



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

УТВЕРЖДАЮ
И.о. директора института

Фонд оценочных средств
(приложение к рабочей программе практики)
«ТЕХНОЛОГИЧЕСКАЯ ПРАКТИКА»

основной профессиональной образовательной программы специалитета
по специальности
**10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ
СИСТЕМ**

Специализация
«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ
РАЗРАБОТЧИК

цифровых технологий
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
<p>ПК-1: Способен разрабатывать проектные решения по защите информации в автоматизированных системах, обеспечивать их внедрение и сопровождение</p>	<p>Технологическая практика</p>	<p>Результаты обучения (владения, умения и знания), соотнесенные с компетенциями</p> <p>Знания:</p> <ol style="list-style-type: none"> 1. современные информационные технологии и программные средства, классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей 2. основные нормативные правовые акты, стандарты оформления документации на различных стадиях жизненного цикла информационной системы 3. современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности 4. Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации <p>Умения:</p> <ol style="list-style-type: none"> 1. выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности 2. применять основные нормативные правовые акты, стандарты в области информационной безопасности и защиты информации 3. выбирать современные информационные технологии и программные средства, в том числе

		<p>отечественного производства при решении задач профессиональной деятельности</p> <p>4. Умеет классифицировать и оценивать угрозы информационной безопасности</p> <p>5. Способен разрабатывать проектные решения по защите информации в автоматизированных системах, обеспечивать их внедрение и сопровождение</p> <p>Навыки:</p> <p>1. применения технических и программных средств</p> <p>2. навыками по разработке, составлению документации на различных этапах жизненного цикла информационной системы</p> <p>3. понятиями, связанными с обеспечением информационной безопасности личности, общества и государства</p> <p>4. Владеет основными понятиями, связанные с обеспечением информационно безопасности, общества и государства; информационного противоборства, информационной войны и формами их проявления в современном мире</p> <p>5. Разработки проектных решений по защите информации в автоматизированных системах и обеспечения их внедрения и сопровождения</p>
--	--	---

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 полной 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 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

Система оценок	2	3	4	5
	0-40%	41-60%	61-80 %	81-100 %
Критерий	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
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. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределённому кругу лиц называют:

Ответ: **распространение информации**

2. Защита информации, базирующаяся на применении статей конституции и законов государства, положений гражданского и уголовного кодексов и других нормативно-правовых документов в области информатики, информационных отношений и защиты информации называется:

Ответ: **правовая форма защиты информации**

3. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это:

Ответ: **Информационная система обработки персональных данных (ИСПДн)**

4. Формальная автоматная модель политики безопасности, описывающая множество правил управления доступом называется:

Ответ: **Модель Белла-Лападула**

5. Отношения, связанные с обработкой и хранением персональных данных регулируются:

Ответ: **Федеральным законом «О персональных данных»**

6. Процесс сообщения субъектом своего имени или номера с целью получения определенных полномочий (прав доступа) на выполнение некоторых действий в системах с ограниченным доступом называют:

Ответ: **идентификация**

7. Разновидность файловых вирусов, заражают файлы документов, позволяющие хранить внутри себя команды на макроязыке называют:

Ответ: **макровирусы**

8. Таблица, в которой строки соответствуют субъектам, столбцы — объектам доступа, а на пересечении строки и столбца содержатся правила (разрешения) доступа субъекта к объекту называется:

Ответ: **матрица доступа**

9. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами называется:

Ответ: **межсетевой экран (файрвол, брандмауэр)**

10. Информационная система, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой ИС называется:

Ответ: **защищенная информационная система**

11. Описание требований безопасности к автоматизированной информационной системе. Обычно заключается в определении потоков информации, разрешенных в системе, и правил управления доступом к информации

Ответ: **модель безопасности**

12. Лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства является:

Ответ: **нарушителем**

13. Основное средство (способ), обеспечивающее конфиденциальность информации, передаваемой по открытым каналам передачи данных называется:

Ответ: **шифрование**

14. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально называют:

Ответ: **несанкционированный доступ к информации**

15. Документированная информация, доступ к которой ограничен в соответствии с законодательством РФ это:

Ответ: **Конфиденциальная информация**

16. Естественные угрозы безопасности информации вызваны:

Ответ: **воздействиями объективных физических процессов или стихийных природных явлений**

17. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных и иных ресурсов системы называют:

Ответ: **непреднамеренные угрозы**

18. Атака с использованием спам писем, собирающих логины и пароли пользователей называется:

Ответ: **Фишинг**

19. Модель, которая регулирует, как компьютеры, смартфоны, планшеты и другие устройства взаимодействуют в рамках одной сети, а также как они обмениваются информацией называется:

Ответ: **OSI**

20. Атака, при которой несколько источников воздействуют на один сервер, сайт или сеть называется:

Ответ: **отказ в обслуживании (распределенная атака, DDoS)**

21. Протокол аутентификации и шифрования для защиты взаимодействий в интернете. Подразумевает, что две стороны обмениваются сообщениями: так они подтверждают друг друга, устанавливают используемые алгоритмы шифрования, согласуют ключи сеанса и называется:

Ответ: **TLS (входит в работу HTTPS)**

22. Протокол, который создает защищенное соединение между сервером и браузером. Он помогает подтвердить, что пользователь является тем, за кого себя выдает и называется:

Ответ: **SSL**

Тестовые задания закрытого типа:

1. Следующие биометрические персональные данные позволяют физическим лицам в РФ получать банковские услуги с помощью удаленной идентификации:

1	изображение лица
2	изображение радужной оболочки глаза
3	отпечатки пальцев
4	голос

Ответ: 1,4

2. Свойство информации, в рамках функционирующей автоматической системы обработки информации (АСОИ), находиться в неискаженном виде – это:

1	целостность
2	доступность
3	безопасность
4	конфиденциальность

Ответ: 1

3. Автономные системы шифрования являются примером реализации следующего подхода к обеспечению безопасности ИС:

1	комплексного
2	фрагментарного
3	организационного

Ответ: 2

4. Электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом – это:

1	Неквалифицированная электронная подпись
2	Простая электронная подпись
3	Квалифицированная электронная подпись
4	Расширенная электронная подпись

Ответ: 2

5. Найдите утилиту, необходимую для работы программного комплекса, проверяющего подлинность электронной отчетности, предоставляемой в кредитные организации:

1	WinToUSB
---	----------

2	Tunngle
3	КриптоПро CSP
4	CoinVaultDecryptor

Ответ: 3

6. Заключительным этапом построения системы защиты является:

1	планирование
2	анализ уязвимых мест
3	сопровождение
4	управление

Ответ: 3

7. Самой опасной категорией нарушителей для компании с точки зрения вероятного мошенничества и нарушения безопасности являются:

1	хакеры
2	конкуренты
3	террористы
4	сотрудники

Ответ: 4

8. Укажите ситуацию, при которой целесообразно не предпринимать никаких действий в отношении выявленных рисков:

1	когда риски не могут быть приняты во внимание по политическим соображениям
2	когда стоимость контрмер превышает ценность актива и потенциальные потери
3	когда стоимость контрмер соизмерима с ценностью активов
4	когда риски не могут быть реализованы чаще одного раза в два года

Ответ: 2

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 «Технологическая 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.А. Бабаева.

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29.08.2024 г).

Председатель методической комиссии



О.С. Витренко