МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

ЕСТЕСТВЕННОНАУЧНЫЙ ФАКУЛЬТЕТ
Кафедра «Информатика и ИТ»

«Утверждаю»
Декан естественнонаучного
факультета
_____ Лешукович А.И.
«_1_» Сентября___2026 г.
.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине (модулю)

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки – 10.03.01 «Информационная безопасность»
Профиль – Безопасность компьютерных систем
(по отрасли или в сфере профессиональной деятельности)
Форма подготовки - очная
Уровень подготовки – бакалавриат

ДУШАНБЕ 2026

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ

Код компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения	Вид оценочного знания
УК-2	**Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений**	**ИУК-2.1.** Формулирует в рамках поставленной цели совокупность взаимосвязанных задач, обеспечивающих ее достижение. **ИУК-2.2.** Определяет ресурсное обеспечение для достижения поставленной цели; **ИУК-2.3.** Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **ИУК-2.4.** Выполняет задачи в рамках своей ответственности в соответствии с запланированными результатами, при необходимости корректирует способы решения задач	Отчеты по практическим работам. Устный опрос. Презентация
ПК-3	**Способен проектировать информационные системы по видам обеспечения**	**ИПК-3.1.** Применяет элементы технологий проектирования информационных систем; осуществляет и обосновывает выбор проектных решений по видам обеспечения информационных систем **ИПК-3.2.** Участвует в проектировании экономических информационных систем или их частей (модулей)	Отчеты по практическим работам. Устный опрос. Презентация

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
(рефератов, письменных работ)

1. Понятие и сущность инцидентов информационной безопасности.
2. Классификация инцидентов информационной безопасности.
3. Причины и условия возникновения инцидентов информационной безопасности.
4. Жизненный цикл инцидента информационной безопасности.
5. Организация расследования инцидентов информационной безопасности.
6. Роль службы информационной безопасности в расследовании инцидентов.
7. Правовые основы расследования инцидентов информационной безопасности.
8. Нормативно-правовое регулирование расследования инцидентов ИБ.
9. Документирование инцидентов информационной безопасности.
10. Сбор, фиксация и хранение доказательств при расследовании инцидентов ИБ.
11. Логи и журналы событий как источник информации при расследовании.
12. Реагирование на инциденты информационной безопасности.
13. Внутренние инциденты информационной безопасности и их особенности.
14. Внешние инциденты информационной безопасности и методы противодействия.
15. Типовые ошибки при расследовании инцидентов информационной безопасности.
16. Ответственность за нарушения в сфере информационной безопасности.
17. Взаимодействие организации с правоохранительными органами при расследовании инцидентов ИБ.
18. Анализ последствий инцидентов информационной безопасности.
19. Меры по предупреждению повторных инцидентов информационной безопасности.
20. Значение расследования инцидентов ИБ для повышения уровня защищённости организации.

Критерии оценки выполнения самостоятельной работы.

В основу разработки балльно рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, равномерно расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

Студентам выставляются следующие баллы за выполнение задания к ПК:

- **оценка «отлично» (10 баллов):** контрольные тесты, а также самостоятельно выполненные семестровые задания, выполненные полностью и сданные в срок в соответствии с предъявляемыми требованиями;
- **оценка «хорошо» (8-9 баллов):** задание выполнено и в целом отвечает предъявляемым требованиям, но имеются отдельные замечания в его оформлении или сроке сдачи;
- **оценка «удовлетворительно» (6-7 баллов):** задание выполнено не до конца, отсутствуют ответы на отдельные вопросы, имеются отклонения в объеме, содержании, сроке выполнения;
- **оценка «неудовлетворительно» (5 и ниже):** отсутствует решение задачи, задание переписано (скачано) из других источников, не проявлена самостоятельность при его выполнении.

Текущий контроль осуществляется в ходе учебного процесса по результатам выполнения самостоятельной работы и контрольной работы.

Основными формами текущего контроля знаний являются:

- обсуждение вынесенных в планах практических занятий лекционного материала и контрольных вопросов;
- решение тестов и их обсуждение с точки зрения умения сформулировать выводы, вносить рекомендации и принимать адекватные управленческие решения;
- выполнение контрольной работы и обсуждение результатов;
- участие в дискуссиях в качестве участника и модератора групповой дискуссии по темам дисциплины;
- написание и презентация доклада;
- написание самостоятельной (контрольной) работы.

Для контроля усвоения данной дисциплины учебным планом предусмотрен экзамен. Общее количество баллов по дисциплине - 100 баллов. Распределение баллов на текущий и промежуточный контроль при освоении дисциплины, а также итоговой оценке представлено ниже.

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ КОНТРОЛЬНОЙ РАБОТЫ

по дисциплине

«Расследование инцидентов информационной безопасности»:

1. Понятие инцидента информационной безопасности.
2. Классификация инцидентов информационной безопасности.
3. Основные причины возникновения инцидентов ИБ.
4. Жизненный цикл инцидента информационной безопасности.
5. Роль расследования инцидентов в системе ИБ организации.
6. Организационные основы расследования инцидентов ИБ.
7. Правовые основы расследования инцидентов информационной безопасности.
8. Нормативные требования к фиксации инцидентов ИБ.
9. Роль службы информационной безопасности в расследовании инцидентов.
10. Участники процесса расследования инцидентов ИБ и их функции.
11. Документирование инцидентов информационной безопасности.
12. Сбор и анализ доказательств при расследовании инцидентов ИБ.
13. Логи и журналы событий как источник информации при расследовании.
14. Внутренние и внешние инциденты информационной безопасности.
15. Реагирование на инциденты информационной безопасности.

16. Типовые ошибки при расследовании инцидентов ИБ.
17. Ответственность за нарушения в сфере информационной безопасности.
18. Взаимодействие с правоохранительными органами при расследовании инцидентов ИБ.
19. Анализ последствий инцидентов информационной безопасности.
20. Значение расследования инцидентов ИБ для повышения уровня защищённости организации.

ЭКЗАМЕНАЦИОННЫЕ (КОНТРОЛЬНЫЕ) ВОПРОСЫ

@1. Инцидент информационной безопасности — это
$A) плановое обновление системы
$B) любое событие в ИС
$C) событие, нарушающее конфиденциальность, целостность или доступность информации
$D) отказ оборудования
$E) аудит ИБ
@2. Основная цель расследования инцидента ИБ
$A) наказание сотрудников
$B) восстановление системы
$C) установление причин и последствий инцидента
$D) отчётность
$E) проверка знаний персонала
@3. К этапам расследования инцидента ИБ относится
$A) обучение персонала
$B) фиксация и анализ инцидента
$C) внедрение ИС
$D) разработка ПО
$E) маркетинг
@4. Кто, как правило, отвечает за расследование инцидентов ИБ в организации
$A) бухгалтер
$B) системный администратор
$C) служба информационной безопасности
$D) отдел кадров
$E) пользователи
@5. Документирование инцидента ИБ необходимо для
$A) рекламы
$B) анализа и отчётности
$C) архивирования данных
$D) повышения зарплаты
$E) сокращения персонала
@6. К источникам информации при расследовании инцидента ИБ относятся
$A) рекламные материалы
$B) служебные записки
$C) журналы событий и логи
$D) отчёты о продажах
$E) договоры поставки
@7. Реагирование на инцидент ИБ должно быть
$A) спонтанным
$B) несистемным
$C) регламентированным
$D) устным
$E) необязательным
@8. Внутренний инцидент ИБ — это
$A) атака из интернета
$B) стихийное бедствие
$C) нарушение со стороны сотрудников
$D) отказ электросети
$E) обновление ОС
@9. Внешний инцидент ИБ связан с
$A) действиями персонала

$B) ошибками документации
$C) действиями внешних нарушителей
$D) аудитом
$E) инструктажем
@10. Основная ошибка при расследовании инцидентов ИБ
$A) фиксация данных
$B) анализ логов
$C) отсутствие документирования
$D) соблюдение регламентов
$E) взаимодействие с руководством
@11. Логи в расследовании инцидентов используются для
$A) резервного копирования
$B) восстановления ПО
$C) анализа действий пользователей и систем
$D) установки антивируса
$E) контроля зарплаты
@12. Инциденты ИБ могут привести к
$A) росту прибыли
$B) утечке информации
$C) повышению производительности
$D) автоматизации процессов
$E) модернизации сети
@13. Правовые меры при расследовании инцидентов ИБ включают
$A) техническое обслуживание
$B) дисциплинарную ответственность
$C) обновление ПО
$D) резервное копирование
$E) настройку сети
@14. Сбор доказательств при расследовании инцидентов ИБ должен быть
$A) произвольным
$B) неформальным
$C) корректным и законным
$D) устным
$E) необязательным
@15. Реагирование на инциденты ИБ направлено на
$A) увольнение сотрудников
$B) минимизацию ущерба
$C) расширение сети
$D) тестирование оборудования
$E) маркетинг
@16. Анализ инцидентов ИБ позволяет
$A) игнорировать угрозы
$B) выявить слабые места системы защиты
$C) сократить персонал
$D) отменить политику ИБ
$E) упростить отчётность
@17. Взаимодействие с правоохранительными органами требуется при
$A) незначительных сбоях
$B) технических ошибках
$C) признаках преступления
$D) плановом аудите
$E) обновлении регламентов
@18. Регламенты расследования инцидентов ИБ относятся к
$A) техническим мерам
$B) организационным мерам
$C) физическим мерам
$D) программным мерам
$E) аппаратным мерам
@19. Инциденты ИБ должны

$A) игнорироваться
$B) скрываться
$C) фиксироваться и анализироваться
$D) рассматриваться устно
$E) передаваться только ИТ-отделу
@20. Основная цель анализа последствий инцидентов ИБ
$A) поиск виновных
$B) улучшение системы защиты
$C) сокращение бюджета
$D) замена персонала
$E) закрытие проекта

Итоговые оценки студентов

Буквенное обозначение итоговых оценок студентов и их цифровые эквиваленты:

Буквенная оценка	**Цифра**	**Общий балл**	**Традиционная оценка**
A	4	95≤A≤100	отлично
A-	3,67	90≤A-<95	
B+	3,33	85≤B+<90	хорошо
B	3	80≤B<85	
B-	2,67	75≤B-<80	
C+	2,33	70≤C+<75	удовлетворительно
C	2	65≤C<70	
C-	1,67	60≤C-<65	
D+	1,33	55≤D+<60	
D	1	50≤D<55	
Fx	0	45≤Fx<50	неудовлетворительно
F	0	0<F<45	

Критерии выведения итоговой оценки промежуточной аттестации:

«Отлично» - средняя оценка ≥ 3,67.
«Хорошо» - средняя оценка ≥ 2,67 и ≤ 3,33.
«Удовлетворительно» - средняя оценка ≥ 1,0 и ≤ 2,33.
«Неудовлетворительно» - средняя оценка < 0.