10.02.05.01-2024

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Институт профессионального образования

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: институт профессионального образования
Должность: директор института
Дата: 19.06.2024 11:58:37

Сьянова Татьяна Юрьевна

Программа учебной практики

по профессиональному модулю
«Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Присваиваемая квалификация
"Техник по защите информации "

Формы обучения
очная

Кемерово 2024 г.

1707271359

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 25.03.2024 16:34:50

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 3 от 25.03.2024

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 25.03.2024 16:35:10

Прокопенко Евгения Викторовна

Согласовано цикловой-методической комиссией по направлению подготовки (специальности) 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Протокол № от 19.06.2024

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 25.03.2024 16:35:42

Прокопенко Евгения Викторовна

Согласовано заместителем директора по УР ИПО

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: Заместитель директора по учебной работе
Дата: 25.03.2024 16:35:42

Полуэктова Наталья Сергеевна

Согласовано заместителем директора по МР ИПО

1. Общая характеристика рабочей программы практики

Учебная практика является частью программы подготовки профессинального модуля «Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин» основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Прохождение практики направлено на формирование компетенций:

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

Знать: особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации;

Уметь: применять программные и программно-аппаратные средства для защиты информации в базах данных;проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись;

Иметь практический опыт: решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных

2. Структура и содержание рабочей программы практики

2.1 Объем практики и виды работы

Вид учебной работы	Объем часов
Обязательная нагрузка (всего)	**216 часов**
Промежуточная аттестация в форме .	

2.2 Тематический план и содержание практики

Наименование тем практики	Виды работ	Объем часов
Вид профессиональной деятельности: Защита информации в автоматизированных системах программными и программноаппаратными средствами		
Программные и программно-аппаратные средства защиты информации.	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.	20
	Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности.	20
	Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.	20
	Составление документации по учету, обработке, хранению и передаче конфиденциальной информации.	22
	Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации.	20
	Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.	20
	Устранение замечаний по результатам проверки.	20
	Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	24
Криптографические средства защиты информации.	Применение математических методов для оценки качества и выбора наилучшего программного средства.	24
	Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.	26
Всего:		**216**

3. Условия реализации программы практики

3.1 Требования к минимальному материально-техническому обеспечению

Оборудование рабочих мест:

1. Специальное помещение № 1406 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональный компьютер.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

2. Специальное помещение № 1435 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3. Специальное помещение № 1251 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

4. Специальное помещение № 1139 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

5. Специальное помещение № 1147 представляет собой помещение для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь

Помещение для самостоятельной работы обучающихся:

6. Специальное помещение № 1237 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Коммутатор AlliedTelesynLayer 2 SmartSwitch,

Перечень программного обеспечения: LibreOffice. MozillaFirefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

Помещение для самостоятельной работы обучающихся:

7. Специальное помещение № 1211 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Специализированная мебель (столы и стулья); компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ, в том числе:

проектор, экран настенный моторизованный.

Перечень программного обеспечения: LibreOffice. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

8. Специальное помещение №1134 представляет собой компьютерный класс оснащенный современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении учебных занятий в данных классах:

Перечень основного оборудования:

Специализированная мебель (столы и стулья), лабораторное оборудование, персональные компьютеры

Перечень программного обеспечения: СПРУТ, Autodesk AutoCAD 2017, Autodesk

Inventor, СПРУТ-ТП, SprutCAD, Autodesk AutoCAD 2018, КОМПАС-3D, Microsoft Windows, SprutCAM,

СПРУТ-ОКП

9. Специальное помещение №1251 представляет собой лабораторию программных и программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами; программно-аппаратными средствами защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности; программными и программно-аппаратными средствами обнаружения вторжений; средствами уничтожения остаточной информации в запоминающих устройствах; программными средствами выявления уязвимостей в автоматизированных системам и средствах вычислительной техники; программными средствами криптографической защиты информации; программными средствами защиты среды виртуализации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3.2 Информационное обеспечение реализации программы

3.2.1 Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для СПО / Внуков А. А.. – 3-е изд., пер. и доп. – Москва : Юрайт, 2020. – 161 с. – ISBN 978-5-534-13948-8. – URL: https://urait.ru/book/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-467356 (дата обращения: 05.02.2024). – Текст : электронный.

3.2.2 Дополнительная литература

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование.: учебное пособие для вузов / Бабенко Л. К., Ищукова Е. А.. – Москва : Юрайт, 2020. – 220 с. – ISBN 978-5-9916-9244-1. – URL: https://urait.ru/book/kriptograficheskaya-zaschita-informacii-simmetrichnoe-shifrovanie-452871 (дата обращения: 05.02.2024). – Текст : электронный.

3.2.3 Методическая литература

1. Профессиональный цикл : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово : КузГТУ, 2020. – 290 с. – URL: http://library.kuzstu.ru/meto.php?n=9964 (дата обращения: 05.02.2024). – Текст : электронный.

2. Методические указания по оформлению отчетов по практике, курсовых работ (проектов) и выпускных квалификационных работ : для всех специальностей СПО / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информатики и информационных систем, составители: Н. С. Полуэктова, Т. С. Семенова. – Кемерово : КузГТУ, 2022. – 1 файл (762 Кб). – URL: http://library.kuzstu.ru/meto.php?n=10478 (дата обращения: 05.02.2024). – Текст : электронный.

3.2.4 Ресурсы информационно-телекоммуникационной сети «Интернет»

1. ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст:

электронный.

3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.

4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.

5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.

6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.

7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.

9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.

10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.

11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4. Фонд оценочных средств

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по учебной практике по профессиональному модулю "Защита информации в автоматизированных системах программными и программноаппаратными средствами"

4.1. Паспорт фонда оценочных средств

Планируемые результаты обучения по практике.

Практика направлена на формирование следующих компетенций выпускника:

Вид профессиональной деятельности	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**

Вид профессиональной деятельности	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
Защита информации в автоматизированных системах программными и программноаппаратными средствами	ПК 2.4	**Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; **Умения:** применять программные и программно-аппаратные средства для защиты информации в базах данных;проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; **Практический опыт:** решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных	Проверка отчёта по разделам практики.

4.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных

материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

4.2.1. Оценочные средства при текущем контроле

Текущий контродь по учебной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:

1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:

90-100 баллов – при раскрытии всех разделов в полном объеме;
80-89 баллов – при раскрытии всех разделов с недочетами;
60-79 баллов – при раскрытии не всех разделов в полном объеме;
0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

Тема 1.1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

Задание 1. Изучите документацию к защищаемой автоматизированной системе и сформируйте перечень наиболее вероятных угроз для нее.

Задание 2. Сформируйте перечень программных и программно-аппаратных средств обеспечения информационной безопасности для защищаемой автоматизированной системы.

Задание 3. На основе проведенного анализа в заданиях 1 и 2, а также паспортов программных и программно-аппаратных средств обеспечения информационной безопасности предложите и обоснуйте выбор конкретных средств, наиболее подходящих в данных условиях и с учетом экономического фактора.

Задание 4. При наличии выбранных вами устройств выполните их монтаж (программную установку), настройку и проверьте их работу.

Тема 1.2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности.

Задание 1. Изучите инструкцию по диагностике, устранению отказов и обеспечению работоспособности программно-аппаратных средств обеспечения информационной безопасности для каждого конкретного средства.

Задание 2. Ознакомьтесь с приборами и инструментами, использующимися в диагностике, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности для каждого конкретного средства.

Задание 3. Используя приборы и инструменты, изученные в задании 2, выполните диагностику неполадки программно-аппаратного средства обеспечения информационной безопасности, а затем для выявленной неполадки предложите варианты ее устранения.

Задание 4. При наличии необходимых запчастей и материалов устраните неполадку и после ремонта проверьте качество работы программно-аппаратного средства обеспечения информационной безопасности.

Тема 1.3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.

Задание 1. Ознакомиться с инфраструктурой защищаемой информационной системы, а также с характеристиками применяемыми программно-аппаратными средствами обеспечения информационной безопасности.

Задание 2. С помощью теста сымитировать информационную атаку на защищаемую систему и оценить эффективность применяемых программно-аппаратных средств обеспечения информационной

безопасности.

Задание 3. Проанализировать результаты теста и при неудовлетворительных показателях предложить варианты их улучшения или замену программно-аппаратных средств, имеющих более высокую степень защиты.

Тема 1.4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации.

Задание 1. Изучить пути движения конфиденциальной информации в данном учреждении, составить схему.

Задание 2. Выполнить сортировку информации по критериям доступа, типу, способ обработки, хранения и передачи.

Задание 3. Составьте в Excel таблицу, в которой в строках будет перечислена дата и описание конфиденциальной информации, а в столбцах – критерии доступа, тип, способ обработки, хранения, передачи, источник, приемник. Как альтернативный вариант – таблица может быть составлена в виде БД в Access. Для безопасности рекомендуется защитить файл паролем.

Тема 1.5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации.

Задание 1. Изучить характер конфиденциальной информации и при наличии нескольких ее типов выполнить классификацию.

Задание 2. Изучить пути передачи информации, а также способ ее обработки.

Задание 3. На основе результатов, полученных в заданиях 1 и 2 выбрать ПО для обработки информации, которое может работать совместно с криптографической системой.

Задание 4. Настроить сетевую папку, доступ к которой возможен по логину и паролю и разместить в ней файлы с конфиденциальной информацией. Также настроить автоматическую архивацию файлов на сервере во избежание их потери.

Задание 5. С помощью межсетевого экрана на сервере заблокировать доступ к сетевой папке для всех несанкционированных пользователей учреждения.

Задание 6. На клиентских ПК настроить работу с файлами конфиденциальной информации в режиме шифрования либо подключить и настроить программу криптографии для передачи файлов по сети в зашифрованном виде.

Тема 1.6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.

Задание 1. Составить (а если уже составлена ранее, то ознакомиться) со схемой движения конфиденциальной информацией.

Задание 2. Классифицировать все элементы информационной системы предприятия по иерархическим уровням, к которым относятся не только компьютеры и сервера, но и помещения, ПО, математическое обеспечение и алгоритмы.

Задание 3. На основе стандартов и шаблонов составить (либо распечатать) бланки проверок для каждого элемента информационной системы, в которых будут указаны: аппаратное обеспечение, помещение, программное обеспечение, математическое обеспечение и алгоритмы, а также критерии проверки.

Задание 4. Составить схему маршрута обхода проверок по принципу «от низшей иерархии элементов ИС к высшей».

Тема 1.7. Устранение замечаний по результатам проверки.

Задание 1. Проанализировать на основе заполненных бланков проверок несоответствия и сформировать сводный лист исправлений замечаний по аттестации объектов, помещений, программ, алгоритмов.

Задание 2. Проанализировать каждое замечание и предложить варианты их устранения.

Задание 3. При наличии необходимых средств, деталей и материалов устранить выявленные замечания, после чего сделать отметку в листе исправлений с указание даты и подписи.

Тема 1.8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.

Задание 1. Изучить инструкции и рекомендации разработчика программно-аппаратных средств информационной безопасности.

Задание 2. Изучить инструкции и внутренние правила предприятия по обеспечению информационной безопасности программно-аппаратными средствами.

Задание 3. С помощью ГОСТов и справочно-правовых систем типа «Гарант» и «Консультант +» изучить нормативных правовых актов относительно обеспечения информационной безопасности

программно-аппаратными средствами.

Задание 4. На основании документов, изученных в заданиях 1-3 скомпилировать проект внутреннего нормативного методического документа по обеспечению информационной безопасности программно-аппаратными средствами.

Тема 2.1. Применение математических методов для оценки качества и выбора наилучшего программного средства

Задание 1. Составить математическую модель, в которой в качестве целевой функции будет интегральный показатель защищенности информации, а в качестве параметров будут такие как: скорость работы системы по преобразованию информации, алгоритм криптографии, битовая длина ключа, вероятность взлома зашифрованного сообщения.

Задание 2. На основе математической модели составить на любом языке программу, в которую подставить значения параметров, соответствующие различным используемым криптографическим программным средствам.

Задание 3. Выполнить вычисления и по наибольшему показателю защищенности информации выбрать наилучшее криптографическое программное средство.

Тема 2.2. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.

Задание 1. Установить и настроить программу-криптопровайдер, например, Крипто-Про.

Задание 2. Установить и настроить необходимые плагины в веб-браузер для работы с информационной системой учреждения - контрагента.

Задание 3. С помощью специального ПО сгенерировать на флэш-носитель ключ электронной цифровой подписи (ЭЦП).

Задание 4. При необходимости установите и настройте программу для создания защищенного VPN-канала.

Задание 5. Установить корневой и личный сертификат ЭЦП в программу-криптопровайдер.

Задание 6. Проверить работу настроенной системы. Для этого войти с помощью браузера в информационную систему учреждения - контрагента под своей учетной записью, сформировать какой-либо документ, а затем подписать его с помощью личной ЭЦП (флэш-носитель должен быть вставлен в ПК) и отправить. На основании уведомлений сделать вывод о работоспособности настроенной системы защиты информации.

4.2.2. Оценочные средства при промежуточном контроле (зачет, диффиринцированный зачет)

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов:

Тема 1.1. Установка программного обеспечения в соответствии с технической документацией.

1. Приведите пример наиболее известных программных средств обеспечения информационной безопасности в автоматизированных системах.

2. Приведите пример наиболее известных программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

3. Приведите пример по ограничению в применении какого-либо программного и программно-аппаратного средства обеспечения информационной безопасности в автоматизированных системах

4. Какие параметры являются критерием применимости программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах?

5. Как, чем и кем оценивается правильность применения программных и программно-

аппаратных средств обеспечения информационной безопасности в автоматизированных системах?

Тема 1.2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.

1. Какие типы отказов существуют в программно-аппаратных средствах обеспечения информационной безопасности?

2. Каким образом производится устранение отказов в программно-аппаратных средствах обеспечения информационной безопасности?

3. Какие инструменты и средства используются при диагностике программно-аппаратных средств обеспечения информационной безопасности?

4. Какие мероприятия способствуют обеспечению работоспособности программно-аппаратных средств обеспечения информационной безопасности?

5. Существуют ли какие-либо нормы времени на устранение отказов программно-аппаратных средств обеспечения информационной безопасности?

Тема 1.3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.

1. На основе каких критериев делается оценка об эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности?

2. Какие методики или тесты используются при оценке эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности?

3. Кто уполномочен делать оценку эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности?

4. Что делать в случае неудовлетворительной оценки эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности?

5. Существует ли какая-то интегральная шкала оценок эффективности? Если да, то как она выглядит?

Тема 1.4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации

1. Как выглядит типовая схема путей движения конфиденциальной информации в большинстве учреждении?

2. В каком виде составляется документация по учету, обработке, хранению и передаче конфиденциальной информации?

3. Кем составляется документация по учету, обработке, хранению и передаче конфиденциальной информации?

4. Используются ли какие-либо принципы автоматизации при составлении документации по учету, обработке, хранению и передаче конфиденциальной информации? Если да, то приведите пример.

5. Для чего составляется документация по учету, обработке, хранению и передаче конфиденциальной информации?

Тема 1.5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации

1. Существует ли какое-либо специализированное ПО для обработки, хранения и передачи конфиденциальной информации? Если да, то приведите пример.

2. Какие используются стандартные программные средства при обработке, хранении и передаче конфиденциальной информации?

3. Какие средства защиты конфиденциальной информации используются для передачи между двумя клиентскими ПК? Приведите пример.

4. Какие существуют встроенные в ОС Windows средства защиты конфиденциальных файлов при работе в сетевой среде?

5. Какие существуют средства защиты для хранения конфиденциальной информации на серверах?

Тема 1.6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.

1. Какие сведения нужны для составления маршрута при проведении различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов?

2. Что представляет собой маршрут для проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов? В каком виде он может быть представлен?

3. Какие элементы информационной системы относятся к низшей иерархии, а какие к высшей?

4. Где можно взять или как составить бланки для проведения различных видов контрольных

проверок при аттестации объектов, помещений, программ, алгоритмов? В каком виде могут существовать эти бланки?

5. Существует ли какое-либо специальное ПО для составления маршрута проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов?

Тема 1.7. Устранение замечаний по результатам проверки.

1. Как выглядит и в какой форме может быть представлен сводный лист исправлений замечаний по аттестации объектов, помещений, программ, алгоритмов?

2. Какие замечания являются существенными, а какие несущественными? Приведите пример.

3. Что требуется для устранения замечаний?

4. Существуют ли какие-либо временные нормативы для устранения замечаний?

5. Кто уполномочен устранять замечания по результатам проверки?

Тема 1.8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов

1. Кто разрабатывает и утверждает внутренние нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами в учреждении?

2. Кто разрабатывает и утверждает федеральные нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами?

3. Как связаны и как соотносятся между собой внутренние и федеральные нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами с инструкциями от разработчика этих средств?

4. При составлении (компиляции) внутреннего нормативного методического документа по обеспечению информационной безопасности программно-аппаратными средствами из инструкций разработчика, федеральных документов, внутренних документов предприятия в каком порядке расставляются приоритеты?

5. Кем рассматриваются и утверждаются проекты внутренних нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами на предприятии?

Тема 2.1. Применение математических методов для оценки качества и выбора наилучшего программного средства

1. Приведите пример математической модели для оценки качества и выбора наилучшего программного средства? Что можно использовать в качестве целевой функции, а что в качестве параметров?

2. Можно ли с помощью Excel реализовать какую-либо математическую модель, оценить качество и сделать выбор наилучшего программного средства?

3. Что представляет собой интегральный показатель защищенности информации? Из чего он состоит?

4. Что является критерием качества ПО для защиты информации?

5. Существуют ли готовые математические формулы для оценки качества и выбора наилучшего программного средства защиты информации? Если да, то приведите пример.

Тема 2.2. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.

1. Что такое программа-криптопровайдер и для чего она нужна? приведите примеры.

2. Какие плагины необходимо чаще всего подключить к веб-браузеру, чтобы работать, например, с казначейством, налоговой инспекцией, банком, пенсионным фондом?

3. Кратко опишите процесс генерации ключей к электронной цифровой подписи (ЭЦП). Кем генерируются ключи?

4. Для чего нужны корневой и личный сертификат, устанавливаемый на рабочее место сотрудника, работающего с информационной системой?

5. Существуют ли особые требования к хранению и использованию ключевых носителей ЭЦП? Если да, то какие именно?

4.2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта, необходимых для формирования соответствующих компетенций

По итогам практики аттестуются обучающиеся, выполнившие программу практики и представившие индивидуальные отчеты по практике.

Формой итогового контроля прохождения практики является зачет с оценкой.

Зачет проводится с учетом защиты отчетов, составленных в соответствии с требованиями

программы практики, на основании утвержденного задания на практику.

Защита отчета проводится руководителем практики от кафедры.

При проведении текущего контроля обучающийся представляет выполненные элементы (разделы) отчета по практике.

Преподаватель анализирует их содержание на соответствие, после чего оценивает достигнутый результат.

При проведении промежуточной аттестации обучающийся представляет отчет по практике.

Преподаватель анализирует содержание отчета, затем путем беседы с обучающимся выявляет его способность обосновывать принятые решения.

5. Иные сведения и (или) материалы

Отчет по практике является основным документом, характеризующим работу обучающегося во время практики. Отчет составляется в соответствии с программой практики и содержит следующие разделы:

1. Титульный лист.
2. Рабочий график (план) практики, утвержденный заведующим кафедрой и согласованный с руководителем практики от КузГТУ и (или) предприятия.
3. Введение.
4. Выполнение индивидуального задания.
5. Выводы.
6. Список использованных источников и литературы.

Требования к оформлению отчета

Результаты практики должны быть оформлены в форме отчета, в соответствии с требованиями:

Страницы не обводятся в рамках, поля не отделяюся чертой. Размеры полей не менее: левого - 30 мм, правого - 10 мм, верхнего - 20 мм и нижнего - 20 мм. Нумерация страниц отчета - сквозная: от титульного листа до последнего листа приложений.

Номер страницы на титульном листе не проставляют.

Номер страницы ставят в центре нижней части листа, точка после номера страницы не ставится.

Страницы, занятые таблицами и иллюстрациями, включают в сквозную нумерацию.

Объем отчета по практике должен быть не менее 16 страниц (без учета приложений) машинописного текста (шрифт 14пт, Times New Roman, через 1 интервал). Отчет должен быть отпечатан на формате А4 и подшит. Описания должны быть сжатыми. Объем приложений не регламентируется, а их содержание определяется обучающимся самостоятельно.

Оформление формул

Формулы должны быть оформлены в редакторе формул. В формулах в качестве символов следует применять обозначения, установленные соответствующими государственными стандартами. Расчет по формулам ведется в основных единицах измерения, формулы записываются следующим образом: сначала записывается формула в буквенном обозначении, после знака равенства вместо каждой буквы подставляется ее численное значение в основной системе единиц измерения; затем ставится знак равенства и записывается конечный результат с единицей измерения. Пояснения символов и числовых коэффициентов, входящих в формулу, если они не пояснены ранее в тексте, должны быть приведены непосредственно под формулой. Пояснения каждого символа следует давать с новой строки в той последовательности, в которой символы приведены в формуле. Первая строка пояснения должна начинаться со слова «где» без двоеточия после него.

Переносить формулы на следующую строку допускается только на знаках выполняемых операций, причем знак в начале следующей строки повторяют. При переносе формулы на знаке умножения применяют знак «×».

Формула нумеруется, если далее по тексту она будет востребована. Формулы, за исключением формул, помещаемых в приложении, должны нумероваться сквозной нумерацией арабскими цифрами, которые записывают на уровне формулы справа в круглых скобках. Допускается нумерация в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой.

Ссылки в тексте на порядковые номера формул дают в круглых скобках, например, в формуле (9.1).

Формулы, помещаемые в приложениях, должны нумероваться отдельной нумерацией, арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения

приложения. Например, формула (А.1).

Оформление иллюстраций

Иллюстрационный материал может быть представлен в виде схем, графиков и т.п. Иллюстрации, помещенные в тексте и приложениях отчета, именуются рисунками.

Иллюстрации выполняются в графических редакторах и располагаются после первой ссылки на них и как можно ближе к ссылке на них в тексте.

Иллюстрации, за исключением иллюстраций приложений, следует нумеровать арабскими цифрами в пределах раздела, либо сквозной нумерацией. Например, «Рисунок 1», «Рисунок 1.1», «Рисунок 2.1».

Ссылку на иллюстрацию дают в следующем виде: «в соответствии с рисунком 1».

Иллюстрация при необходимости может иметь наименование и пояснительные данные (подрисуночный текст). Слово "Рисунок" и наименование помещают после пояснительного текста без точки в конце.

Все рисунки формата большего, чем А4, выносятся в приложения.

Построение таблиц

Слово «Таблица», ее номер и название помещают слева над таблицей. Название таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Название таблицы записывают через тире после слова «Таблица» с прописной буквы без точки в конце. Например: «Таблица 2.1 – Технические данные».

Заголовки граф и строк таблицы пишутся с прописной буквы, а подзаголовки граф- со строчной буквы, если они составляют одно предложение с заголовком, или с прописной буквы, если они имеют самостоятельное значение. В конце заголовков и подзаголовков таблиц точки не ставят. Заголовки и подзаголовки граф указывают в единственном числе.

Заголовки граф записывают параллельно строкам таблицы. При необходимости допускается перпендикулярное расположение заголовков граф.

Таблицу в зависимости от ее размера помещают под текстом, в котором впервые дана ссылка на нее, или на следующей странице, а при необходимости, в приложении к документу. Допускается помещать таблицу вдоль длинной стороны листа документа.

Если в конце страницы таблица прерывается, ее продолжение помещают на следующей странице. При переносе таблицы на другую страницу название помещают только над первой частью таблицы. Слово «Таблица» указывают только один раз слева над первой частью таблицы а, над другими частями пишут слова «Продолжение таблицы» с указанием номера таблицы.

Все таблицы, за исключением таблиц приложений, нумеруются арабскими цифрами сквозной нумерацией. Допускается нумеровать таблицы в пределах раздела. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенного точкой.

Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавления перед цифрой обозначения приложения, например, «Таблица А.1», если она приведена в приложении А.

На все таблицы документа должны быть приведены ссылки в тексте, при ссылке слово «таблица» пишется полностью с указанием ее номера.

Оформление списка литературы

Список литературы является обязательным (ненумерованным) разделом отчета, оформляется в соответствии с ГОСТ 7.1-2003 "Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления", включается в содержание отчета.

Список должен содержать сведения обо всех источниках, использованных при составлении отчета. Располагать источники в списке рекомендуется в порядке появления ссылок в тексте. Возможно и другое разрешенное нормативными документами расположение источников в списке.

Оформление приложений

Приложения оформляют как продолжение отчета и помещают в конце отчета в порядке ссылок на них в тексте. В тексте отчета на все приложения должны быть даны ссылки. Каждое приложение следует начинать с нового листа с указанием на верху посредине страницы слова «ПРИЛОЖЕНИЕ» и его обозначения, например, «ПРИЛОЖЕНИЕ А». Приложение должно иметь заголовок, который записывается симметрично относительно текста с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами алфавита, начиная с А, кроме букв Е, З, Й, О, Ч, Ь, Ы, Ъ. Допускается обозначение приложения буквами латинского алфавита, за исключением букв I и O. Приложения выполняют на листах формата А4, А3, А4Х3,А4х4, А2, А1 по ГОСТ 2.301.

Приложения должны иметь общую с остальной частью документа сквозную нумерацию страниц.

Все приложения должны быть перечислены в содержании отчета и с указанием их номеров и заголовков.

Документ подписан электронной подписью
Яковлев Алексей Николаевич
Ректор
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т.Ф. ГОРБАЧЕВА"

00E16CF19AEF1B29DB06BEB121D580D3D8
Срок действия с 19.03.2024 до 12.06.2025
УЦ: Казначейство России

Подписано: 30.09.2024 11:21 (UTC+7)

1707271359