Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
Директор института

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 68 3f 3c 2b 51 50 37 ea 75 a9 e9 15 1f 86 78 7f
Владелец: Мнацаканян Альберт Гургенович
Действителен: с 29.08.2024 по 22.11.2025

Фонд оценочных средств
(приложение к рабочей программе дисциплины)
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

основной профессиональной образовательной программы магистратуры
по направлению подготовки
38.04.01 ЭКОНОМИКА
профиль программы
«КОРПОРАТИВНАЯ ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ»

ИНСТИТУТ отраслевой экономики и управления
РАЗРАБОТЧИК кафедра экономической безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

1.1 Результаты освоения дисциплины

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными компетенциями

Код и наименование компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями
ПК-2: Способен осуществлять методическое обеспечение, взаимодействие с заинтересованными сторонами, координацию и консультирование по вопросам управления рисками в целях укрепления корпоративной экономической безопасности	Информационная безопасность	**Знать:** - теоретико-методологические основы обеспечения информационной безопасности; - основные меры, направленные на обеспечение информационной безопасности на различных уровнях деятельности современного предприятия; - роль информационной составляющей в обеспечении безопасности современного бизнеса, перспективные направления развития технологий обеспечения информационной безопасности. **Уметь:** - выявлять риски в сфере информационной безопасности организации, разрабатывать направления по их нейтрализации в целях обеспечения экономической безопасности; - анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню информационной безопасности; - применять отдельные приемы и методы управления информационной безопасности для разработки реальных методов формирования защиты информационной инфраструктуры в целях укрепления экономической безопасности организаций. **Владеть:** - способностью применять на практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации информационной безопасности; - способностью разрабатывать концепцию, программу, политику информационной безопасности предприятия; - использовать современные инструментальные

		средства анализа рисков и разработки политики информационной безопасности; - навыками работы с современными информационными системами и средствами обеспечения их безопасности/

1.2 Промежуточная аттестация по дисциплине проводится в форме зачета с оценкой (дифференцированного зачета), который выставляется по результатам прохождения всех видов текущего контроля успеваемости. При необходимости тестовые задания закрытого и открытого типов могут быть использованы для проведения текущей аттестации.

1.3 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов;

- типовые задания по контрольной работе.

К оценочным средствам для промежуточной аттестации относятся:

- типовые задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов.

1.4 Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (табл. 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую	Может найти необходимую информацию в	Может найти, интерпретироват ь и	Может найти, систематизироват ь необходимую

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
	информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	рамках поставленной задачи	систематизировать необходимую информацию в рамках поставленной задачи	информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

1.5 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41-100% правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» - менее 40 %

правильных ответов; оценка «удовлетворительно» - от 41 до 60 % правильных ответов; оценка «хорошо» - от 61 до 80% правильных ответов; оценка «отлично» - от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Компетенции:
ПК-2:
Способен осуществлять методическое обеспечение, взаимодействие с заинтересованными сторонами, координацию и консультирование по вопросам управления рисками в целях укрепления корпоративной экономической безопасности

Тестовые задания закрытого типа:

1. Информационная безопасность представляет собой:

1) Защиту информации от несанкционированного доступа, изменения, уничтожения, разглашения или иного неправомерного использования;
2) Защиту информации от физических воздействий, таких как пожар или наводнение;
3) Защиту информации от вирусов и вредоносных программ;
4) Защиту информации от утечки в средства массовой информации.

2. Наиболее эффективным для защиты от несанкционированного доступа к информации является метод:

1) Установки паролей;
2) Использования антивирусных программ;
3) Шифрования данных;
4) Обучения сотрудников правилам информационной безопасности.

3. К организационным мерам обеспечения информационной безопасности относятся:

1) Установка антивирусных программ;
2) Разработка политики безопасности;
3) Внедрение системы контроля доступа;
4) Проведение регулярных аудитов информационной безопасности.

4. "Информационная система" представляет собой:

1) Совокупность взаимосвязанных элементов, предназначенных для обработки информации;
2) Программу, установленную на компьютере;
3) Совокупность данных, хранящихся на компьютере;
4) Комплекс устройств, обеспечивающих работу информационных технологий.

5. Для защиты от социальной инженерии могут быть использованы следующие меры:

1) Обучение сотрудников правилам информационной безопасности;

2) Установка антивирусных программ;
3) Внедрение системы контроля доступа;
4) Проведение регулярных проверок на соответствие политики безопасности.

6. К утечке конфиденциальной информации может привести:
1) Несанкционированный доступ к информации;
2) Отправка конфиденциальных данных по незащищенным каналам связи;
3) Потеря носителей информации;
4) Неправильное использование паролей.

7. Установите последовательность действий при проведении аудита информационной безопасности:
1) Анализ полученных результатов и выработка рекомендаций;
2) Планирование и определение целей аудита;
3) Сбор информации о системе безопасности;
4) Тестирование средств защиты и оценка рисков.

Ответ: 2, 3, 4, 1

8. Установите соответствие между типами атак с их описаниями:

1	DDoS-атака	А	Атака, направленная на перегрузку сервера запросами, в результате чего он становится недоступным для пользователей.
2	SQL-инъекция	Б	Несанкционированный доступ к аккаунту с помощью подбора пароля, использования брутфорса или кражи пароля.
3	Фишинг	В	Мошенничество, в котором злоумышленники пытаются получить доступ к конфиденциальной информации пользователей, например, паролям и номерам кредитных карт, под видом легитимных организаций.
4		Г	Атака, направленная на получение доступа к базе данных путем внедрения вредоносного кода в SQL-запросы.

Ответ: 1 – А; 2 – Г; 3 – В.

Тестовые задания открытого типа:

9. Обеспечение информационной безопасности - это комплекс мер, направленный на защиту информации от несанкционированного доступа, модификации, уничтожения или разглашения, а также на обеспечение ее целостности, доступности и _____.
Вставьте пропущенное слово

Ответ: конфиденциальности

10. Слабая точка в системе безопасности, которая может быть использована злоумышленником для получения несанкционированного доступа к данным или для нарушения работоспособности системы называется: _____

Ответ: уязвимостью (уязвимость*)

11. Вредоносное программное обеспечение (malware) - это вредоносная программа, которая распространяется по сети и _____ компьютеры, используя уязвимости в операционных системах или приложениях.

Вставьте пропущенное слово

Ответ: заражает

12. Асимметричное шифрование - это шифрование данных, при котором ключ шифрования и ключ дешифрования _____.

Вставьте пропущенное слово

Ответ: различны

13. Процесс проверки и подтверждения подлинности личности пользователя перед предоставлением ему доступа к системе называется: _____

Ответ: аутентификацией (аутентификация*)

14. Политикой безопасности называется _____, определяющих права доступа пользователей к ресурсам и информации.

Вставьте пропущенное словосочетание

Ответ: набор правил

15. Программное обеспечение, которое защищает компьютер от вирусов, червей, троянских коней и других вредоносных программ называется: _____

Ответ: антивирусным ПО (антивирусное ПО*)

16. Документ, описывающий политику организации в области информационной безопасности, включая цели, принципы, роли и ответственность называется политикой: _____

Ответ: информационной безопасности

17. Набор действий, направленный на снижение риска возникновения инцидентов информационной безопасности называется _____ рисками.

Вставьте пропущенное слово

Ответ: управление

18. Процесс изменения данных, направленный на то, чтобы сделать их нечитаемыми без соответствующего ключа называется: _____

Ответ: шифрованием (шифрование*)

19. Проверка целостности данных - это процесс проверки данных, чтобы убедиться в их целостности и _____.

Вставьте пропущенное слово

Ответ: подлинности

20. Документ, подтверждающий личность пользователя и право на доступ к ресурсам и информации называется: _____

Ответ: электронной подписью (электронная подпись*)

21. Системой контроля доступа является система, которая используется для контроля доступа к ресурсам и _____.

Вставьте пропущенное слово

Ответ: информации

22. Атака на уязвимость - это тип атаки, при котором злоумышленник пытается получить _____, используя уязвимости в программном обеспечении.

Вставьте пропущенное словосочетание

Ответ: доступ к системе

23. Системы обнаружения и предотвращения вторжений (IDS/IPS) - это программное обеспечение, которое обнаруживает и _____ вредоносное программное обеспечение.

Вставьте пропущенное слово

Ответ: блокирует

24. Анализ событий безопасности - это процесс анализа данных, позволяющий выявлять _____.

Вставьте пропущенное словосочетание

Ответ: подозрительную активность

25. Технология, позволяющая создавать безопасное соединение по сети интернет называется: _____

Ответ: VPN

26. Устройство или программное обеспечение, которое защищает сеть от несанкционированного доступа извне называется: _____

Ответ: брандмауэр (Firewall)

27. Процесс создания копий данных для восстановления в случае их потери называется резервное: _____

Ответ: копирование данных

28. Использование математических методов для шифрования и дешифрования данных называется: _____

Ответ: криптография

29. Возможность сбора, обработки и распространения непрерывного потока информации при воспрещении использования информации противником представляет собой: _____

Ответ: информационное превосходство

30. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных называется: _____

Ответ: защита информации

3 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ

3.1 Контрольная работа является одним из способов оценки результатов освоения дисциплины и направлена на самостоятельное решение конкретной задачи, сформулированной в задании на её выполнении.

Варианты заданий для контрольной работы принимается в соответствии с вариантами, приведенными в учебно-методическом пособии по изучению дисциплины.

3.2 Работу следует разбить на теоретическую и практические части. Теоретическая часть направлена на раскрытие двух вопросов.

Практическая часть предполагает использование MS EXCEL при проведении расчетов, связанных с парольной защитой и шифрованием.

Исходные данные по вариант представлены в УМПИДе.

3.3 Объем контрольной работы следует ограничить 15 страницами, оформление производится в соответствии с требованиями, принятыми в ИНОТЭКУ КГТУ.

Работу следует разбить на следующие структурные разделы:

- содержание;
- введение;
- теоретические вопросы;
- решение задач;
- заключение.

В конце работы должен быть приведен список использованных источников, состоящий не менее чем из 10 наименований.

Критерии оценивания контрольной работы представлен в таблице 2.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Информационная безопасность» представляет собой компонент основной профессиональной образовательной программы магистратуры по направлению подготовки 38.04.01 Экономика (профиль программы «Корпоративная экономическая безопасность»).

Преподаватель-разработчик – к.э.н. Р.А. Мнацаканян.

Фонд оценочных средств рассмотрен и одобрен на кафедре экономической безопасности.

Заведующий кафедрой _____ Т.Е. Степанова

Фонд оценочных средств рассмотрен и одобрен методической комиссией ИНОТЭКУ (протокол № 5 от 20.05.2024 г).

Фонд оценочных средств актуализирован, рассмотрен и одобрен методической комиссией ИНОТЭКУ (протокол № 8 от 28.08.2024 г).

Председатель методической комиссии _____ И.А. Крамаренко