура политики ИБ и процесс ее разработки.
8. Содержание политики ИБ предприятия верхнего и среднего уровня.
9. Задачи департамента информационной безопасности предприятия.
10. Направления организационной работы в области ИБ, связанной с персоналом.
11. Меры по организации физической безопасности.
12. Этапы процесса реагирования на инциденты
13. Организация и цели аудита состояния ИБ безопасности предприятия.
14. Этапы и стадии аудита ИБ предприятия.
15. Основные понятия и определения управления информационными рисками.
16. Процесс управления рисками. Этапы обработки рисков.

17. Стандарты в области управления информационными рисками

Информация о разработчиках

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ.