УТВЕРЖДЕНО
Постановление
Министерства образования
Республики Беларусь
09.06.2022 № 144

ТИПОВАЯ УЧЕБНАЯ ПРОГРАММА ПО УЧЕБНОЙ ДИСЦИПЛИНЕ ”ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ“

профессионального компонента типового учебного плана по специальности 2-40 01 01 ”Программное обеспечение информационных технологий“ для реализации образовательной программы среднего специального образования, обеспечивающей получение квалификации специалиста со средним специальным образованием

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая типовая учебная программа по учебной дисциплине ”Защита компьютерной информации“ (далее – программа) предусматривает изучение современных методов и алгоритмов защиты компьютерной информации в информационных системах различного назначения, развитие профессиональной компетентности в области разработки, анализа и эксплуатации средств защиты компьютерной информации, приобретение практических навыков криптографической защиты.

В процессе преподавания учебной дисциплины ”Защита компьютерной информации“ необходимо учитывать междисциплинарные связи программного учебного материала с такими учебными дисциплинами типового учебного плана по специальностям, как ”Математика“, ”Теория вероятностей и математическая статистика“, ”Инструментальное программное обеспечение“, ”Основы алгоритмизации и программирования“, ”Арифметико-логические основы вычислительной техники“.

В ходе изложения программного учебного материала следует руководствоваться актами законодательства, регламентирующими область профессиональной деятельности, соблюдать единство терминологии и обозначений.

Для закрепления теоретического материала и формирования у учащихся необходимых умений настоящей программой предусматривается проведение лабораторных занятий.

В целях контроля усвоения программного учебного материала предусмотрено проведение одной обязательной контрольной работы, задания для которой разрабатываются преподавателем учебной дисциплины ”Защита компьютерной информации“ и обсуждаются на заседании предметной (цикловой) комиссии учреждения образования.

Настоящей программой определены цели изучения каждой темы, спрогнозированы результаты их достижения в соответствии с уровнями усвоения учебного материала.

В результате изучения учебной дисциплины ”Информационные технологии“ учащиеся должны:

знать на уровне представления:

акты законодательства в области безопасности информации;

концепцию адаптивного управления безопасностью;

проблемы обеспечения безопасности операционных систем;

методы и средства защиты от удаленных атак через глобальную компьютерную сеть Интернет (далее – сеть Интернет);

особенности функционирования межсетевых экранов;

особенности защиты информации в электронных платежных системах;

знать на уровне понимания:

алгоритмы блочного шифрования;

алгоритмы асимметричного шифрования;

алгоритмы электронной цифровой подписи (далее – ЭЦП);

алгоритмы идентификации и проверки подлинности;

уметь:

шифровать данные классическими криптосистемами;

осуществлять проверку подлинности пользователей с помощью упрощенной и параллельной схем идентификации с нулевой передачей знаний;

применять ЭЦП;

скрывать информацию на персональном компьютере;

создавать виртуальные зашифрованные диски;

использовать программное обеспечение (далее – ПО) для блокировки или ограничения доступа к программам, файлам, элементам управления и к компьютеру в целом.

В настоящей программе приведены примерные критерии оценки результатов учебной деятельности учащихся по учебной дисциплине ”Защита компьютерной информации“, разработанные на основе десятибалльной шкалы и показателей оценки результатов учебной деятельности учащихся в учреждениях среднего специального образования; примерный перечень оснащения кабинета оборудованием, техническими и демонстрационными средствами обучения, необходимыми для обеспечения образовательного процесса.

Приведенный в настоящей программе тематический план является рекомендательным. При необходимости внесения изменений в настоящую программу учреждение образования, реализующее образовательные программы среднего специального образования, разрабатывает на ее основе учебную программу учреждения образования. Предметная (цикловая) комиссия учреждения образования может вносить обоснованные изменения в содержание и последовательность изложения программного учебного материала, распределение учебных часов по темам в пределах общего бюджета времени, отведенного на изучение учебной дисциплины ”Защита компьютерной информации“. Учебная программа учреждения образования утверждается его руководителем.

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

Раздел, тема	Количество учебных часов	
	всего	в том числе на лабораторные занятия
Введение	**1**	
Раздел I. **Защита информации в информационно-вычислительных системах**	**3**	
1.1. Проблемы защиты компьютерной информации	1	
1.2. Угрозы безопасности информации в информационно-вычислительных системах	2	
Раздел II. **Криптографическая защита информации**	**32**	**18**
2.1. Принципы криптографической защиты информации	2	
2.2. Классические симметричные криптосистемы	10	6
2.3. Современные симметричные криптосистемы	12	8
2.4. Асимметричные криптосистемы	8	4
Раздел III. **Идентификация и проверка подлинности**	**12**	**4**
3.1 Основные понятия и концепции идентификации и аутентификации пользователей	2	
3.2 Взаимная проверка подлинности пользователей	10	4
Раздел IV. **Электронная цифровая подпись**	**16**	**8**
4.1. Понятие электронной цифровой подписи	2	
4.2. Однонаправленные хеш-функции	2	
4.3. Алгоритмы электронной цифровой подписи	12	8
Раздел V. **Системы защиты программных средств**	**14**	**6**
5.1. Подходы к организации разграничения доступа к информации в компьютерных системах. Защита компьютера от несанкционированного доступа к информации	2	
5.2. Шифрование данных с использованием программного средства PGP	2	
5.3. Использование программного обеспечения для шифрования / дешифрования файлов, дисков	10	6
Раздел VI. **Политика безопасности**	**4**	
6.1. Правовое регулирование в области безопасности информации. Организационные методы защиты	2	

Раздел, тема	Количество учебных часов	
	всего	в том числе на лабораторные занятия
6.2. Структура политики безопасности организации	2	
Раздел VII. **Особенности построения систем защиты информации в информационных системах различного типа**	**14**	**4**
7.1. Адаптивное управление безопасностью. Анализ защищенности	2	
7.2. Технология обнаружения атак	6	4
7.3. Безопасность работы в глобальной компьютерной сети Интернет	1	
Обязательная контрольная работа	1	
7.4. Особенности защиты информации в системах электронного документооборота	4	
Итого	**96**	**40**

СОДЕРЖАНИЕ ПРОГРАММЫ

Цель обучения	Содержание темы	Результат обучения
	Введение	
Ознакомить с целями и задачами учебной дисциплины ”Защита компьютерной информации“, ее связью с другими учебными дисциплинами, значением в системе подготовки техника-программиста. Дать представление о роли защиты компьютерной информации в развитии информационных технологий.	Цели и задачи учебной дисциплины ”Защита компьютерной информации“, ее связь с другими учебными дисциплинами, значение в формировании профессиональных компетенций техника-программиста. Развитие защиты компьютерной информации.	Называет цели и задачи учебной дисциплины ”Защита компьютерной информации“, высказывает общее суждение о ее связи с другими учебными дисциплинами, значении в формировании профессиональных компетенций техника-программиста. Различает роль защиты компьютерной информации в развитии информационных технологий.
	Раздел I. **Защита информации в информационно-вычислительных системах**	
	Тема 1.1. **Проблемы защиты компьютерной информации**	
Сформировать представление об информационной безопасности, актуальности ее обеспечения. Ознакомить с основными задачами информационной безопасности и защиты информации.	Информационная безопасность компьютерных систем. Актуальность проблемы обеспечения информационной безопасности. Задачи защиты информации. Задачи информационной безопасности.	Высказывает общее суждение об информационной безопасности, актуальности ее обеспечения. Называет основные задачи информационной безопасности и защиты информации.
	Тема 1.2. **Угрозы безопасности информации в информационно-вычислительных системах**	
Сформировать знания о сущности угрозы информационной безопасности, классификации угроз, об основных методах реализации угроз, этапах осуществления атаки на информационную систему, о способах борьбы с атаками.	Сущность угрозы информационной безопасности. Классификация угроз информационной безопасности. Статистика по угрозам. Основные методы реализации угроз информационной безопасности. Этапы осуществления атаки на	Раскрывает сущность угрозы информационной безопасности. Излагает классификацию угроз. Описывает основные методы реализации угроз, этапы осуществления атаки на информационную систему, способы

Цель обучения	Содержание темы	Результат обучения
	информационную систему. Способы борьбы с атаками.	борьбы с атаками.
РАЗДЕЛ II. **КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ**		
Тема 2.1. **Принципы криптографической защиты информации**		
Сформировать знания о сущности и видах криптосистем. Дать представление о видах криптоаналитических атак, об аппаратно-программных средствах защиты информации.	Криптосистемы: сущность, виды. Криптоаналитические атаки, их виды. Аппаратно-программные средства защиты информации.	Раскрывает сущность и описывает виды криптосистем. Называет виды криптоаналитических атак, аппаратно-программные средств защиты информации.
Тема 2.2. **Классические симметричные криптосистемы**		
Сформировать знания об особенностях классических симметричных методов шифрования.	Классические симметричные методы шифрования. Шифрование методами перестановки: простая перестановка, одиночная перестановка по ключу, двойная перестановка, магический квадрат. Шифрование методами замены: шифр Цезаря, шифр Цезаря с ключевым словом, аффинная система подстановок Цезаря, система Трисемуса. Шифры сложной замены: системы Вижинера, Плейфера и шифра ”двойной квадрат“ Уитстона. Шифрование методом гаммирования. Потоковые шифры.	Раскрывает особенности классических симметричных методов шифрования.
	Лабораторная работа № 1	
Обучить шифрованию исходного текста и дешифрованию шифротекста методами шифрующих таблиц и	Шифрование методами шифрующих таблиц и магического квадрата.	Выполняет шифрование исходного текста и дешифрование шифротекста методами шифрующих таблиц и

Цель обучения	Содержание темы	Результат обучения
магического квадрата. Научить разрабатывать программу на языке программирования.		магического квадрата. Разрабатывает программу на языке программирования.
	Лабораторная работа № 2	
Обучить шифрованию исходного текста и дешифрованию шифротекста с использованием шифров простой перестановки. Научить разрабатывать программу на языке программирования.	Шифрование с использованием шифров простой перестановки.	Выполняет шифрование исходного текста и дешифрование шифротекста с использованием шифров простой перестановки. Разрабатывает программу на языке программирования.
	Лабораторная работа № 3	
Обучить шифрованию исходного текста и дешифрованию шифротекста с использованием шифров сложной перестановки. Научить разрабатывать программу на языке программирования.	Шифрование с использованием шифров сложной перестановки.	Выполняет шифрование исходного текста и дешифрование шифротекста с использованием шифров сложной перестановки. Разрабатывает программу на языке программирования.
Тема 2.3. **Современные симметричные криптосистемы**		
Сформировать понятие об общих принципах построения современных симметричных криптосистем, особенностях блочных шифров, алгоритмах криптографического преобразования симметричных блочных шифров.	Общие принципы построения современных симметричных криптосистем. Общая характеристика блочных шифров. Алгоритмы криптографического преобразования симметричных блочных шифров.	Излагает общие принципы построения современных симметричных криптосистем. Объясняет особенности блочных шифров. Описывает алгоритмы криптографического преобразования симметричных блочных шифров.
	Лабораторная работа № 4	
Обучить программной реализации алгоритма получения ключей для	Реализация алгоритма получения ключей для криптосистемы DES.	Выполняет программную реализацию алгоритма получения

Цель обучения	Содержание темы	Результат обучения
криптосистемы DES.		ключей для криптосистемы DES.
Обучить программной реализации алгоритма шифрования для криптосистемы DES.	Лабораторная работа № 5 Реализация функции шифрования для криптосистемы DES.	Выполняет программную реализацию алгоритма шифрования для криптосистемы DES.
Обучить программной реализации алгоритма получения ключей для симметричного блочного шифра.	Лабораторная работа № 6 Реализация функции нахождения ключей для алгоритма криптографического преобразования симметричного блочного шифра.	Выполняет программную реализацию алгоритма получения ключей для симметричного блочного шифра.
Обучить программной реализации алгоритма шифрования для симметричного блочного шифра.	Лабораторная работа № 7 Реализация элементов схемы шифрования симметричного блочного шифра.	Выполняет программную реализацию алгоритма шифрования для криптосистемы.
Тема 2.4. **Асимметричные криптосистемы**		
Сформировать понятие об общих принципах построения современных асимметричных криптосистем, схемах шифрования RSA, Полига – Холлмана, Эль-Гамаля.	Общие принципы построения современных асимметричных криптосистем. Однонаправленные функции. Криптосистема RSA. Схема шифрования Полига – Холлмана. Схема шифрования Эль-Гамаля (EGSA).	Излагает общие принципы построения современных асимметричных криптосистем. Описывает схемы шифрования RSA, Полига – Холлмана, Эль-Гамаля.
Обучить шифрованию исходного текста и дешифрованию шифротекста с использованием криптосистемы RSA, программной реализации элементов криптосистемы.	Лабораторная работа № 8 Реализация элементов криптосистемы RSA. Лабораторная работа № 9	Выполняет шифрование исходного текста и дешифрование шифротекста с использованием криптосистемы RSA, программную реализацию элементов криптосистемы.

Цель обучения	Содержание темы	Результат обучения
Обучить шифрованию исходного текста и дешифрованию шифротекста с использованием криптосистемы Эль-Гамаля, программной реализации элементов криптосистемы.	Реализация элементов схемы шифрования Эль-Гамаля.	Выполняет шифрование исходного текста и дешифрование шифротекста с использованием криптосистемы Эль-Гамаля, программную реализацию элементов криптосистемы.
РАЗДЕЛ III. **ИДЕНТИФИКАЦИЯ И ПРОВЕРКА ПОДЛИННОСТИ**		
Тема 3.1. **Основные понятия и концепции идентификации и аутентификации пользователей**		
Сформировать знания о парольных системах идентификации и аутентификации пользователей, процедурах опознавания пользователя в простых и динамически изменяющихся парольных системах, методах оценки стойкости парольных систем. Дать представление о биометрической идентификации и аутентификации пользователей.	Общие подходы к построению парольных систем и основные угрозы их безопасности. Использование простого пароля. Использование динамически изменяющегося пароля. Рекомендации по выбору паролей пользователем. Методы оценки стойкости парольных систем и способы повышения стойкости. Особенности применения пароля для аутентификации пользователей. Биометрическая идентификация и аутентификация пользователей.	Описывает парольные системы идентификации и аутентификации пользователей, процедуры опознавания пользователя в простых и динамически изменяющихся парольных системах, методы оценки стойкости парольных систем. Высказывает общее суждение о биометрической идентификации и аутентификации пользователей.
Тема 3.2. **Взаимная проверка подлинности пользователей**		
Сформировать знания об алгоритмах взаимной проверки подлинности пользователей.	Алгоритмы взаимной проверки подлинности пользователей. Протоколы идентификации с нулевой передачей знаний. Упрощенная схема идентификации с нулевой передачей знаний. Параллельная схема идентификации с нулевой передачей знаний. Лабораторная работа № 10	Излагает алгоритмы взаимной проверки подлинности пользователей.

Цель обучения	Содержание темы	Результат обучения
Обучить программной реализации упрощенной схемы протокола идентификации с нулевой передачей знаний.	Реализация протокола идентификации с нулевой передачей знаний.	Выполняет программную реализацию упрощенной схемы протокола идентификации с нулевой передачей знаний.
	Лабораторная работа № 11	
Обучить программной реализации параллельной схемы протокола идентификации с нулевой передачей знаний.	Реализация параллельного протокола идентификации с нулевой передачей знаний.	Выполняет программную реализацию параллельной схемы протокола идентификации с нулевой передачей знаний.
РАЗДЕЛ IV. **ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ**		
Тема 4.1. **Понятие электронной цифровой подписи**		
Сформировать понятие о сущности и принципах применения ЭЦП, об особенностях применения асимметричных и симметричных криптосистем для ЭЦП.	Обобщенная модель ЭЦП. Особенности применения асимметричных и симметричных криптосистем для ЭЦП.	Раскрывает сущность и излагает принципы применения ЭЦП. Объясняет особенности применения асимметричных и симметричных криптосистем для ЭЦП.
Тема 4.2. **Однонаправленные хеш-функции**		
Дать понятие об особенностях криптографических функций хеширования, алгоритмах хеш-функций.	Функции хеширования и целостность данных. Криптографические однонаправленные функции хеширования. Алгоритмы хеш-функций MD5, SHA-1.	Объясняет особенности криптографических функций хеширования. Излагает алгоритмы хеш-функций.
Тема 4.3. **Алгоритмы электронной цифровой подписи**		
Сформировать понятие об особенностях алгоритмов реализации ЭЦП, алгоритмах ЭЦП.	Особенности алгоритмов реализации ЭЦП. Цифровые подписи, основанные на асимметричных криптосистемах RSA, Эль-Гамаля (EGSA), DSA.	Объясняет особенности алгоритмов реализации ЭЦП. Излагает алгоритмы ЭЦП.

Цель обучения	Содержание темы	Результат обучения
	Лабораторная работа № 12	
Обучить программной реализации функции вычисления ЭЦП RSA.	Реализация функции вычисления ЭЦП RSA	Выполняет программную реализацию функции вычисления ЭЦП RSA.
	Лабораторная работа № 13	
Обучить программной реализации функции проверки ЭЦП RSA.	Реализация функции проверки ЭЦП RSA.	Выполняет программную реализацию функции проверки ЭЦП RSA.
	Лабораторная работа № 14	
Обучить программной реализации функции вычисления ЭЦП Эль-Гамаля.	Реализация функции вычисления ЭЦП Эль-Гамаля.	Выполняет программную реализацию функции вычисления ЭЦП Эль-Гамаля.
	Лабораторная работа № 15	
Сформировать умения реализации схемы ЭЦП Эль-Гамаля.	Реализация функции проверки ЭЦП Эль-Гамаля.	Выполняет программную реализацию функции проверки ЭЦП Эль-Гамаля.
РАЗДЕЛ V. **СИСТЕМЫ ЗАЩИТЫ ПРОГРАММНЫХ СРЕДСТВ**		
Тема 5.1. **Подходы к организации разграничения доступа к информации в компьютерных системах. Защита компьютера от несанкционированного доступа к информации**		
Сформировать знания об угрозах безопасности ПО, о модели и методах внедрения разрушающих ПС, последствиях заражения вредоносной программой, современных системах защиты компьютера от несанкционированного доступа к информации.	Угрозы безопасности ПО. Модель угроз и принципы обеспечения безопасности ПО. Разрушающие программные средства (далее – ПС). Модель и методы внедрения разрушающего ПС. Программные закладки. Троянские программы. Клавиатурные шпионы. Классификация и способы распространения вредоносных программ. Последствия заражения вредоносной программой.	Описывает угрозы безопасности ПО и разрушающие ПС, модель и методы внедрения разрушающих ПС, последствия заражения вредоносной программой, современные системы защиты компьютера от несанкционированного доступа к информации.

Цель обучения	Содержание темы	Результат обучения
	Современные системы защиты компьютера от несанкционированного доступа к информации.	
Тема 5.2. **Шифрование данных с использованием программных средства PGP**		
Сформировать знания об основных возможностях ПС PGP и GPG, о способах применения PGP и GPG для защиты данных.	Шифрование данных с помощью ПС PGP и GPG.	Описывает основные возможности программных средств PGP и GPG.
Тема 5.3. **Использование программного обеспечения для шифрования / дешифрования файлов, дисков**		
Сформировать знания о принципах обеспечения безопасности ПО на различных этапах его жизненного цикла, технологической и эксплуатационной безопасности ПО, об особенностях различных средств защиты ПО.	Принципы обеспечения безопасности ПО на различных этапах его жизненного цикла. Технологическая и эксплуатационная безопасность ПО. Программы для шифрования или дешифрования файлов, дисков.	Излагает принципы обеспечения безопасности ПО на различных этапах его жизненного цикла. Описывает технологическую и эксплуатационную безопасность ПО. Объясняет особенности различных средств защиты ПО.
	Лабораторная работа № 16	
Обучить защите программы от несанкционированной эксплуатации и копирования при помощи специальных ПС.	Защита программы от несанкционированной эксплуатации и копирования при помощи специальных ПС.	Производит защиту программы от несанкционированной эксплуатации и копирования при помощи специальных ПС.
	Лабораторная работа № 17	
Обучить сокрытию данных на винчестере, шифрованию винчестера при помощи специальных ПС.	Защита программ от несанкционированной эксплуатации и сокрытие данных на винчестере.	Производит сокрытие данных на винчестере, шифрование винчестера при помощи специальных ПС.
	Лабораторная работа № 18	
Сформировать умения выполнять генерацию ключа шифрования, шифрование и дешифрование	Применение ПС PGP для генерации ключа шифрования, шифрования и дешифрования сообщений и создания	Выполняет генерацию ключа шифрования, шифрование и дешифрование сообщений. Создает

Цель обучения	Содержание темы	Результат обучения
сообщений, создавать зашифрованный виртуальный диск.	зашифрованного виртуального диска.	зашифрованный виртуальный диск.
РАЗДЕЛ VI. **ПОЛИТИКА БЕЗОПАСНОСТИ**		
Тема 6.1. **Правовое регулирование в области безопасности информации. Организационные методы защиты**		
Сформировать представление об актах законодательства в области безопасности информации, организационных методах защиты.	Обзор актов законодательства в области безопасности информации. Характеристика организационных методов защиты.	Называет акты законодательства в области безопасности информации, организационные методы защиты.
Тема 6.2. **Структура политики безопасности организации**		
Сформировать представление о типах и структуре политики безопасности организации.	Политика безопасности: анализ риска; угрозы/видимость; уязвимость/последствия; учет информационных ценностей. Глобальная и локальная политика безопасности. Базовая политика безопасности. Специализированные типы политики безопасности. Процедуры безопасности.	Высказывает общее суждение о типах и структуре политики безопасности организации.
РАЗДЕЛ VII. **ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ РАЗЛИЧНОГО ТИПА**		
Тема 7.1. **Адаптивное управление безопасностью. Анализ защищенности**		
Сформировать представление о концепции адаптивного управления безопасностью сети, технологии и средствах анализа защищенности.	Концепция адаптивного управления безопасностью сети. Этапы осуществления атаки на компьютерные системы. Технология анализа защищенности. Средства анализа защищенности.	Высказывает общее суждение о концепции адаптивного управления безопасностью сети, технологии и средствах анализа защищенности.

Цель обучения	Содержание темы	Результат обучения
Тема 7.2. **Технология обнаружения атак**		
Сформировать понятие о технологии обнаружения атак, методах анализа сетевой информации.	Классификация систем обнаружения атак IDS. Компоненты и архитектура IDS. Методы реагирования.	Описывает технологию обнаружения атак и методы анализа сетевой информации.
	Лабораторная работа № 19	
Научить анализировать с помощью ПС внутреннего и внешнего аудита основные классы угроз, которым подвержен проверяемый узел сети.	Применение ПС внутреннего и внешнего аудита сетей.	Анализирует с помощью ПС внутреннего и внешнего аудита основные классы угроз, которым подвержен проверяемый узел сети.
	Лабораторная работа № 20	
Сформировать умения применять ПС для анализа трафика в сети, классифицировать расход трафика.	Применение ПС для анализа трафика в сети. Классификация расхода трафика.	Применяет ПС для анализа трафика в сети. Классифицирует расход трафика.
Тема 7.3. **Безопасность работы в глобальной компьютерной сети Интернет**		
Сформировать представление о типовых удаленных атаках в сети Интернет и механизмах их реализации.	Типовые удаленные атаки в сети Интернет и механизмы их реализации.	Высказывает общее суждение о типовых удаленных атаках в сети Интернет и механизмах их реализации.
Дать понятие о типовых уязвимостях и методах обеспечения безопасности систем, входящих в состав глобальных сетей, и безопасности электронной почты.	Типовые уязвимости, позволяющие реализовать удаленные атаки.	Описывает типовые уязвимости и методы обеспечения безопасности систем, входящих в состав глобальных сетей, и безопасности электронной почты.
	Обеспечение безопасности систем, входящих в состав глобальных сетей: межсетевые экраны, виртуальные частные сети.	
Сформировать представление об особенностях защиты информации в электронных платежных системах.	Обеспечение безопасности электронной почты.	Различает особенности защиты информации в электронных платежных системах.
	Особенности защиты информации в электронных платежных системах.	
Обязательная контрольная работа		

Цель обучения	Содержание темы	Результат обучения
Тема 7.4. **Особенности защиты информации в системах электронного документооборота**		
Сформировать представление о структуре и составе подсистемы защиты информации в системах электронного документооборота	Назначение, состав и архитектура систем электронного документооборота. Угрозы информации, характерные для них. Модель потенциального нарушителя	Высказывает общее суждение о структуре и составе подсистемы защиты информации в системах электронного документооборота

ПРИМЕРНЫЕ КРИТЕРИИ ОЦЕНКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ УЧАЩИХСЯ

Отметка в баллах	Показатели оценки
1 (один)	Узнавание отдельных объектов изучения программного учебного материала, предъявленных в готовом виде (основных терминов, понятий, определений в области защиты компьютерной информации)
2 (два)	Различение объектов изучения программного учебного материала, предъявленных в готовом виде (основных терминов, понятий, определений в области защиты компьютерной информации); осуществление соответствующих практических действий
3 (три)	Воспроизведение части программного учебного материала по памяти (фрагментарный пересказ и перечисление изученных методов и алгоритмов защиты компьютерной информации); осуществление умственных и практических действий по образцу
4 (четыре)	Воспроизведение большей части программного учебного материала (описание с элементами объяснения изученных методов и алгоритмов защиты компьютерной информации); применение знаний в знакомой ситуации по образцу; наличие единичных существенных ошибок
5 (пять)	Осознанное воспроизведение большей части программного учебного материала (описание с объяснением изученных методов и алгоритмов защиты компьютерной информации); применение знаний в знакомой ситуации по образцу; наличие несущественных ошибок
6 (шесть)	Полное знание и осознанное воспроизведение всего программного учебного материала; владение программным учебным материалом в знакомой ситуации (описание и объяснение изученных методов и алгоритмов защиты компьютерной информации); выполнение заданий по образцу, на основе предписаний; наличие несущественных ошибок
7 (семь)	Полное, прочное знание и воспроизведение программного учебного материала; владение программным учебным материалом в знакомой ситуации (развернутое описание и объяснение изученных методов и алгоритмов защиты компьютерной информации; формулирование выводов); недостаточно самостоятельное выполнение заданий; наличие единичных несущественных ошибок
8 (восемь)	Полное, прочное, глубокое знание и воспроизведение программного учебного материала; оперирование программным учебным материалом в знакомой ситуации (развернутое описание и объяснение изученных методов и алгоритмов защиты компьютерной информации; формулирование выводов); самостоятельное выполнение заданий; наличие единичных несущественных ошибок

Отметка в баллах	Показатели оценки
9 (девять)	Полное, прочное, глубокое системное знание программного учебного материала, оперирование программным материалом в частично измененной ситуации (разбор производственных ситуаций, самостоятельный выбор способов их разрешения)
10 (десять)	Свободное оперирование программным учебным материалом; применение знаний и умений в незнакомой ситуации (самостоятельные действия по описанию, объяснению изученных методов и алгоритмов защиты компьютерной информации); предложение новых подходов к организации процессов, наличие элементов творческого характера при выполнении заданий

Примечание. При отсутствии результатов учебной деятельности учащимся выставляется ”0“ (ноль) баллов.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОСНАЩЕНИЯ ЛАБОРАТОРИИ

Наименование	Количество
Технические средства обучения	
Технические устройства	
Компьютер	16
Мультимедийный проектор	1
Дидактическое обеспечение	
Видеозаписи учебного назначения	Комплект
Слайды, презентации учебного назначения	Комплект
Электронные средства обучения	
Электронное учебное пособие	1
Программное обеспечение	Комплект
Microsoft Visual Studio . NET., C#(Delphi или иной язык разработки приложения)	
Программное средство ”Сканер ВС“ либо аналоги	
Программное средство TrueCrypt либо аналоги	
Программное средство PGP	
Средства защиты	
Аптечка первой помощи	1
Огнетушитель	1
Оборудование помещения	
Доска аудиторная	1
Стол аудиторный (компьютерный)	15
Стол для преподавателя	1
Стул	31
Шкаф книжный	2
Экран проекционный	1

ЛИТЕРАТУРА

Васильева, И.Н. Криптографические методы защиты информации : учеб. и практикум / И.Н. Васильева. М. : Юрайт, 2020. 349 с.

Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие / А.А. Малюк. М. : Горячая линия-Телеком, 2015. 280 с.

Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. М. : Форум ; Инфра-М, 2021. 416 с.