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

УТВЕРЖДАЮ
И.о. директора института

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
4ae0684d0d529bb9d0248a5b51302ea1
Владелец: Гоконаев Мирослав Валерьевич
Действителен: с 02.08.2024 по 26.10.2025

Фонд оценочных средств
(приложение к рабочей программе практики)

УЧЕБНАЯ ПРАКТИКА – ОЗНАКОМИТЕЛЬНАЯ ПРАКТИКА

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ	Цифровых технологий
РАЗРАБОТЧИК	Кафедра информационной безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРАКТИКИ, ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

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

Код и наименование компетенции	Наименование практики	Результаты обучения/индикаторы, соотнесенные с установленными компетенциями
ПК-1: Способен разрабатывать проектные решения по защите информации в автоматизированных системах, обеспечивать их внедрение и сопровождение	Учебная практика – ознакомительная практика	*Знать:* 1. основные информационные технологии, используемые в автоматизированных системах. 2. основные угрозы безопасности информации и модели нарушителя в автоматизированных системах. 3. программно-аппаратные средства обеспечения защиты информации автоматизированных систем. 4. принципы формирования и реализации политики безопасности информации в автоматизированных системах. *Уметь:* 1. производить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности информации в автоматизированной системе. 2. выявлять уязвимости информационно-технологических ресурсов автоматизированных систем. 3. Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации. *Владеть:* 1. навыками проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах; 2. навыками анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите.

1.2 Промежуточная аттестация по практике проводится в форме 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 промежуточной аттестации.

К оценочным средствам для промежуточной аттестации, проводимой в форме дифференцированного зачета (зачет с оценкой), относятся:

- отчет по практике;

- тестовые задания закрытого и открытого типов.

1.3 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 информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
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

1.4 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

Компетенция ПК-1: Способен разрабатывать проектные решения по защите информации в автоматизированных системах, обеспечивать их внедрение и сопровождение

Тестовые задания открытого типа:

1. Умение осуществлять поиск, преобразование и передачу информации средствами информационно-коммуникационных технологий и выполнять различные социальные роли в группе и коллективе - ….

Эталонный ответ: личностные качества, включаемые в компетенции и подлежащие развитию.

2. Самореализация - это …

Эталонный ответ: осуществление индивидных и личностных возможностей посредством собственных усилий, а также содеятельности с другими людьми.

3. Государственная тайна –

Эталонный ответ: защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

4. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации называется …

Эталонный ответ: защищаемая информация.

5. Правовая защита – это …

Эталонный ответ: специальные законы и другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

6. Персональные данные –

Эталонный ответ: любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

7. Обобщенный параметр, учитывающий ценность ресурса, уровень угрозы и степень уязвимости, называется …

Эталонный ответ: уровнем риска.

8. Угроза информации – это …

Эталонный ответ: совокупность условий и факторов, которые потенциально могут нанести вред (ущерб) собственнику, владельцу путем раскрытия, модификации или разрушения информации либо отказа в обслуживании.

9. Мониторинг событий ИБ – это…

Эталонный ответ: процесс просмотра и анализа журналов зарегистрированных событий информационных систем, средств защиты информации и сетевых устройств Компании, проводимый с целью выявления инцидентов ИБ и их регистрации.

10. Уязвимость информации — это: …

Эталонный ответ: событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности, обрабатываемой в ней информации.

11. Несанкционированный доступ к информации – это: …

Эталонный ответ: доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств

12. В системе поблочного отображения адресов виртуальной памяти указываются:

Эталонный ответ: блок, в котором расположен этот элемент, и смещение элемента относительно начала блока

13. Правильный порядок задания права доступа в ОС Linux – это…

Эталонный ответ: владелец-группа-остальные

14. Тупиковая ситуация для процесса это – …..

Эталонный ответ: ситуация, когда процесс ожидает некоторого события, которое никогда не произойдет.

15. Целостность информации - это

Эталонный ответ: состояние информации, при котором она либо остается неизменной, либо изменения осуществляются только теми, кто имеет на это право.

16. Конфиденциальность информации - это

Эталонный ответ: состояние информации, при котором доступ к ней имеют только те, кто обладает соответствующими правами доступа.

17. Доступность информации (ресурсов информационной системы) - это

Эталонный ответ: состояние информации (ресурсов информационной системы), при котором обладающие необходимыми правами доступа могут их беспрепятственно реализовать.

18. Права доступа - это

Эталонный ответ: полномочия пользователя или сущности (например, программы или устройства) на обработку информации - чтение, запись, изменение, копирование, передачу, удаление.

19. Субъект доступа - это

Эталонный ответ: пользователь или сущность, которые выполняют обработку информации в соответствии с назначенными им правами доступа.

20. Объект доступа - это

Эталонный ответ: информация или ресурс информационной системы (например, файл или запись в базе данных), с которым взаимодействует субъект доступа в соответствии с назначенными ему правами доступа.

21. Актив (информационный актив) - это

Эталонный ответ: информация или ресурс информационной системы, имеющие ценность для организации, использующиеся для достижения целей организации, являющиеся объектами защиты и кибератаки с целью нарушения свойств безопасности.

22. Кибератака (компьютерная атака) - это

Эталонный ответ: целенаправленное вредоносное воздействие на актив для нарушения его нормального функционирования и/или для реализации угрозы ИБ обрабатываемой ресурсом информации.

23. Инцидент ИБ - это

Эталонный ответ: событие (или группа событий) ИБ, которые могут привести или уже привели к успешной кибератаке, нарушению работы информационного актива, нанесению ущерба интересам компании.

24. Событие ИБ - это

Эталонный ответ: зафиксированное изменение состояния информационного актива, которое может являться причиной инцидента ИБ.

Тестовые задания закрытого типа:

1. Укажите соответствие действий исполнителя при формировании основных документов по результатам исполнения работ на этапе внедрения системы защиты информации:

	Действие		**Документ**
1	Установка и настройка средств защиты информации	а	Акт установки средств защиты информации
2	Внедрение организационных мер, разработка организационно-распорядительных документов	б	Документы по регламентации правил по эксплуатации и вывода из эксплуатации системы защиты информации
3	Выявление и анализ	в	Протокол контроля уязвимостей программного обеспечения и технических средств
4	Испытания и опытная эксплуатация системы защиты информации уязвимостей	г	Протоколы контроля оценки эффективности средств и оценки защищенности информации

Ответ: 1а; 2б; 3в; 4г

2. Укажите последовательность действий исполнителя при проведении аттестации информационных систем по требованиям безопасности информации

1	а	Подача и рассмотрение заявки на аттестацию.
2	б	Предварительное ознакомление с аттестуемым объектом (при необходимости).
3	в	Разработка программы и методики аттестационных испытаний.
4	г	Проведение аттестационных испытаний объекта.
5	д	Оформление, регистрация и выдача аттестата соответствия.

Ответ: 1а; 2б; 3в; 4г; 5д

3. Укажите последовательность действий при создании системы защиты информации

1	а	Формирование требований к системе защиты информации (предпроектный этап).
2	б	Разработка системы защиты информации (этап проектирования).
3	в	Внедрение системы защиты информации (этап установки, настройки, испытаний).
4	г	Подтверждение соответствия системы защиты информации (этап оценки).

Ответ: 1а; 2б; 3в; 4г

4. К правовым методам, обеспечивающим информационную безопасность, относятся:

- разработка аппаратных средств обеспечения правовых данных;

- разработка и установка во всех компьютерных правовых сетях журналов учета действий;

- разработка и конкретизация правовых нормативных актов обеспечения безопасности.

5. Основными источниками угроз информационной безопасности являются все указанное в списке:

- хищение жестких дисков, подключение к сети, инсайдерство;

- перехват данных, хищение данных, изменение архитектуры системы;

- хищение данных, подкуп системных администраторов, нарушение регламента работы.

6. Виды информационной безопасности:

- персональная, корпоративная, государственная;

- клиентская, серверная, сетевая;

- локальная, глобальная, смешанная.

7. Цели информационной безопасности – своевременное обнаружение, предупреждение:

- несанкционированного доступа, воздействия в сети;

- инсайдерства в организации;

- чрезвычайных ситуаций.

8. Основные объекты информационной безопасности:

- компьютерные сети, базы данных;

- информационные системы, психологическое состояние пользователей;

- бизнес-ориентированные, коммерческие системы.

3 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/КУРСОВОЙ ПРОЕКТ, РАСЧЕТНО-ГРАФИЧЕСКУЮ РАБОТУ

В данном разделе по учебному плану типовые задания на контрольную работу, курсовую работу/курсовой проект, расчётно-графическую работу не предусмотрены.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по практике «Учебная практика – ознакомительная практика» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация Безопасность открытых информационных систем).

Преподаватель – разработчик – А.Г. Жестовский.

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29 августа 2024 г).

Председатель методической комиссии  О.С. Витренко