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 модуля)

«КИБЕРБЕЗОПАСНОСТЬ АСУТП»

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 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-1. Способен разрабатывать проектные решения по защите информации в автоматизированных системах, обеспечивать их внедрение и сопровождение	Кибербезопасность АСУТП	*Знать:* - нормативные правовые акты в области защиты информации в АСУТП; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации в КИИ и АСУТП; - порядок проектирования АС в защищенном исполнении; - национальные, межгосударственные и международные стандарты в области защиты информации АСУТП. *Уметь:* - выявлять уязвимости информационно-технологических ресурсов автоматизированных систем - определять класс защищенности автоматизированных систем и ее составных частей в КИИ, ГИС и АСУТП. *Владеть:* - навыками анализа характера обрабатываемой информации и определение перечня информации, подлежащей защите в АСУТП; - навыками разработки отчетных документов и разделов технических заданий в КИИ и АСУТП; - разрабатывать части проектной документации на системы защиты автоматизированных систем; - обоснования перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы в КИИ и АСУТП

1.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов.

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости. В отдельных случаях (при не прохождении всех видов текущего контроля) зачет может быть проведен в виде тестирования.

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
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, во-	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовле-

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
	из имеющихся у него сведений		влекает в исследование новые релевантные задаче данные	кает 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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Тестовые задания закрытого типа:

1. Из списка компонентов АСУТП (список: контроллер, датчик, драйверы, антивирусная программа), выберите тот компонент, который не входит в список компонентов АСУТП:

a) контроллеры

b) датчики

c) драйверы

d) **антивирусная программа**

Ответ: d) **антивирусная программа**

2. Укажите тип угроз, который не рассматривается в проблемной области кибербезопасности АСУТП:

a) компьютерные вирусы

b) физические атаки

c) социальная инженерия

d**) природные**

Ответ: d**) природные**

3. Укажите вид защиты, который не используется для защиты АСУТП от кибератак:

a) Шифрование данных

b) Регулярные обновления программного обеспечения

c) Мониторинг сетевой активности

d**) деперсонализация данных**

Ответ: d**) деперсонализация данных**

4. Стандарт используется для обеспечения безопасности в АСУТП – это:

a) ISO 27001

b) IEC 62443

c) NIST SP 800-53

d) PCI DSS

Ответ: b**) IEC 62443**

5. Укажите действие, которое относится к физической безопасности в АСУТП:
a) Установка антивирусного ПО

b) Ограничение доступа к серверным помещениям

c) Шифрование данных

d) Обучение сотрудников

Ответ: b) Ограничение доступа к серверным помещениям

6. Укажите тип атаки, при которой злоумышленник встраивается в штатную работу АСУТП:

a) DDoS-атака

b) Атака с использованием уязвимостей

c) Атака на физические компоненты

d) MITM

Ответ: d**) MITM**

7. Укажите средство, которое **НЕЛЬЗЯ** использовать для обнаружения сетевых вторжений в АСУТП – это:

a) IDS (Intrusion Detection System)

b) IPS (Intrusion Prevention System)

c) Система мониторинга логов

d) Система распределения прав доступа

Ответ: **d) Система распределения прав доступа**

8. Укажите предназначение файрволла АСУТП:

a) хранение данных

b) защита сети

c) аппаратное обеспечение контроля трафика

d) аппаратное обеспечение управления сетевыми процессами

Ответ: b) защита сети

Тестовые задания открытого типа:

9. Разновидность протокола Modbus, который совместим с TCP – это:

Ответ: ModbusTCP

10. Понятие «политика безопасности информации» подразумевает:

Ответ: набор правил и процедур для защиты информации.

11. Типы аудита АСУТП бывают следующие:

Ответ: активный аудит, пассивный аудит

12. Для защиты систем АСУТП от внешних угроз необходимо использовать:

Ответ: "межсетевые экраны".

13. В контексте автоматизированных систем управления технологическими процессами "киберугроза" — это:

Ответ: киберугроза — это потенциальное событие или действие, которое может привести к несанкционированному доступу, повреждению или уничтожению данных и **систем в автоматизированных системах управления технологическими процессами.**

14. Понятие "инцидент кибербезопасности" в контексте автоматизированных систем управления технологическими процессами подразумевает:

Ответ: любое событие, которое может угрожать конфиденциальности, целостности или доступности данных и систем в автоматизированных системах управления технологическими процессами.

15. В контексте кибербезопасности "социальная инженерия" — это:

Ответ: это метод манипуляции людьми с целью получения конфиденциальной информации или доступа к системам, основанный на доверии и психологических приемах.

16. Документ "План реагирования на инциденты" в контексте кибербезопасности содержит:

Ответ: процедуры и действия, которые необходимо предпринять в случае возникновения инцидента кибербезопасности с целью минимизации ущерба и восстановления нормальной работы систем

17. Укажите, какие нарушения в работе физической инфраструктуры могут вызвать атаки на АСУТП.

Ответ: сбои в работе оборудования критически важных систем

18. «Контрольные суммы» в системах АСУТП используются для:

Ответ: для обеспечения целостности данных в системах АСУТП.

19. Понятие "вредоносное ПО" в контексте кибербезопасности расшифровывается следующим образом:

Ответ: это программное обеспечение, разработанное с целью нарушения работы компьютеров или сетей, кражи данных, шпионажа или выполнения других вредоносных действий.

20. Системы ISMS для АСУТП используются для:

Ответ: для управления безопасностью информации в АСУТП

21. Тип документа, который содержит информацию о действиях, предпринимаемых в случае наступления инцидента безопасности в АСУТП, называется:

Ответ: план реагирования

22. Ресурсы ОС, позволяющие определить время начала атаки на АСУТП:

Ответ: журналы событий

23. Для защиты от утечек данных в системах АСУТП необходимо использовать:

Ответ: системы предотвращения утечек данных

24. Документ «Политика безопасности» содержит информацию о:

Ответ: политиках и процедурах, связанных с реагированием на инциденты

25. Укажите системы, которые используются для мониторинга безопасности АСУТП:

Ответ: SIEM, IDS, IPS

26. Тестирование на проникновение (пентест) играет важную роль в обеспечении безопасности АСУТП подразумевает:

Ответ: симуляцию атак на систему с целью проверки ее защиты и выявление слабых мест.

27. Стандарт, охватывающий безопасность протоколов в промышленных системах, – это:

Ответ: IEC 62443

28. Протокол MQTT используется для:

Ответ: передачи данных в реальном времени в АСУТП

29. Динамический анализ в области кибербезопасности используется в АСУТП для анализа:

Ответ: поведения программ во время инцидента

30. Действия, которые следует провести после вирусной атаки в АСУТП в отношении программного обеспечения, следующие:

Ответ: обновление антивирусного и пользовательского ПО

31. Подбор функций безопасности для компонентов критической инфраструктуры осуществляется по приказу ФСТЭ №_____

Ответ: 31.

Для фильтрации данных без внедрения в «разрыв» средств фильтрации использует_____

Ответ: SPAN-порт

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

Учебным планом не предусмотрены

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Кибербезопасность АСУТП» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация Безопасность открытых информационных систем).

Преподаватель-разработчик – В.В. Подтопельный

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

Председатель методической комиссии  О.С. Витренко