Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___” _____г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

Расследование инцидентов информационной безопасности
Образовательная программа: 10.04.01 Информационная безопасность, магистерская программа: Методы и средства обеспечения технической защиты информации

Новосибирск 2023

1. Методика оценки этапов формирования компетенций по дисциплине

Уровни сформированности компетенции проверяется при проведении мероприятий текущей аттестации (контроля) в процессе изучения дисциплины.

В 3 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Промежуточная аттестация по **дисциплине** проводится в 3 семестре - в форме зачета, который направлен на оценку сформированности компетенций ПК-3.В/НИ и соотнесенных с ними индикаторов.

Зачет проводится в форме письменного тестирования с использованием электронной информационно-образовательной среда НГТУ (http:// www.nstu.ru/sveden/eos).

Общие правила выставления оценок текущей и промежуточной аттестации по дисциплинеопределяются балльно-рейтинговой системой, приведенной в рабочей программе дисциплины.

На основании приведенных далее критериев можно оценить уровни сформированностикомпетенции ПК-3.В/НИ, закрепленных за дисциплиной.

2. Общая характеристика уровней освоения компетенций

Продвинутый. Теоретическое содержание курса освоено полностью. Студент демонстрирует систематическое и глубокое понимание учебного материала и способность к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности. Сформированы необходимые навыки практической работы. Все учебные задания, предусмотренные программой обучения, выполнены качественно, без замечаний. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов, входящим в диапазон продвинутого уровня.

Базовый. Теоретическое содержание курса освоено в объеме, необходимом для дальнейшей учебы и профессиональной деятельности. Навыки практической работы сформированы на базовом уровне. Все предусмотренные программой обучения учебные задания выполнены с небольшими погрешностями. Уровень
сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов в пределах базового уровня.

Пороговый. Теоретическое содержание курса освоено, необходимом для дальнейшей учебы и профессиональной деятельности. Некоторые практические навыки работы с сформированы с незначительными пробелами. Учебные задания, предусмотренные программой обучения, выполнялись с ошибками, исправленными под руководством преподавателя. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числом баллов в пределах порогового уровня.

Ниже порогового. Теоретическое содержание курса освоено фрагментарно. Необходимые навыки практической работы сформированы минимально. Большинство учебных заданий, предусмотренных программой обучения, не выполнены. Уровень сформированности компетенций и соотнесенных с ними индикаторов, закрепленных за дисциплиной, оценен числомбаллов, входящих в диапазон ниже порогового уровня.

Паспорт зачета

по дисциплине «Расследование инцидентов информационной безопасности», 3 семестр

1. **Методика оценки** Зачет проводится в форме письменного тестирования с использованием электронной информационно-образовательной среда НГТУ (http:// www.nstu.ru/sveden/eos).

Тестовые задания охватывают все содержание «Расследование инцидентов информационной безопасности» (модуля).

Тест состоит из вопросов различного вида и позволяет проверить результаты обучения по дисциплине (модулю), соотнесенные с установленными в программе индикаторами достижения компетенций.

2. **Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций**

Выполнение теста засчитывается на **продвинутом** уровне, если студент правильно ответил на все вопросы теста, знает определения всех понятий, продемонстрировал способность безошибочно устанавливать последовательность и соответствие между процессами и явлениями, выявлять проблемы, предлагать механизмы их решения, представляет количественные и качественные характеристики определенных процессов. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 18 до 20 баллов.*

Выполнение теста засчитывается на **базовом** уровне, если студент правильно ответил на ⅔ вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, правильно характеризует процессы, явления. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 15 до 17 баллов.*

Выполнение теста засчитывается на **пороговом** уровне, если студент правильно ответил от ½ до ⅔ вопросов теста, знает определения основных понятий, продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, допускает непринципиальные ошибки, например, вычислительные. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от 10 до 14 баллов.*

Выполнение теста считается **неудовлетворительным**, если студент правильно ответил менее чем на половину вопросов теста, не знает определений понятий, не продемонстрировал способность устанавливать последовательность и соответствие между процессами и явлениями, допускает принципиальные ошибки. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее 10 баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям составляет от 10 до 20 баллов включительно. Сумма менее 10 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Фонд оценочных материалов (вопросы теста) для оценки уровня сформированности компетенций и соотнесенных с ними индикаторов

Формируемая компетенции	Индикаторы компетенции
ПК-3.В/НИ Способен проводить расследования компьютерных преступлений	1. умеет анализировать данные, связанные с компьютерным преступлением 2. знает инструменты для проведения расследования киберинцидентов

Вопрос 1. Что такое (Indicator of Compromise) IoC?

- **Наблюдаемый в сети или на устройстве объект или активность, которая в большей долей вероятности указывает на компрометацию системы ✓**
- Инцидент информационной безопасности
- Событие информационной безопасности

(один вариант)

Вопрос 2. Дополните

Преступлениями против конфиденциальности, целостности и доступности компьютерных данных и систем являются: несанкционированный доступ, незаконное получение данных, незаконный перехват, искажение информации, нарушение работоспособности ____ _____

Ответ:

Решение:

Информационной системы

Вопрос 3. Дополните. Суть этапа сдерживания в процессе Incident Response - это выполнение оперативных мероприятий по изоляции затронутых узлов от остальной инфраструктуры, сбор _____ с затронутых в ходе инцидента машин, сбор данных для более точного понимания картины инцидента.

Ответ:

Решение:

артефактов

Вопрос 4. Событие ИБ - это…

- **идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики ИБ или аварию защитных мер (средств), а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью ✓**
- идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики ИБ или аварию защитных мер (средств)
- нарушение политики ИБ или авария защитных мер (средств) системы

(один вариант)

Вопрос 5. Деятельность по раскрытию преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств это _____
Ответ:

Решение:
форензика

Вопрос 6. Дополните. Суть этапа нейтрализации в процессе Incident Response - анализ собранных артефактов, поиск индикаторов _____, удаление вредоносного содержимого, блокирование вредоносных ресурсов, выявление причины инцидента, модификация системы ЗИ.
Ответ:

Решение:
компрометации

Вопрос 7. Контроль за реализацией единых правил эксплуатации средств обнаружения компьютерных атак на информационные ресурсы входит в деятельность:

- **обнаружения, регистрации компьютерных атак ✓**
- анализа событий безопасности
- регистрации инцидентов

(один вариант)

Вопрос 8. Дополните
К комбинированным преступлениям относятся: использование сети Интернет в террористических целях, кибервойны, _____, отмывание денег с использованием компьютерных технологий
Ответ:

Решение:
фишинг

Вопрос 9. Компьютерная атака - это

- **Злонамеренное воздействие нарушителей на объекты инфраструктуры организации ✓**
- Нарушения свойств безопасности информации
- Реализация злоумышленником контролируемой зоны

(один вариант)

Вопрос 10. В соответствии с каким кодексом РФ выбирается наказание за разработку ВПО или модулей ВПО
Ответ:

Решение:
уголовным

Вопрос 11. Компьютерный инцидент - это

- **Факт нарушения или прекращения функционирования объекта организации, нарушения свойств безопасности информации ✓**
- Злонамеренное воздействие нарушителей на объекты инфраструктуры организации
- Реализация злоумышленником контролируемой зоны

(один вариант)

Вопрос 12. К какой линии SOC относятся специалисты по расследованию компьютерных инцидентов?
Ответ*:*

Решение:
второй

Вопрос 13. Что такое реагирование на компьютерные атаки и инциденты?

- **Оперативные действия по нейтрализации последствий КА и КИ и восстановление работоспособности ИС ✓**
- Действия, направленные на выявление предпосылок появления КИ
- Процесс выявления инцидентов информационной безопасности

(один вариант)

Вопрос 14. Что необходимо обязательно предпринимать при анализе жестких дисков и поиске в них индикаторов компрометации?
Ответ*:*

Решение:
Блокировку функции записи

Вопрос 15. Что такое расследование компьютерных инцидентов?

- **Действия, направленные на выявление предпосылок появления КИ и выявление методов, техник и тактик реализации КА ✓**
- Оперативные действия по нейтрализации последствий КА и КИ
- Процесс выявления инцидентов информационной безопасности

(один вариант)

Вопрос 16. Опишите действия при возникновении инцидента ИБ: отказ в обслуживании (DoS, DDoS)
Ответ*:*

Решение:
Блокирование IP

Вопрос 17. Опишите суть этапа восстановления в процессе Incident Response.
Ответ:

Решение:
восстановление функционирования системы

Вопрос 18. Дополните
Этап применения полученного опыта в процессе Incident Response заключается в совершенствовании системы защиты информации, анализе эффективности плана _____, выявлении ошибок, соблюдении сроков реагирования и внесения изменений в плейбуки с учётом полученного опыта
Ответ:

Решение:
реагирования

Вопрос 19. Какой первый этап реагирования на компьютерный инцидент типа «Заражение ВПО»?
Ответ:

Решение:
Отключение устройства от ЛВС

Вопрос 20. Назовите главный процесс этапа восстановления в Incident Response.
Ответ:

Решение:
Восстановление данных из бэкапов

Вопрос 21. Дополните
Threat Intelligence (данные о киберугрозах) – это информация об актуальных угрозах и группировках киберпреступников, которая позволяет организациям изучить цели, _____ и инструменты злоумышленников и выстроить эффективную стратегию защиты от атак.
Ответ:

Решение:
тактики

Вопрос 22. Дополните.
Резервное копирование данных необходимо для быстрого восстановления системы или разворачивания копии системы с минимальными задержками для бизнеса и минимальными потерями данных. Резервный фонд _____ необходим для оперативной замены скомпрометированного или вышедшего из строя оборудования.
Ответ:

Решение:
оборудования

Вопрос 23. С какой целью происходит анализ инцидентов ИБ.
Ответ:

Решение:
С целью выявления вектора атаки

Вопрос 24. Кто занимается обнаружением инцидентов ИБ?
Ответ:

Решение: аналитики SOC

Вопрос 25. Какое обучение персонала группы реагирования на инциденты ИБ необходимо проводить?
Ответ:

Решение:
периодические тренировки

Вопрос 26. Дополните.
Штатные сотрудники организации должны периодически проходить обучение по информационной безопасности для повышения _____ о тех угрозах ИБ, с которыми они могут столкнуться при выполнении своих должностных обязанностей. Целью проведения обучения персонала является донесение до сотрудников способов выявления компрометации ресурсов и правила оповещения ответственных сотрудников о произошедшем инциденте.
Ответ:

Решение:
осведомленности

Вопрос 27. Дополните.
Группа реагирования на инциденты ИБ предназначена для выполнения оперативных действий для реагирования на инцидент ИБ, для сбора _____ и индикаторов компрометации для расследования компьютерных инцидентов. Структурно группа реагирования состоит из руководителя, который несет административную и стратегическую функцию, и из профильных ИТ и ИБ специалистов, которые непосредственно реализуют действия по реагированию и расследованию инцидентов ИБ в области своих компетенций.
Ответ:

Решение:
артефактов

Вопрос 28. В чем заключается смысл этапа сдерживания в Incident Response?
Ответ:

Решение:
Локализация инцидента

Вопрос 29. Опишите действия при возникновении инцидента ИБ типа «сбор информации»
Ответ:

Решение:
Блокирование IP

Вопрос 30. Опишите действия при возникновении инцидента ИБ типа «заражение ВПО»
Ответ:
Решение:
Антивирусная проверка

Паспорт
расчетно-графического задания (работы)

по дисциплине «Расследование инцидентов информационной безопасности», 3 семестр

1. Методика оценки

Выполнение расчетно-графического задания (работы) (далее - РГЗ(Р)) является формой текущей аттестации (контроля) по дисциплине, предусмотренной учебным планом. Цель РГЗ(Р): студенты должны освоить и научиться программной реализации принципов, методов и алгоритмов решения основных и вспомогательных задач, получить навыки использования теоретических знаний для решения практических задач.

Обязательным элементом РГЗ(Р) являются разработка концепцию информационной безопасности компании.

Номер задания соответствует последней цифре (цифрам) в номере зачетной книжки (студенческого билета).

РГЗ(Р) выполняется индивидуально.

Количество заданий достаточно для обеспечения, каждого обучающегося индивидуальным заданием РГЗ(Р).

Замена задания РГЗ(Р) осуществляется по согласованию с преподавателем из числа резервных (не занятых) заданий.

Перед выполнением задания студент должен ознакомиться с рядом отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799).

Преподаватель осуществляет руководство по выполнению задания, оказывает консультационную помощь и принимает отчет по РГЗ(Р).

По результатам выполнения РГЗ(Р) выполняется отчет, который состоит из следующих частей:

1) Титульный лист
2) Содержание
3) Задание
4) Концепция ИБ заданного предприятия по плану, приведенному в задании

Требования к оформлению:

Объем РГЗ(З) до 20 страниц машинописного текста формата А4. Шрифт Times New Roman, 12. Формулы набираются в редакторе Math Type. Размещение сканированных формул не допускается. Нумерация страниц сквозная, в нижней части листа по центру арабскими цифрами. Работа должна быть отредактирована, не содержать орфографических, синтаксических и стилевых ошибок.

Отчет в установленные сроки сдается на кафедру для проверки. Преподаватель оценивает качество работы, отмечает положительные стороны и недостатки работы и определяет, допускается ли она к защите. При необходимости преподаватель возвращает РГЗ(Р) студенту для доработки и устанавливает сроки повторного предоставления для проверки. До защиты работы студентом должны быть сделаны необходимые исправления и дополнения по всем замечаниям преподавателя.

При положительном результате оценивания РГЗ(Р) студент еѐ распечатывает, передает на кафедру и защищает до сессии в назначенное преподавателем время.

Защита РГЗ(Р) состоит в индивидуальном устном собеседовании студента с преподавателем. В процессе защиты выявляется уровень знаний студента, степень его самостоятельности при выполнении работы. По результатам защиты студенту выставляется оценка в соответствии с критериями, приведенными в п. 2 настоящего Паспорта.

2. Уровни сформированности компетенций и критерии оценки

РГЗ(Р) считается выполненной **на продвинутом** уровне, если все необходимые расчеты произведены самостоятельно и без ошибок; все разделы РГЗ(Р) выполнены правильно и в полном объеме; работа оформлена в соответствии с требованиями; сдана преподавателю в указанные сроки и не возвращалась для доработки; даны полные и развернутые выводы и рекомендации; на защите студентом даны уверенные и аргументированные ответы, что свидетельствует об уровне сформированности компетенций и соотнесенных с ними индикаторов на продвинутом уровне. Оценка составляет *от 17 до 20 баллов.*

РГЗ(Р) считается выполненной **на базовом** уровне, если все необходимые расчеты произведены самостоятельно и без существенных ошибок; все разделы РГЗ(Р) выполнены правильно, но есть замечания к полноте предоставления информации; работа оформлена в соответствии с требованиями; сдана преподавателю в указанные сроки и однократно возвращалась студенту для незначительной доработки; в заключении даны выводы и рекомендации; на защите студентом допущены непринципиальные ошибки, что свидетельствует об уровне сформированности компетенций и соотнесенных с ними индикаторов на базовом уровне. Оценка составляет *от 14 до 16 баллов.*

РГЗ(Р) считается выполненной **на пороговом** уровне, если все необходимые расчеты произведены самостоятельно, но с ошибками, часть из которых носит принципиальный характер; есть замечания к полноте предоставления информации; работа оформлена в соответствии с требованиями; сдана преподавателю, но неоднократно возвращалась студенту

для доработки; в заключении даны краткие выводы; защита РГЗ(Р) вызывает у студента серьезные затруднения, что свидетельствует об уровне сформированности компетенций и соотнесенных с ними индикаторов на пороговом уровне. Оценка составляет *от 10 до 13 баллов.*

РГЗ(Р) считается **не выполненной**, если расчеты произведены с серьезными ошибками; есть замечания к полноте предоставления информации и оформлению; РГЗ(Р) была сдана преподавателю, но неоднократно возвращалась студенту для доработки, что не привело к улучшению ее качества; РГЗ(Р) не допущена до защиты, что свидетельствует об не сформированности компетенций и соотнесенных с ними индикаторов. Оценка составляет *менее 10 баллов*.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

РГЗ(Р) как форма текущей аттестации (контроля) по дисциплине считается успешно выполненной, если сумма полученных баллов по всем его заданиям составляет от 10 до 20 баллов включительно.

4. Примерный перечень тем РГЗ(Р)

Разработать концепцию информационной безопасности компании (см. вариант):

Номер варианта	Организация
1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда
17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив

29	Диспетчерская служба такси
30	Железнодорожная касса

Концепция должна содержать следующие основные пункты (приведен примерный план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности 1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности 2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы.

3. Механизмы обеспечения информационной безопасности предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности предприятия.

3.4. Критерии и показатели информационной безопасности предприятия.

4. Мероприятия по реализации мер информационной безопасности предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности предприятия.

- Правовое обеспечение юридических отношений с работниками предприятия.
- Правовое обеспечение юридических отношений с партнерами предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности предприятия.

5. Программа создания системы информационной безопасности предприятия