



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)**

Кафедра «Информационная безопасность в вычислительных системах и сетях»

**Методические рекомендации
по изучению дисциплины «Программно-аппаратные средства обеспечения
информационной безопасности ресурсов информационных технологий /
Программно-аппаратные средства защиты информации информационных
систем»
для обучающихся 1-го и 2го курса
по направлению 09.04.02 Информационные системы и технологии
заочной формы обучения (классификация – магистр)**

Ростов – на – Дону
2024г.

УДК 004

Составитель:
Н.Д. Панасенко

Методические рекомендации
к контрольной работе дисциплины «**Программно-аппаратные средства
обеспечения информационной безопасности ресурсов информационных
технологий / Программно-аппаратные средства защиты информации
информационных систем**»
/ ДГТУ, Ростов – на – Дону, 2024

Методические рекомендации по изучению дисциплины для обучающихся представляют собой комплекс рекомендаций и разъяснений, позволяющих обучающимся оптимальным образом организовать процесс изучения данной дисциплины. Методические рекомендации могут быть использованы для самостоятельной работы. Позволяет обучающимся оптимальным образом организовать процесс выполнения контрольной работы.

Предназначено для обучающихся по направлению 09.04.02 Информационные системы и технологии заочной формы обучения (классификация – магистр)

Печатается по решению редакционно-издательского совета
Донского государственного технического университета

Ответственный за выпуск: зав. кафедрой «Информационная безопасность в
вычислительных системах и сетях»
канд. пед. наук, доц. А.Р. Газизов

В печать _____ 2024 г.

Формат 60×84/16.

Объем 0,8 усл. п. л.

Тираж 50 экз. Заказ №. _____

Издательский центр ДГТУ

Адрес университета и полиграфического предприятия:
344003, г. Ростов-на-Дону, пл. Гагарина, 1

© Донской государственный
технический университет, 2024

ВВЕДЕНИЕ

Цели и задачи дисциплины

Подготовка обучающихся к деятельности, связанной с использованием различных современных средств защиты информации, а также формирование представлений о разработке, реализации, эксплуатации, анализе, сопровождения и совершенствования систем управления информационной безопасностью компьютерных систем.

Задачи дисциплины:

- знать классификации программно-аппаратных средств защиты информации и их особенностям;
- научить студентов оценивать степень защищенности информации автоматизированной системы и потенциально возможные действия злоумышленника;
- научить студентов использовать известные специализированные программно-аппаратных средств защиты информации.

1. Алгоритм выбора варианта контрольной работы

Для выбора варианта контрольной работы необходимо взять предпоследнюю и последнюю цифры номера зачетной книжки. Номер варианта находится на пересечении соответствующей строки и столбца.

	Последняя цифра номера зачетной книжки										
		0	1	2	3	4	5	6	7	8	9
Предпоследняя цифра номера зачетной книжки	0	42	3	37	22	37	36	42	12	35	27
	1	6	9	10	21	7	1	2	8	27	14
	2	34	6	15	16	34	20	7	41	40	20
	3	15	19	12	28	31	3	24	15	26	38
	4	29	40	32	5	19	30	23	25	17	13
	5	40	11	31	4	26	18	11	33	34	19
	6	5	35	27	8	17	38	16	25	4	24
	7	32	39	22	11	42	29	20	28	39	21
	8	25	2	10	42	30	19	18	3	31	26
	9	23	38	38	10	9	30	18	9	35	1

Например, для зачетки с номером 123456 необходимо взять номер варианта из 5 – ой строки и 6 – го столбца (вариант 11).

2. Задания для выполнения контрольной работы

При выполнении контрольной работы необходимы компьютеры с установленной ОС Windows, пакет Microsoft Office, пакет КриптоАРМ. К полученной контрольной работе прилагать выполненные работы в электронном виде на цифровом носителе.

Работа № 1.

Написать реферат на одну из нижеперечисленных тем в соответствии с вариантом (оформление согласно правилам вуза)

1. Создание шифрованных пользовательских виртуальных дисков.
2. Биометрическая идентификация.
3. Штрихкодированная идентификация.
4. Анализ программных средств криптографической защиты информации.
5. Анализ программно-аппаратных средств усиленной аутентификации.
6. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
7. Типы контроля безопасности: потоковый, контроль вывода, контроль доступа.
8. Защита программ от изучения.
9. Настройка политики безопасности операционной системы.
10. Аутентификация по многофакторным паролям.
11. Использование смарт-карт и USB-ключей.
12. Анализ защищенности изолированной программной среды.
13. Исследование систем идентификации на основе устройств Bluetooth.
14. Технология Kerberos.
15. Изучение средств межсетевого экранирования.
16. Обзор функций хеширования паролей в ОС и СУБД.
17. Исследование технологий доверенной загрузки операционной системы.

18. Технологии защищенной загрузки терминальных клиентов.
19. Методы сокрытия программных закладок.
20. Радиочастотная идентификация.
21. Методы сокращения влияния человеческого фактора на защищенность системы
22. Средства идентификации и аутентификации объектов баз данных, управление доступом.
23. Средства контроля целостности информации, организация аудита.
24. Использование транзакции для изолирования действий пользователей.
25. Ссылочная целостность.
26. Технологии идентификации на основе карт с магнитной полосой.
27. Протоколы аутентификации для удаленного доступа.
28. Атаки на системы биометрической аутентификации.
29. Аутентификация на основе одноразовых паролей.
30. Аутентификация на основе токенов.
31. Аутентификация по предъявлению цифрового сертификата.
32. Средства аутентификации в компьютерных системах Apple Macintosh.
33. Способы усиления парольной аутентификации.
34. Эволюция методов и средств биометрической аутентификации.
35. Способы защиты от подбора паролей.
36. Обзор средств «запоминания» паролей в сетевых службах.
37. Особенности биометрической аутентификации.
38. Обзор средств генерации паролей.
39. Обзор средств выявления «слабых» паролей.
40. Обзор средств фильтрации паролей.
41. Использование биометрии в идентификационных картах и паспортах.
42. Практическое применение биометрии в России.

Работа №2.

Создать электронную подпись. Привести полученные результаты создания в виде рисунков, оформив, как второе задание реферата (оформленного согласно правилам вуза)

Цель работы: изучить механизм шифрования и подписания документов средствами КриптоАРМ, создания сертификатов, особенности задания цифровых подписей в Microsoft Word.

Задание:

1. изучите средства КриптоАРМ согласно инструкции ниже;
2. самостоятельно изучите функцию Снятие и проверку подписи, Подписи и зашифровки, Расшифровки и проверки подписи;
3. изучите пересылку подписанных документ через сервер другим пользователям;
4. аналогичным образом, самостоятельно, добавьте цифровую подпись с помощью сертификата КриптоАРМ к контрольной работе.

Теоретические сведения

Электронная подпись (ЭП) — это электронная зашифрованная печать, удостоверяющая подлинность цифровых данных, таких как сообщения электронной почты, макросы или электронные документы. Подпись подтверждает, что сведения предоставлены подписавшим их создателем и не были изменены.

ЭП обеспечивает: подлинность (подтверждает личность подписавшего), целостность (гарантирует, что содержимое документа не было изменено или подделано с момента подписания) и неотрекаемость (подтверждает происхождение подписанного содержимого).

Цифровые подписи сочетают в себе черты обычных подписей и удобство цифрового формата. Такая возможность позволяет пользователям убедиться в целостности документа. При этом следует помнить, что юридическая значимость

таких подписей (нормы) для разных стран могут отличаться. В ряде случаев в файлах программных пакетов Microsoft Office ЭП с отметкой защищенного сервера времени при определенных обстоятельствах равносильны нотариальному заверению.

Для создания цифровой подписи необходим сертификат подписи, удостоверяющий личность. При отправке макроса или документа, подписанного цифровой подписью, также отправляется сертификат и открытый ключ. Сертификаты выпускаются центром сертификации и, аналогично водительскому удостоверению, могут быть отозваны. Как правило, сертификат действителен в течение года, по истечении которого подписывающий должен обновить имеющийся сертификат или получить новый для удостоверения своей личности.

Центр сертификации похож на нотариальную контору. Он выпускает цифровые сертификаты, подписывает сертификаты для подтверждения их достоверности, а также отслеживает отозванные сертификаты и сертификаты с истекшим сроком действия. В Microsoft Office доступно несколько способов получения сертификата с использованием каталога партнеров Office в области цифровых подписей.

Для обеспечения этих гарантий создатель содержимого должен заверить его цифровой подписью, соответствующей указанным следующим требованиям:

1. цифровая подпись должна быть действительной;
2. сертификат, связанный с цифровой подписью, является действующим (не просрочен);
3. лицо или организация, поставившая цифровую подпись (издатель), является доверенной;
4. сертификат, связанный с цифровой подписью, выдан издателю компетентным центром сертификации.

КриптоАРМ — универсальное программное средство, предназначенное для шифрования и электронной подписи файлов. Программа используется для защиты

информации, передаваемой по Интернету, электронной почте и на съемных носителях.

Одной из её особенностей является возможность работы с цифровыми сертификатами: устанавливать на компьютер, проверять статус, просматривать и печатать информацию о сертификате и многое другое.

Кроме того, программное средство позволяет выбирать криптопровайдер, который планируется использовать и обладает возможностью интеграции с такими ключевыми носителями как смарт-карта или USB-токен.

Порядок выполнения работы

I Реализация электронной подписи в пакете КриптоАРМ

Перед началом работы установите пакет КриптоАРМ, используя файлдистрибутив `trusteddesktop.exe` после чего перезагрузите виртуальную машину.

Одна из демо-версий КриптоАРМ доступна по ссылке: <https://cryptoarm.ru/>

Создание самоподписанного сертификата

Запустите программу КриптоАРМ: Пуск → Программы → КриптоАРМ.

Выберите меню Сертификаты → Создать самоподписанный сертификат, заполните требуемые поля (рисунок 1).

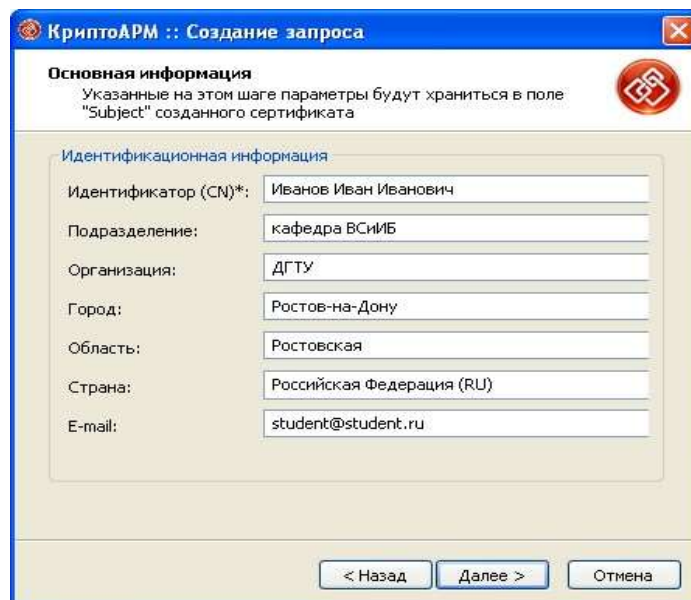


Рисунок 1 – Создание самоподписанного сертификата

Далее выберите используемый криптопровайдер¹, назначение ключа, изучите дополнительные опции во вкладке Дополнительно.

Завершите создание сертификата (рисунок 2).

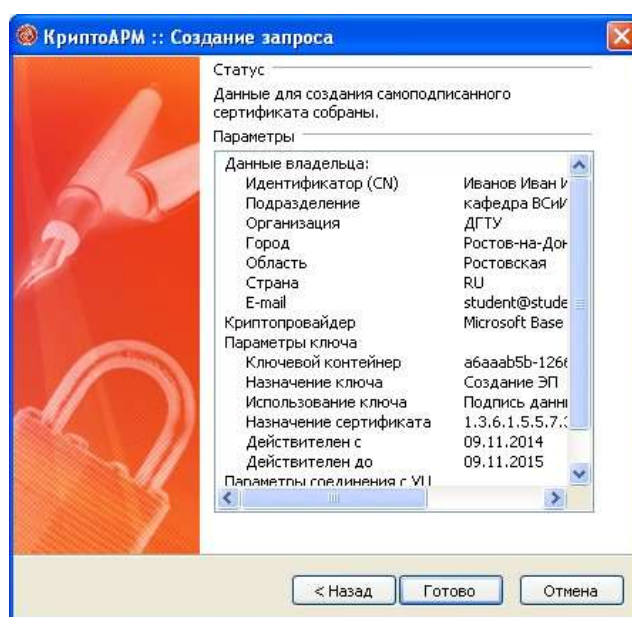


Рисунок 2 – Самоподписанный сертификат

Подпись документа

Создайте doc-документ, который в дальнейшем будет подписан ЭП.

¹ **Криптопровайдер (CSP)** – это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций интерфейса программирования приложений CryptoAPI.

Выберите меню Подпись → Подписать и добавьте doc-файл, который необходимо подписать (рисунок 3).

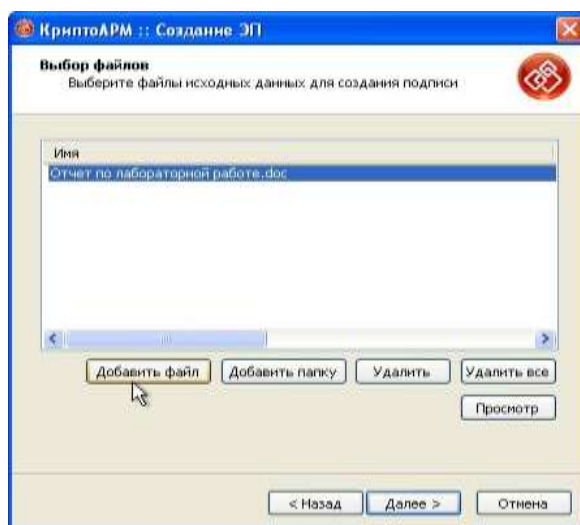


Рисунок 3 – Добавление файла для подписи

При желании можно изменить выходной формат записанного файла. В окне Параметры подписи введите необходимые свойства подписи, комментарии, идентификаторы.

Далее выберите назначение и ваш личный сертификат, которым вы собираетесь подписать документ (рисунок 4). Хэш-алгоритм определится автоматически.

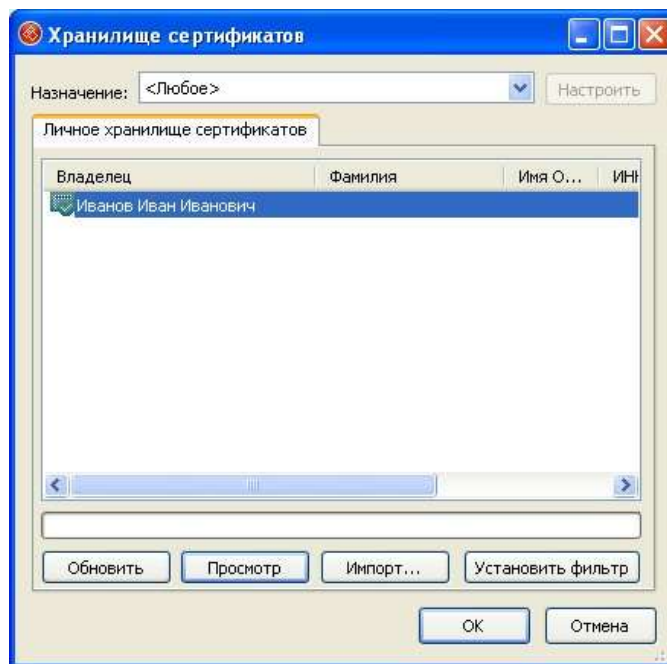


Рисунок 4 – Выбор сертификата

Далее сохраните настройку для дальнейшего использования. Сформированный файл подписи по умолчанию будет сохранен в тот же каталог, в котором находится файл с данными. Имя файла подписи совпадает с именем подписываемого файла, дополненным расширением .sig (рисунок 5).



Рисунок 5 – Подписанный файл

После завершения операции возникнет окно Результат выполнения операции. Чтобы просмотреть детальную информацию о результатах создания подписи и используемых параметрах (имя исходного файла, имя выходного файла, длительность выполнения операции), нажмите Детали.

Если требуется просмотреть информацию о проверяемой ЭП и сертификате подписчика, выделите необходимую запись в списке окна Результат выполнения операции и нажмите Менеджер сообщения. Отчет о проверке подписи можно просмотреть, выбрав запись в поле Дерево подписей и нажав на кнопку Просмотреть – откроется окно с информацией о подписи, сертификате и его статусе (рисунок 6).

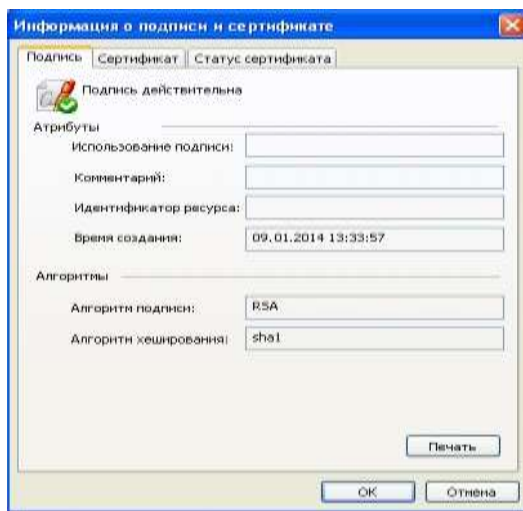


Рисунок 6 – Информация о подписи и сертификате.

Закладка Подпись содержит информацию об атрибутах подписи, времени её создания, используемых алгоритмах подписи и хэширования.

Закладка Сертификат содержит сведения о сертификате и его статусе. Также в этом окне доступна информация о владельце и издателе сертификата, сроках его действия и возможных вариантах исполнения.

Закладка Статус сертификата отображает общий статус проверки полного пути сертификации. Проверка пути сертификации доступна по кнопке Проверить.

Проверка корректности ЭП

В основном окне КриптоАРМ Выберите меню Подпись → Проверить подпись. На первом шаге для упрощения работы можно выбрать в списке наименований одну из уже установленных настроек.

Выберите файл или папку файлов, подписанных ЭП, корректность которых необходимо проверить. В окне Результат выполнения операции отобразится статус операции. Если одна или несколько подписей недействительны, это будет отражено в статусе. Для более подробной информации о результатах проверки ЭП изучите вкладку Детали.

Добавление подписи

В основном окне КриптоАРМ Выберите меню Подпись → Добавить подпись. На первом шаге для упрощения работы можно выбрать в списке наименований одну из уже установленных настроек.

Выберите файл или папку файлов, которые необходимо подписать.

Введите необходимые свойства добавляемой подписи.

Выберите сертификат для добавления подписи, т.е. ваш личный сертификат.

Хэш-алгоритм определится автоматически.

Заверение подписи

В основном окне КриптоАРМ Выберите меню Подпись → Заверить подпись. Выберите подписанный ЭП файл (папку файлов) для заверения.

В поле Дерево подписей выберите подпись, которую необходимо заверить и нажмите кнопку Заверить подпись. Далее проследуйте по уже изученному алгоритму.

В результате операции в окне Управление подписанными данными появится значок заверяющей подписи (в иерархии заверяющая подпись будет подписью второго уровня) (рисунок 7).

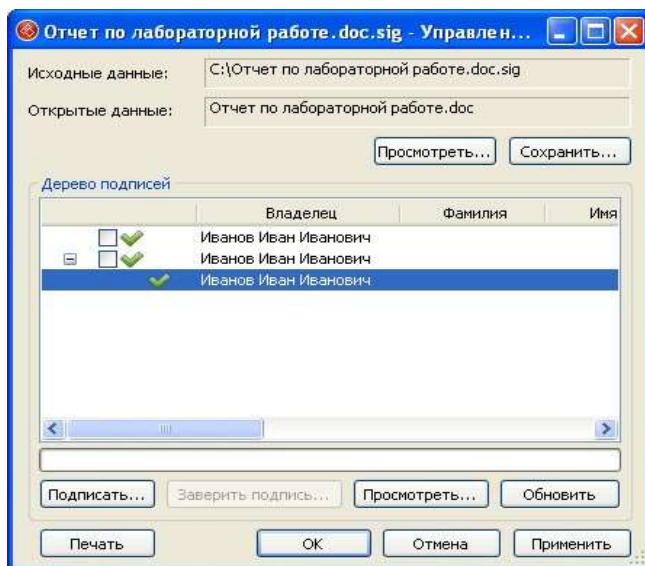


Рисунок 7 – Заверяющая подпись.

II Реализация электронной подписи в пакете Microsoft Word

Создайте документ Microsoft Word и сохраните его на рабочем столе.

В разделе Сведения → Разрешения выберите «Добавить цифровую подпись» (рисунок 8). Обратите внимание, что без установленного пакета КриптоАРМ отсутствует категория «Добавить цифровую подпись (КРИПТО-ПРО)».

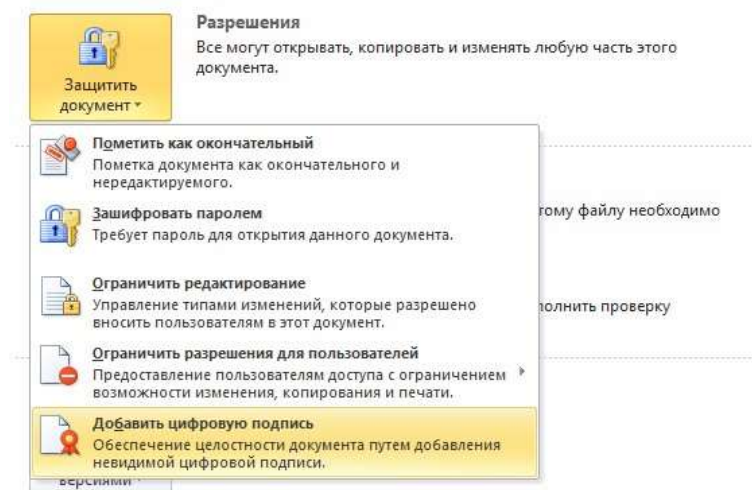


Рисунок 8 – Добавление цифровой подписи в Microsoft Word
Создайте свое цифровое удостоверение (рисунок 9).

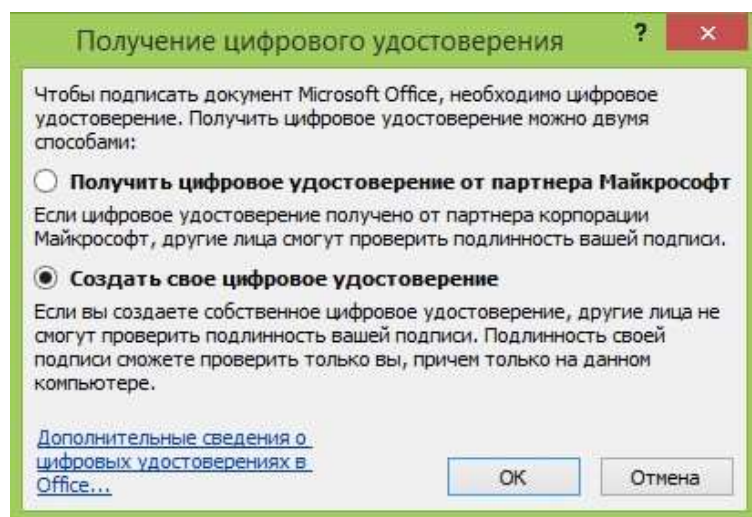


Рисунок 9 – Создание цифрового удостоверения

Задайте цифровую подпись созданного документа.

В появившемся окне осуществляется выбор ранее созданных в сертификатов (рисунок 10). Выберите необходимого пользователя, с чьим ЭП планируется подписать документ. В окне «Цифровые подписи» появится Подписывающий. Таким же образом можно добавить дополнительных подписантов.

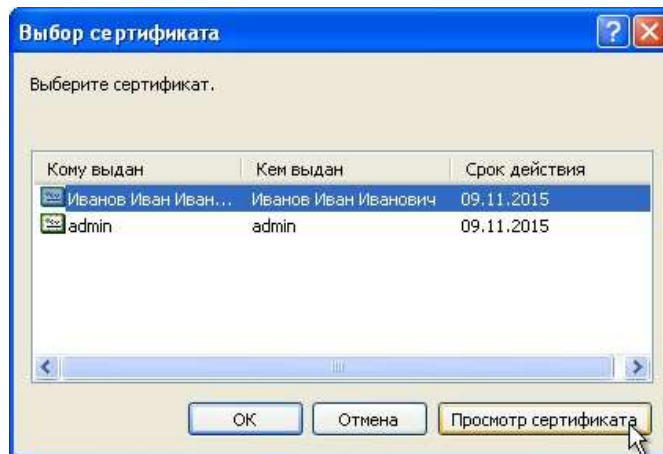


Рисунок 10 – Выбор сертификата

Удостоверьтесь в появлении в правой нижней части окна Microsoft Word значка «Этот документ содержит цифровую подпись». С этого момента, любые изменения, вносимые в документ, удаляют цифровые подписи, о чем программа информирует при попытке сохранить изменения.

Закройте и откройте документ, проверив этим корректность его подписи.

3 Требования к выполнению и оформлению контрольной работы

Требования к выполнению и оформлению контрольной работы приведены в документе «Правила оформления письменных работ обучающихся для технических направлений подготовки» ДГТУ, введенные приказами от 16.12.2020 г. № 242.

4 Пример выполнения и оформления контрольной работы

(рамка – это обозначение страницы, её добавлять не надо)



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Информационная безопасность в вычислительных системах и сетях»

КОНТРОЛЬНАЯ РАБОТА

Дисциплина: «Технологии Web-программирования»

Направление подготовки/специальность: 09.03.02 Информационные системы и технологии

Направленность (профиль): Информационные системы и технологии

Номер зачетной книжки 123456 Номер варианта 10 Группа ВЗИС31

Обучающийся _____ Иван Иванович Иванов
(подпись, дата)

Контрольную работу проверил _____ канд. техн. наук, доцент каф. ИБ, Н.Д. Панасенко
(подпись, дата)

Ростов-на-Дону
2022

Содержание

	Введение	3
1	Выполнение задания 1	4
	1.1 Уточнения	5
	1.2 Уточнения	8
2	Выполнение задания 2 ...	20
	Заключение	26
	Перечень использованных информационных ресурсов	27

(необходимо выполнить в соответствии со стандартом ДГТУ оформления контрольных и курсовых работ)

1 Выполнение задания

1.1 Раскрытие темы

Согласно индивидуальному заданию, был создан сайт ресторана.

В процессе работы применялись знания из следующей литературы [1, 2]. (Это ссылка на список перечень использованных информационных ресурсов)

В результате выполнения задания были получены результаты, приведенные на рисунках 1-5.



Рисунок 1 – Результат создания сайта ресторана



Рисунок 2 – Результат создания сайта ресторана



Рисунок 3 – Результат создания сайта ресторана



Рисунок 4 – Результат создания сайта ресторана

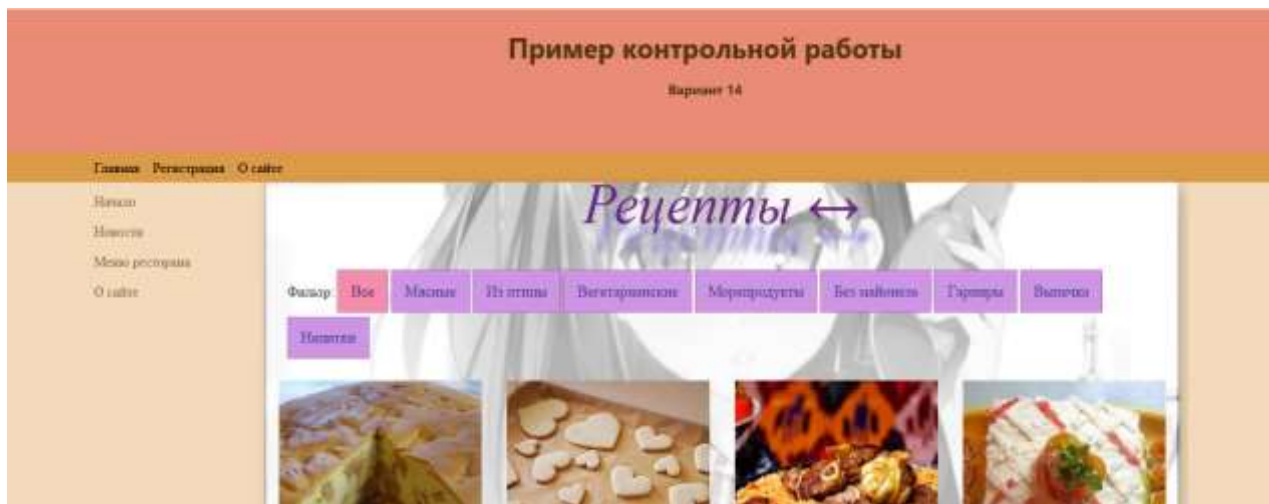


Рисунок 5 – Результат создания сайта ресторана

Листинг рисунка 1

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <link rel="shortcut icon" href="asico.ico"/>
    <link href="newcss.css" rel="stylesheet" type="text/css"/>
    <title></title>
  </head>
  <body>
    <div class=...
..... далее аналогично
```

Перечень использованных информационных ресурсов

1. Баранов, Р.Д., Иноземцева, С.А. Практические аспекты разработки веб-ресурсов : учебное пособие // Саратов: Вузовское образование, 2018.
2. Техэксперт: официальный сайт сети центров нормативно-технической документации «Техэксперт» : сайт/ АО «Кодекс», 2021. –URL : <https://cntd.ru/> (дата обращения: 01.09.2021). – Текст: электронный.

Перечень использованных информационных ресурсов

При изучении дисциплины особое внимание следует обратить на литературные источники согласно таблице 1.

Таблица 1 - Учебно-методическое и информационное обеспечение дисциплины (модуля)

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
1. Рекомендуемая литература				
1.1. Основная литература				
	Авторы, составители	Заглавие	Издательство, год	Количество
Л1.1	Маршаков, Д.В., Фатхи, Д.В.	Программно-аппаратные средства защиты информации: учеб. пособие	Ростов н/Д.: ИЦ ДГТУ, 2021	ЭБС
Л1.2	Хорев Павел Борисович	Программно-аппаратная защита информации: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2022	ЭБС
Л1.3	Потехин, Д.С., Тарасов, И.Е.	Разработка программно-аппаратного обеспечения информационных и автоматизированных систем: учебное пособие	Москва: РТУ МИРЭА, 2022	ЭБС
1.2. Дополнительная литература				
Л2.1	Астайкин, А.И., Мартынов, А.П.	Методы и средства обеспечения программно-аппаратной защиты информации: монография	Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015	ЭБС
Л2.2	Платонов, В.В.	Программно-аппаратные средства защиты информации	М.: ACADEMIA, 2013	1
1.3. Методические разработки				
Л3.1	Помешкин, А.А., Коротких, И.В.	Система защиты информации от несанкционированного доступа на основе	Новосибирск: Новосибирский	ЭБС
Л3.2	Туманов, С.А., Рева, И.Л.	Система защиты информации от несанкционированного доступа на основе	Новосибирск: Новосибирский	ЭБС
3 Перечень информационных технологий				
3.1 Перечень программного обеспечения				
3.1.1	Microsoft DsktpEdu ALNG LicSAPk OLV E			
3.1.2	Microsoft 0365ProPlusOpenStudents ShrdSvr ALNG SubsVL OLV NL 1Mth Acdmc Stdnt w/Faculty			
3.2 Перечень информационных справочных систем, профессиональные базы данных				
3.2.1	ЭБС «Лань» (https://e.lanbook.com)			
3.2.2	ЭБС «ZNANIUM.COM» (http://znanium.com/)			
3.2.3	ЭБС «РУКОНТ» (http://lib.rucont.ru)			
3.2.4	ЭБС «Университетская библиотека онлайн» (www.biblioclub.ru)			
3.2.5	ЭБС «Юрайт» https://urait.ru/			
3.2.6	ЭБС IPRbooks http://www.iprbookshop.ru/			
3.2.7	Научная электронная библиотека https://elibrary.ru/			
3.2.8	Международная реферативная база данных научных изданий Scopus https://www.scopus.com/			
3.2.9	Международная реферативная база данных научных изданий Web of Science http://www.wokinfo.com/			
3.2.10	Электронная образовательная среда ДГТУ http://skif.donstu.ru/			
3.2.11	Информационно-справочная система «Гарант».			
3.2.12	Информационно-справочная система «Кодекс».			
3.2.13	Информационно-справочная система «Консультант плюс».			
3.2.14	Информационно-справочная система «Техэксперт».			

Содержание

Введение

1 Алгоритм выбора варианта контрольной работы

2 Задания для выполнения контрольной работы

3 Требования к выполнению и оформлению контрольной работы

4 Пример выполнения и оформления контрольной работы

Перечень использованных информационных ресурсов