АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»
Факультет экономики, управления и юриспруденции
Кафедра управления и бизнес-информатики

УТВЕРЖДАЮ
Проректор по учебно-
методической работе
_____/ Г.П. Узунова
«02» февраля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

Направление подготовки
09.03.01 Информатика и вычислительная техника

Профиль: специалист по компьютерным системам

Квалификация выпускника: бакалавр

Для всех
форм обучения

Симферополь, 2026 г.

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

Средства оценивания в ходе текущего контроля:

– устные опросы в ходе семинарских занятий;
– рефераты;
– тестирование;
– практические задания, выполняемые в ходе семинарского (практического) занятия или рекомендуемые для самостоятельной работы.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеть: составления технической документации на различных этапах жизненного цикла информационной системы
ОПК-7	Способен участвовать в настройке и наладке программно-аппаратных комплексов	ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть: навыками проверки работоспособности программно-аппаратных комплексов

1.1 Вопросы к текущему контролю

1 Какой из изученных в лабораторной работе редакторов реестра предоставляет функции по разграничению доступа к разделам реестра и как использовать эти функции?

2 Как с помощью программы restrick.exe ограничить доступ пользователей к дисковым устройствам?

3 Как ограничить доступ пользователей к функциям Панели управления с помощью программы restrick.exe?

4 Доступ к каким функциям Панели управления может быть ограничен с помощью программы restrick.exe?

5 В чем недостаточность средств ограничения прав пользователей, предоставляемых программой restrick.exe?

6 Как может быть заблокирована рабочая станция на период временного отсутствия пользователя? Укажите несколько вариантов.

7 Какой из способов блокирования рабочей станции на период временного отсутствия пользователя является наиболее безопасным и почему?

8 Назначение шифрования информации.

9 Какие атрибуты шифрования папки можно указать?

10 Почему необходимо чтобы при копировании или перемещении шифрованной папки пункт назначения поддерживал это шифрование?
11 Как восстановить сертификат из резервной копии?
12 Особенности технология EFS?
13 Что подразумевается под политикой восстановления?
14 Дайте определение аутентификации.
15 Дайте определение авторизации.
16 Какие вам известны способы аутентификации/идентификации?
17 Какие вам известны способы аутентификации с помощью средства безопасности Asp_Net?
18 В чем суть аутентификации Windows?
19 В чем суть аутентификации формой?
20. Способы защиты информации в БД Access.
21. Группы и пользователи БД Access . Файл рабочей группы.
22. Этапы создания рабочей группы с помощью мастера.
23. Порядок изменения пароля пользователя или группы.
24. Для чего создается связь защищенной на уровне пользователя базы данных с файлом рабочей группы (электронным ключом)?
25. К каким файлам БД относятся расширения *.mdw, *.bak, *.mdb?
26. К какому методу шифрования относится криптостандарт DES?
27. Какое действие предполагает следующий участок кода:
28. В чем разница между шифрованием с использованием вектора инициализации и без него?
19.1К какому методу шифрования относится криптостандарт RSA?
19.2Укажите структуру инициализации криптопровайдера RSA.
20 Объясните причину того, что приложении может не с первого раза сработать корректно
21 Администрирование АИС: функции администратора, функции службы безопасности.
22 Какие механизмы безопасности используются для обеспечения "неотказуемости" системы?
23 Что понимается под администрированием средств безопасности?
24 Какие виды избыточности могут использоваться в вычислительных сетях?
25 В чем заключаются преимущества сети с выделенными каналами?
26 Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
27 Виды криптосистем.
28 Задачи, решаемые методами криптографии.
29 История криптографии. Основные этапы становления науки криптографии.
30 Методы криптографических преобразований.
31 Шифрование перестановкой.
32 Шифрование методом гаммирования и аналитического преобразования.
33 Многократное шифрование.
34 Композиция блочных шифров.
35 Совершенные шифры. Пример совершенного шифра.

36 Энтропийные характеристики шифров.

37 Идеальные шифры.

38 Стратегия национальной безопасности Российской Федерации: особенности, цели, составляющие национальных интересов России в информационной сфере.

39 Доктрина информационной безопасности Российской Федерации: назначение документа, источники угроз информационной безопасности Российской Федерации, общие методы обеспечения информационной безопасности РФ.

40 Нормативно-правовое регулирование защиты информации: направления защиты

41 Виды конфиденциальной информации: коммерческая тайна, персональные данные

42 Виды конфиденциальной информации: государственная служебная тайна, процессуальная тайна, авторское, патентное право.

43 Организационно-распорядительная защита информации: цели защиты, принципы построения защиты

1.2 Темы рефератов:

2. Уровни представления информации в компьютерных системах и сетях.
3. Основные свойства защищаемой информации и методы их обеспечения.
4. Классификация видов тайн (государственная, служебная, коммерческая, профессиональная и др.).
5. Терминологический аппарат, связанный с видами защиты информации.
6. Способы защиты информации: современные подходы и технологии.
7. Замысел и принципы защиты информации в корпоративных и государственных структурах.
8. Объекты защиты информации и критерии их выделения.
9. Современные угрозы информационной безопасности и их классификация.
10. Технические средства и оборудование защиты информации.
11. Национальная безопасность Российской Федерации: роль информационной составляющей.
12. Доктрина информационной безопасности Российской Федерации: цели, задачи, направления реализации.
13. Законодательная база обеспечения информационной безопасности в России.
14. Нормативные правовые акты, регулирующие обеспечение информационной безопасности.
15. Защита критически важной информационной инфраструктуры Российской Федерации.
16. Государственная система обеспечения информационной безопасности: структура и функционирование.
17. Несанкционированный доступ к информации: формы проявления и последствия.
18. Источники возникновения угроз информационной безопасности и их классификация.
19. Типовые непреднамеренные искусственные угрозы информационной безопасности.
20. Преднамеренные искусственные угрозы информационной безопасности: типы и способы воздействия.
21. Методы и средства выявления и нейтрализации несанкционированного доступа.
22. Атаки на коммуникационные протоколы: виды, сценарии и методы защиты.
23. Правовые меры противодействия угрозам информационной безопасности.
24. Организационно-технические мероприятия по защите информации.
25. Физические и инженерно-технические методы защиты информации.
26. Аутентификация субъектов информационных процессов: современные технологии и стандарты.
27. Имитостойкость и цифровая подпись: назначение, алгоритмы, области применения.
28. Симметричные и асимметричные криптосистемы: сравнительная характеристика и сферы применения.
29. Критерии и показатели стойкости криптографических шифров.

30. Методики и инструменты криптографического анализа защищённых коммуникаций.
31. Принципы разработки и функционирования криптографических протоколов.
32. Применение криптографических хэш-функций в обеспечении информационной безопасности.
33. Классификация и сравнительный анализ криптографических протоколов.
34. Цифровая электронная подпись: свойства, стандарты, область применения.
35. Протоколы аутентификации сообщений в современных телекоммуникационных системах.
36. Криптографические протоколы идентификации пользователей и устройств.
37. Правила разграничения прав доступа субъектов к объектам информации.
38. Процедуры идентификации, аутентификации и авторизации в автоматизированных системах.
39. Активный аудит и протоколирование событий информационной безопасности.
40. Статистические методы обнаружения вторжений и аномалий в компьютерных сетях.
41. Сигнатурные методы детектирования атак и их эффективность.
42. Дискреционное управление доступом: концепции, реализация, ограничения.
43. Мандатное управление доступом: принцип работы, преимущества и недостатки.
44. Ролевое управление доступом: организация, настройка, практика внедрения.
45. Средства и методы защиты информации при хранении и передаче.
46. Антивирусная защита и борьба с вредоносным ПО в корпоративных сетях.
47. Компьютерные вирусы и вредоносные программы: классификация, признаки, профилактика.
48. Защита межсетевого взаимодействия: межсетевые экраны и прокси-серверы.
49. Современные технологии предотвращения утечек конфиденциальной информации.
50. Аудит информационной безопасности организаций: цели, этапы, процедуры.
51. Анализ угроз корпоративной сети и построение эффективной защиты периметра.
52. Механизмы и компоненты комплексной защиты корпоративных информационных систем.
53. Межсетевое экранирование и фильтрация трафика: архитектура и технология.

1.3 Тестовые задания

1. Какая из перечисленных характеристик относится к триаде информационной безопасности?

а) Скорость, масштабируемость, доступность
б) Конфиденциальность, целостность, доступность (*Правильный ответ: б*)
в) Авторизация, аутентификация, шифрование
г) Надежность, резервирование, маршрутизация

2. Какова основная функция межсетевого экрана?

а) Шифрование трафика
б) Ускорение передачи данных
в) Фильтрация сетевого трафика (*Правильный ответ: в*)
г) Резервное копирование данных

3. Что из перечисленного является примером симметричного шифрования?

а) RSA
б) ECC
в) AES (*Правильный ответ: в*)
г) Diffie-Hellman

4. Какой тип атаки направлен на перегрузку сервера большим количеством запросов?

а) Phishing
б) Brute-force
в) DDoS (*Правильный ответ: в*)
г) Spoofing

5. Что такое хэш-функция?
а) Метод передачи данных по VPN
б) Функция, преобразующая данные в фиксированную строку (*Правильный ответ: б*)
в) Алгоритм сжатия данных без потерь
г) Способ шифрования с открытым ключом
6. В чём основное отличие аутентификации от авторизации?
а) Нет различий
б) Аутентификация определяет права доступа
в) Аутентификация подтверждает личность, авторизация определяет права (*Правильный ответ: в*)
г) Авторизация используется только в локальных сетях
7. Какой протокол используется для защищённой передачи данных в интернете?
а) FTP
б) HTTP
в) TLS/SSL (*Правильный ответ: в*)
г) DNS
8. Что такое VPN?
а) Антивирусная программа
б) Виртуальная частная сеть
в) Протокол маршрутизации (*Правильный ответ: б*)
г) Система обнаружения атак
9. Что делает IDS (Intrusion Detection System)?
а) Блокирует вирусы на сервере
б) Шифрует сетевой трафик
в) Обнаруживает подозрительную активность (*Правильный ответ: в*)
г) Ускоряет передачу данных
10. Какой порт по умолчанию используется для HTTPS?
а) 21
б) 80
в) 443 (*Правильный ответ: в*)
г) 25
11. Какие свойства относятся к информационной безопасности?
а) Конфиденциальность
б) Масштабируемость
в) Целостность
г) Доступность
Ответ: а, в, г.
12. Какие методы относятся к аутентификации пользователя?
а) Пароль
б) MAC-адрес
в) Биометрия
г) Шифрование трафика
Ответ: а, в.
13. Какие алгоритмы являются асимметричными?
а) AES
б) RSA
в) ECC
г) DES
Ответ: б, в.
14. Какие угрозы относятся к сетевым атакам?

а) DDoS
б) Phishing
в) SQL-инъекция
г) Дефрагментация диска
Ответ: а, б, в

15. Какие протоколы обеспечивают защищённую передачу данных?
а) HTTPS
б) FTP
в) TLS
г) SSH
Ответ: а, в, г.

16. Какие функции выполняет межсетевой экран (firewall)?
а) Фильтрация трафика
б) Шифрование файлов
в) Блокировка портов
г) Мониторинг пакетов
Ответ: а, в, г.

17. Какие из перечисленного являются криптографическими хэш-функциями?
а) MD5
б) SHA-256
в) RSA
г) SHA-1
Ответ: а, б, г.

18. Какие действия характерны для DDoS-атаки?
а) Перегрузка сервера запросами
б) Удаление файлов с сервера
в) Использование ботнета
Ответ: а, в.
г) Шифрование данных пользователя

19. Какие устройства/системы относятся к защите сети?
а) IDS
б) IPS
в) Firewall
г) Proxy-сервер
Ответ: а, б, в, г.

20. Какие действия относятся к социальной инженерии?
а) Фишинг
б) Подбор паролей
в) Подделка личности
г) Шифрование данных
Ответ: а, б, в.

21. Установить соответствие:

1. Firewall	А) Обнаружение вторжений в сеть
2. IDS	Б) Защищенный туннель поверх

	интернета
3. VPN	В) Фильтрация сетевого трафика
4. DDos	Г) Массовая перегрузка сервера запросами

22. Установить соответствие:

1. Конфиденциальность	А) Проверка подлинности пользователя
2. Целостность	Б) Защита от несанкционированного доступа
3. Доступность	В) Данные не изменяются без разрешения
4. Аутентификация	Г) Возможность доступа к ресурсам

23. Установить соответствие:

1. RSA	А) Хэш-функция
2. AES	Б) Симметричный алгоритм
3. SHA-256	В) Асимметричный алгоритм
4. ECC	Г) Криптография на эллиптических кривых

24. Установить соответствие:

1. Фишинг	А) Взлом через базу данных
2. Социальная инженерия	Б) Психологическое воздействие на пользователя
3. Brute-force	В) Подбор пароля перебором
4. SQL-инъекция	Г) Поддельные сайты для кражи данных

25. Установить соответствие:

1. HTTPS	А) Протокол передачи файлов
2. SSH	Б) Защищенные веб-протокол
3. FTP	В) Протокол удаленного доступа
4. DNS	Г) Система доменных имен

26. Установить соответствие:

1. Хэш-функция	А) Обратное преобразование зашифрованных данных
2. Шифрование	Б) Преобразование данных в уникальный отпечаток

3. Кодирование	В) Защита информации от чтения без ключа
4. Дешифрование	Г) Представление данных в другом формате

27. Установить соответствие:

1. Proxy-server	А) Маршрутизация сетевых пакетов
2. Firewall	Б) Маскировка IP-адресов
3. NAT	В) Промежуточный сервер
4. Router	Г) Фильтрация трафика

28. Установить соответствие:

1. Malware	А) Саморастространяющийся вирус
2. Trojan	Б) Вредоносное ПО в целом
3. Worm	В) Вирус с маскировкой под полезную программу
4. Ransomware	Г) Вирус, шифрующий данные

29. Установить соответствие:

1. SSL/TLS	А) Протокол защищенной передачи
2. IPsec	Б) Защита сетевого уровня
3. VPN	В) Туннелирование трафика
4. HTTPS	Г) Защищенный HTTP

30. Установить соответствие:

1. Логирование	А) Анализ событий безопасности
2. Мониторинг	Б) Запись событий системы
3. Аудит	В) Наблюдение за состоянием сети
4. Система IDS	Г) Обнаружение атак

1.4 Практические задания

Практическое задание № 1.

Изучение программных средств защиты от несанкционированного доступа.

1. Запустить программы просмотра и редактирования реестра Windows regedit.exe и regedt32.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра.

1.1. Включить в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE).

1.2. Включить в отчет сведения о различиях в функциональных возможностях изученных программ редактирования реестра (если лабораторная работа выполняется в операционной системе Windows).

Примечание: в операционную систему Windows XP Professional включен один редактор реестра, который можно запустить с помощью любого из указанных выше имен.

Практическое задание № 2.

Средства безопасности в ОС Windows.

1. Создайте на диске C:\Темп папку и скопируйте в нее любой файл.
2. Зашифруйте файл вместе с папкой таким образом, чтобы все помещаемые в папку файлы тоже шифровались (если шифрование не удалось-дальнейшие действия с папкой делайте как с зашифрованной).
3. Создайте на рабочем столе папку с вашей фамилией и добавьте в неё резервную копию зашифрованной вами папки (сохраняя шифрование).
4. Установите оснастку Сертификаты.
5. Создайте резервную копию вашего сертификата и поместите ее в вашу папку на рабочем столе.

Практическое задание № 3.

Обеспечения безопасности хранения данных в ОС Windows.

Задание 1. Выполнение архивации

В этом задании с помощью программы Backup вы выполните полную, а затем добавочную архивацию. Вы также научитесь создавать задания для программы архивации, которые будут выполняться по расписанию.

1. В папке C:\Темп:\Документы создайте три текстовых документа с произвольным содержимым, например, Отчет . txt, Планы.txt и Заказы.txt.
2. В проводнике Windows выберите режим просмотра содержимого папки D:\ Документы в виде таблицы (Меню «Вид» / «Таблица»). Обратите внимание, что в столбце «Атрибуты» у всех трех файлов установлен атрибут «архивный» (бит архива обозначается буквой «А»).
3. Выберите «Пуск» / «Программы» / «Стандартные» / «Служебные» / «Архивация данных». Программа Backup Windows первый раз запускается в режиме мастера. На первой странице мастера (см. рис. 4.5) снимите флажок «Всегда запускать в режиме мастера» и нажмите на ссылку «Расширенный режим». Запустится программа архивации. Перейдите на вкладку «Архивация».
4. В меню «Задание» выберите команду «Создать». Раскройте узел «Мой компьютер», диск C:\, папка «Документы». Установите флажок напротив папки «Документы». Внизу, в поле «Носитель архива или имя файла» введите имя будущего архива -например C : \doc-normal. bkf.
5. Нажмите кнопку «Архивировать». Откроется окно «Сведения о задании архивации». В разделе «Если носитель уже содержит архивы» оставьте переключатель «Дозаписать этот архив к данным носителя».
6. Нажмите кнопку «Дополнительно». Убедитесь, что выбран тип архива «Обычный» и установите флажок «Проверка данных после архивации». Нажмите кнопку «ОК», а затем «Архивировать».
7. Откроется диалоговое окно «Ход архивации», и начнется процесс архивации. По завершении создания архива нажмите кнопку «Отчет» и посмотрите отчет. В нем не

должно быть ошибок архивации. Закройте отчет и окно «Ход архивации». Не закрывайте программу Backup Windows.
8. Обратите внимание, что в папке C:\Документы теперь у всех файлов снят атрибут «архивный». Откройте файл Планы. txt и добавьте новую строку с текущей датой. Сохраните и закройте файл. Обратите внимание, что после внесения изменений в файл атрибут «архивный» автоматически устанавливается операционной системой.
9. Вернитесь к программе Backup Windows на вкладку «Архивация». В меню «Задание» выберите команду «Создать».
10. Раскройте узел «Мой компьютер», диск C:\, папка «Документы». Установите флажок напротив папки «Документы».
11. Внизу, в поле «Носитель архива или имя файла» введите имя добавочного архива- например C: \doc-inc.bkf.
12. Нажмите кнопку «Архивировать». Откроется окно «Сведения о задании архивации».
13. Нажмите кнопку «Дополнительно». Выберите тип архива «добавочный» и установите флажок «Проверка данных после архивации». Нажмите кнопку «ОК».
14. Теперь кнопку «Расписание». Появится диалоговое окно, которое предложит вам сохранить заданные параметры, перед установкой архивации по расписанию. Нажмите кнопку «Да».
15. Сохраните набор ваших файлов под именем documents . bks.
16. В окне «Указание учетной записи» введите свой пароль и нажмите кнопку «ОК».
17. В появившемся окне «Параметры запланированного задания» введите имя задания - «Ежедневный добавочный архив».
18. Затем нажмите кнопку «Свойства».
19. Откроется окно «Запланированное задание», вкладка «Расписание». В выпадающем списке «Назначить задание» выберите вариант «ежедневно» и установите время начала на три минуты вперед от текущего времени, чтобы увидеть результат выполнения задания. Нажмите кнопку «ОК».
20. Введите повторно свой пароль и нажмите кнопку «ОК».
21. В окне «Параметры запланированного задания» также нажмите «ОК».
22. Перейдите на вкладку «Запланированные задания» программы архивации Backup и убедитесь, что ваше задание «Ежедневный добавочный архив» появилось в расписании (Каждый день, начиная с текущего).
23. Закройте программу Backup. Дождитесь наступления времени установленного вами на запуск задания архивации. Вы увидите как запустится по расписанию программа Backup. После ее выполнения на диске E появится добавочный архив doc-inc. bkf.
24. Запустите программу Backup. В меню «Сервис» выберите «Отчет». появится окно со списком отчетов архивации. Выберите последний и откройте его.
25. Сравните полученный отчет с предыдущим.
26. Закройте все окна программы Backup. Обратите внимание, что в папке C:\Документы опять у всех файлов снят атрибут «архивный».
27. Удалите папку «Документы» со всеми файлами.

Задание 2. Восстановление данных

В этом задании с помощью программы Backup вы восстановите данные ранее заархивированные.

1. Запустите программу Backup и перейдите на вкладку «Восстановление и управление носителем». В левом окне щелкните на узел «Файлы», чтобы раскрыть его. Выберите архив doc-normal. bkf.
2. Раскройте архив doc-normal .bkf и установите флажок напротив папки «Документы». Восстановим эту папку в ее исходное размещение. По умолчанию задан такой параметр снизу в выпадающем списке «Восстановить файлы в:».
3. Нажмите кнопку «Восстановить». В диалоговом окне «Подтверждение восстановления» нажмите кнопку «ОК».
4. В окне «Проверка расположения архивного файла» также нажмите кнопку «ОК».
5. После завершения восстановления закройте окно «Ход восстановления», нажав кнопку «Закрыть». Не закрывайте программу Backup Windows.
6. Убедитесь, что папка «Документы» со всеми файлами восстановлена в прежнее место на диск C:\. Откройте файл Планы. txt и убедитесь, что он не содержит последнюю строку текста с текущей датой.
7. Вернитесь в программу Backup на вкладку «Восстановление и управление носителем».
8. В левом окне щелкните и раскройте архив doc-inc.bkf и установите флажок напротив папки «Документы», в которой содержится один файл Планы. txt. По умолчанию программа Backup не заменяет существующие файлы с одинаковым именем. Поэтому необходимо сделать следующую настройку.
9. В меню «Сервис» выберите пункт «Параметры» и перейдите на вкладку «Восстановление». На этой вкладке переключитесь на вариант «Заменять файл на компьютере, только если он старее» и нажмите кнопку «ОК».
10. Нажмите кнопку «Восстановить». В диалоговом окне «Подтверждение восстановления» нажмите кнопку «ОК».
12. Если появится окно «Проверка расположения архивного файла», то так же нажмите кнопку «ОК».
13. После завершения восстановления закройте окно «Ход восстановления», нажав кнопку «Закрыть».
14. Закройте программу Backup Windows.
15. Убедитесь, что восстановлена последняя версия файла Планы. txt.

Задание 3. Архивация и восстановление данных при использовании программ архивации данных

В этом упражнении с помощью программы WinRar вы заархивируете данные и защитите архив паролем.

1. Создайте документ на диски С в папке Temp.
2. Загрузите программу - архиватор WinRar.
3. Перейдите в среде архиватора в созданную вами папку.
4. Создайте архив в вашей папке.
5. Перейдите на вкладку Дополнительно в среде архиватора. Выберите Установить пароль, задайте и подтвердите пароль.
6. Проверьте парольную защиту архива.

Практическое задание № 4.

Защита баз данных.

Задание

1. Создать новую базу данных и создать в ней следующие объекты:

Таблицу Заказы;
Запрос Сведения о заказах;
Форму Заказы клиентов.
Заполнить таблицу несколькими записями.
2. Определить два уровня доступа к БД:
на уровне пароля;
на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Практическое задание № 5.

Средства безопасности ASP_NET. Аутентификация.
В рамках среды ASP.NET предоставлены 3 вида аутентификации:
Аутентификация Windows
Формой
Паспортом

Практическое задание № 6.

Разработка простых криптографических алгоритмов на основе методы замены.
В соответствии со своим вариантом разработать программу для шифрования русскоязычного текста при помощи шифра подстановки. Программы должны обеспечивать:
- шифрование информации, находящейся в текстовом файле, с записью результата в другой файл;
- шифрование информации, вводимой с клавиатуры, с выводом только шифр - текста;

Практическое задание № 7.

Разработка простых криптографических алгоритмов на основе метода перестановки.
Варианты заданий:
1. Вывести сообщение с права на лево.
2. Простая шифрующая таблица перестановки.
3. Одиночная перестановка оп ключу.
4. Двойная перестановка по ключу.

Практическое задание № 8.

Шифрование информации с использованием стандарта DES.
Задание 1.
Создание нового Web –приложения
1. Запустите Visual Studio и откройте пункт меню File.
2. В контекстном меню выберите New щелкните на Web Site. Когда вы выбираете этот значок, Visual Studio подготавливает среду разработки и файлы вашей программы для интернет-программирования. Создание нового проекта веб-приложения ASP.NET аналогично созданию проекта Windows Application. Однако текстовое поле Name (Имя) отключено, а текстовое поле Location (Расположение) предназначено для другого типа установки. В среде веб-приложения вам предлагается указать веб-сервер для вашего проекта или принять значение по умолчанию http://localhost**.** При создании проекта вы можете выбрать для него локальный или удаленный веб-сервер (на котором установлены .NET Framework и файлы поддержки), и Visual Studio будет использовать указанный веб-сервер для

размещения и организации файлов вашего проекта. Веб-сервер определяется не с помощью имен диска и папки, а с помощью корректного адреса в интернете (URL).

Создание Web – формы

Как отмечалось ранее, Web Forms хранится в файле .aspx. В нашем случае это будет default.aspx. Для создания интерфейса мы можем:

1. оставаться в окне редактора кода и формировать интерфейс с использование стандартных html-тэгов
2. перейти в режим конструктора и наполнить форму необходимыми компонентами.

Практическое задание № 9.

Шифрование информации с использованием стандарта RSA.

Для выполнения работы, как и в предыдущей лабораторной работе мы создадим новое Web - приложение.

Для создания интерфейса:

1. оставаться в окне редактора кода и формировать интерфейс с использование стандартных html-тэгов
2. перейти в режим конструктора и наполнить форму необходимыми компонентами.

При использовании второго метода заполнения необходимо перейти в режим конструктора и перетащить на форму компоненты Button и 3 текстовых поля.

Отредактируйте свойства этих компонентов в соответствии со следующим кодом (для просмотра редактора перейдем в соответствующее окно кода нажав кнопку Sourse)

Практическое задание № 10.

Антивирусные программы.

Задания:

1. Программы-шпионы. Защита от программ шпионов.
2. Троянские программы.
3. "Черви", методики проникновения.
4. Вирусы, алгоритмы работы.
5. Антивирусное программное обеспечение: рекомендуемые настройки, правила использования.

Практическое задание № 11.

Работа в К+. Международные, российские и отраслевые правовые документы.

1. Найдите действующий закон об авторском праве. Найдите статьи, касающиеся защиты авторских прав.
2. Сделайте выдержку из документа с указанием полного названия документа и статей о защите авторских прав.
3. Какие средства массовой информации являются официальными источниками опубликования указов и распоряжений Президента РФ?

Практическое задание № 12.

Работа в К+. Концепция правового обеспечения информационной безопасности РФ.

1. Найдите ПРОЕКТ КОНЦЕПЦИИ Совета безопасности Российской Федерации по «Информационной безопасности Российской Федерации».
2. Сделайте выдержку из документа о «Роли и месте информационной безопасности в общей системе национальной безопасности Российской Федерации»

Практическое задание № 13.

Работа в К+. Международные правовые акты по защите информации.

1. Найти

- Закон об информационной безопасности" (Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988г.
- Законопроект "О совершенствовании информационной безопасности" (Computer Security Enhancement Act of 1997, H.R. 1903), направленный на усиление роли Национального института стандартов и технологий и упрощение операций с криптосредствами.

Практическое задание № 14.

Работа в К+. Международные акты информационной безопасности.

1. Найдите действующий закон об информации, информационных технологиях и о защите информации» от 2006 г. № 149-ФЗ (новая редакция 2010 г.)
2. Сделайте выдержку из документа с указанием полного названия документа и статей о защите информации.
3. ФЗ РФ «О государственной тайне» от 21.06.1993 г. № 5485-1 - регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ.

Практическое задание № 15.

Работа в К+. Федеральный закон «Об информации, информационных технологиях и о защите информации».

1. Найти статью Закона о принципах правового регулирования отношений в сфере информации, информационных технологий и защиты информации.
2. Сделайте выдержку из документа с указанием полного названия документа и статей о защите информации.
3. Проработать статью об ограничение доступа к информации.

2. КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОВЕДЕНИИ ТЕКУЩЕГО КОНТРОЛЯ

Вид контроля	Наименование работы	Наименование оценочных средств	Шкала оценивания
Текущий контроль	- Вопросы для обсуждения на занятиях; - Устные опросы по ранее изученному материалу; - Письменные работы: рефераты, тестовые задания; - Практические задания; - Рефераты и доклады по темам (вопросам), вынесенным на самостоятельную работу.	Оценка выступлений на практическом (семинарском) занятии, проверка заданий и аудиторных работ, устный опрос, оценивание докладов, рефератов	отлично хорошо удовлетворительно неудовлетворительно

Критерии оценивания устных ответов обучающихся

Шкала оценивания	Характеристика оценивания
отлично	оценивается ответ, который показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и

	полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа.
хорошо	оценивается ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.
удовлетворительно	оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа.
неудовлетворительно	оценивается ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа.

Критерии оценивания работы обучающихся на практических и семинарских занятиях

Шкала оценивания	Показатели	Критерии
Отлично	1. Полнота выполнения практического и тестового задания (полнота ответа); 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения практического задания (логичность и четкость ответа); 4. Правильность ответов на вопросы; 5. Самостоятельность решения (владение	Задание решено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе формул и решении нет ошибок, получен верный ответ, задание решено рациональным способом. Дан правильный и исчерпывающий ответ на поставленные теоретические и тестовые вопросы, в которых обучающийся показал всестороннее системное знание программного материала, усвоение основной и дополнительной литературы, четкое владение понятийным аппаратом.
Хорошо		Задание решено с помощью преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задание решено нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ. На поставленные теоретические и тестовые вопросы,

Шкала оценивания	Показатели	Критерии
	дополнительным материалом); 6. Знание нормативно-законодательной базы и терминологии курса	при которых обучающийся показал достаточный уровень знаний основного программного материала: освоение информации лекционного курса и учебных пособий, овладение понятийным аппаратом, методикой исследований при попытке анализа различных ситуаций.
Удовлетворительно		Задание решено с подсказками преподавателя. Задание решено в общем виде. Обучающийся показал средний уровень знаний основного программного материала, но не мог убедительно аргументировать свой ответ, ошибся в использовании понятийного аппарата, показал недостаточные знания литературных источников.
Неудовлетворительно		Задание не решено. Обучающийся продемонстрировал значительные пробелы в знаниях основного программного материала, не аргументировал свой ответ, показал неудовлетворительные знания понятийного аппарата и специальной литературы.

Критерии оценивания рефератов

Средство контроля	Критерии оценивания	Шкала оценивания
Реферат	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. Реферат раскрывает поднятую проблематику в полном объеме.	отлично
	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы. В реферате имеются неточности и предметная область выступления раскрыта не в полной мере.	хорошо
	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. В реферате не в полной степени раскрыт понятийный аппарат, имеются существенные неточности в процессе формирования выводов.	удовлетвори-тельно
	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Тема реферата не раскрыта или выполнена не по существу ранее	неудовлетво-рительно

	поставленного вопроса. Реферат не сдан / доклад не сделан.	

Критерии оценивания тестов

Средство контроля	Критерии оценивания – процент положительных ответов	Шкала оценивания
Тестирование	90-100	отлично
	70-89	хорошо
	40-69	удовлетворительно
	< 39	неудовлетворительно

3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Средства оценивания в ходе промежуточной аттестации:
– вопросы для зачета с оценкой;
– тестовые задания к зачету с оценкой.

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знать: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.2. Уметь: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. ОПК-4.3. Владеть: составления технической документации на различных этапах жизненного цикла информационной системы
ОПК-7	Способен участвовать в настройке и наладке программно-аппаратных комплексов	ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть: навыками проверки работоспособности программно-аппаратных комплексов

3.1. Вопросы к зачету с оценкой

1. Уровни представления информации.
2. Свойства защищаемой информации.
3. Виды тайн (государственная, служебная, профессиональная,...).
4. Термины, относящиеся к видам защиты информации.
5. Термины, относящиеся к способам защиты информации.
6. Термины, относящиеся к замыслу защиты информации.
7. Термины, относящиеся к объекту защиты информации.
8. Термины, относящиеся к угрозам безопасности информации.

9. Термины, относящиеся к технике защиты информации.
10. Национальная безопасность РФ.
11. Доктрина информационной безопасности РФ.
12. Законодательная основа обеспечения информационной безопасности.
13. Нормативная основа обеспечения информационной безопасности.
14. Безопасность критической информационной инфраструктуры РФ.
15. Государственная система обеспечения информационной безопасности.
16. Несанкционированные операции с информацией.
17. Источники и классификация угроз.
18. Перечень типовых непреднамеренных искусственных угроз.
19. Перечень типовых преднамеренных искусственных угроз.
20. Классификация способов несанкционированного доступа.
21. Типовые атаки на коммуникационные протоколы.
22. Законодательные меры противодействия угрозам безопасности.
23. Организационные меры противодействия угрозам безопасности.
24. Физические и технические меры противодействия угрозам безопасности.
25. Аутентификация. Невозможность отказа от авторства.
26. Имитозащита. Цифровая подпись.
27. Симметричный / асимметричный шифр.
28. Криптографическая стойкость шифра.
29. Метод криптографического анализа.
30. Криптографический протокол.
31. Криптографическая хеш-функция.
32. Классификация крипто-протоколов.
33. Свойства цифровой подписи.
34. Криптографические протоколы аутентификации сообщений.
35. Криптографические протоколы идентификации.
36. Объект, субъект, доступ к информации, правила разграничения доступа.
37. Идентификация, аутентификация, авторизация.
38. Протоколирование и аудит (активный аудит).
39. Статистический метод обнаружения атак.
40. Сигнатурный метод обнаружения атак.
41. Дискреционное управление доступом.
42. Мандатное управление доступом.
43. Ролевое управление доступом.
44. Защита информации при хранении и передаче.
45. Защита от вредоносных программ.
46. Виды компьютерных вирусов и вредоносных программ.
47. Защита межсетевого взаимодействия.
48. Предотвращение утечек информации.
49. Аудит безопасности.
50. Угрозы корпоративной сети. Защита периметра сети.
51. Основные механизмы защиты корпоративной сети.
52. Средства защиты информации: межсетевые экраны.
53. Средства защиты информации: виртуальные частные сети.
54. Средства защиты информации: системы анализа защищённости.
55. Средства защиты информации: системы обнаружения атак.
56. Системы предотвращения утечки конфиденциальной информации.

57. Политика информационной безопасности организации.

3.2. Задания для зачета:

Задание 1

Опишите модель CIA-триады и приведите по одному примеру нарушения каждого свойства в сети.

Задание 2

Сравните аутентификацию и авторизацию на примере веб-сервиса.

Задание 3

Опишите различия симметричного и асимметричного шифрования.

Задание 4

Объясните, почему хэширование нельзя использовать для восстановления данных.

Задание 5

Приведите примеры угроз конфиденциальности в локальной сети.

Задание 6

Зашифруйте сообщение простым методом (например, сдвиг Цезаря) и объясните принцип.

Задание 7

Опишите процесс работы RSA на концептуальном уровне.

Задание 8

Объясните, зачем используется соль (salt) при хранении паролей.

Задание 9

Сравните MD5 и SHA-256 по безопасности.

Задание 10

Объясните, что такое цифровая подпись и где она применяется.

Задание 11

Проанализируйте сценарий DDoS-атаки и предложите способы защиты.

Задание 12

Опишите механизм фишинга и признаки его обнаружения.

Задание 13

Разберите пример SQL-инъекции и принцип её предотвращения.

Задание 14

Объясните, как работает brute-force атака.

Задание 15

Опишите последствия MITM-атаки (man-in-the-middle).

Задание 16

Сравните HTTP и HTTPS с точки зрения безопасности.

Задание 17

Опишите назначение TLS/SSL.

Задание 18

Объясните принцип работы VPN.

Задание 19

Разберите структуру защищённого SSH-сеанса.

Задание 20

Опишите роль DNS и возможные атаки на него.

Задание 21

Объясните функции firewall в корпоративной сети.

Задание 22

Сравните IDS и IPS.

Задание 23

Опишите работу proxy-сервера.

Задание 24

Объясните роль NAT в безопасности сети.

Задание 25

Опишите архитектуру защищённой корпоративной сети.

Задание 26

Разберите пример утечки данных и предложите меры предотвращения.

Задание 27

Составьте план реагирования на инцидент безопасности.

Задание 28

Опишите процесс расследования сетевой атаки.

Задание 29

Определите возможные источники компрометации учётной записи.

Задание 30

Разработайте базовую политику безопасности для учебной сети.

4. ОСНОВНЫЕ КРИТЕРИИ ОЦЕНИВАНИЯ ПРИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Шкала оценивания уровня сформированности универсальной компетенций (зачет с оценкой)

Формируемые уровни освоения компетенций	Критерии оценивания	Шкала оценивания
Высокий уровень	Изложено правильное понимание вопроса, четко и самостоятельно дан исчерпывающий ответ, содержание раскрыто полно, профессионально, грамотно. Обучающимся усвоена взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии. Отражает успешное и систематическое применение навыков и умений по данной дисциплине в соответствии с ФГОС.	отлично
Базовый уровень	Изложено правильное понимание вопроса, дано достаточно подробное описание предмета ответа, приведены и раскрыты в тезисной форме основные понятия, относящиеся к предмету ответа. Ответ отражает полное знание учебно-программного материала, систематический характер знаний по дисциплине, а также наличие базового уровня овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС	хорошо
Пороговый уровень	Ответ отражает теоретические знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии. Данная оценка может быть выставлена обучающемуся, допустившему неточности в ответе, но обладающими необходимыми	удовлетвори тельно

	знаниями для их устранения под руководством преподавателя, отмечен начальный уровень овладения практическими умениями и навыками по данной дисциплине в соответствии с ФГОС	
Неудовлетворительный уровень	При ответе обучающегося обнаружено отсутствие знаний, умений и навыков и/или фрагментарные знания основного учебно-программного материала.	неудовлетворительно

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущей и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет с оценкой.

Форма проведения промежуточной аттестации – письменный зачет.