УПРАВЛЕНИЕ ОБРАЗОВАНИЯ БРЕСТСКОГО ОБЛИСПОЛКОМА

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«ПИНСКИЙ ГОСУДАРСТВЕННЫЙ ПРОФЕССИОНАЛЬНО-ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ЛЁГКОЙ ПРОМЫШЛЕННОСТИ»

УТВЕРЖДАЮ
Директор УО «Пинский ГПТК ЛП»
_____ Н.И. Вакульчик
«____»_____ 2015г.

Учебная программа
по учебной дисциплине
«Защита компьютерной информации»

Разработана на основе примерного тематического плана по учебной дисциплине «Защита компьютерной информации», утвержденного Министерством образования Республики Беларусь 15.07.2013

Специальность
2-40 01 01 Программное обеспечение информационных технологий

Специализация
2-40 01 01-35 Программное обеспечение обработки экономической и деловой информации

2015

Разработчик *В.В. Гришко*, преподаватель учреждения образования «Пинский государственный профессионально-технический колледж легкой промышленности»

Рассмотрена и утверждена на заседании совета колледжа
Протокол №6 от 25 мая 2015г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа учебной дисциплины «Защита компьютерной информации» предназначена для подготовки специалистов специальности 2-40 01 01 «Программное обеспечение информационных технологий».

Прогресс в сфере информационных технологий и компьютеризация практически всех сфер деятельности приводят к возрастанию требований, предъявляемых к защите компьютерной информации. Таким образом, владение методами ее защиты является одним из компонентов компетентности специалиста в области разработки программного обеспечения (ПО).

Целью курса является изучение теоретических основ защиты компьютерной информации и освоение ее методов, выработка профессиональных навыков разработки и программирования задач различного уровня с использованием современных методов и средств.

В результате изучения дисциплины учащиеся должны:

знать на уровне представления:

- особенности функционирования межсетевых экранов;
- способы защиты информации в электронных платежных системах;
- технологии анализа защищенности и обнаружения атак;

знать на уровне понимания:

- алгоритмы блочного шифрования;
- алгоритмы асимметричного шифрования;
- хэш-функции;
- алгоритмы электронной цифровой подписи;
- алгоритмы идентификации и проверки подлинности;

уметь:

- шифровать данные классическими криптосистемами;
- защитить ПК от несанкционированного доступа;
- скрывать информацию на ПК;
- использовать ПО для шифрования/дешифрования файлов, частей или всего винчестера;
- создавать виртуальные зашифрованные диски.

Рабочая программа дисциплины состоит из семи основных разделов:

- информационная безопасность компьютерных систем;
- криптографическая защита информации;
- идентификация и проверка подлинности;
- электронная цифровая подпись;
- средства и методы ограничения доступа к информации;
- технологии обнаружения вторжений;
- технологии защиты межсетевого обмена данных.

ТЕМАТИЧЕСКИЙ ПЛАН

Раздел, тема	Количество часов	
	Всего	В том числе на лабораторные работы
Раздел 1. Информационная безопасность компьютерных систем	**2**	
1.1 Основные понятия и определения информационной безопасности. Основные угрозы безопасности компьютерных систем. Механизмы защиты компьютерных систем	2	
Раздел 2. Криптографическая защита информации	**44**	**22**
2.1 Принципы криптографической защиты информации	2	
2.2 Классические симметричные криптосистемы	14	10
2.3 Современные симметричные криптосистемы	8	
2.4 Ассиметричные криптосистемы	20	12
Раздел 3. Идентификация и проверка подлинности	**10**	**4**
3.1 Основные понятия и концепции идентификации и аутентификации пользователей	2	
3.2 Взаимная проверка подлинности пользователей. Протоколы идентификации с нулевой передачей знаний	8	4
Раздел 4. Электронная цифровая подпись (ЭЦП)	**12**	**8**
4.1 Понятие ЭЦП. Однонаправленные хэш-функции.	2	
4.2 Алгоритмы ЭЦП	10	8
Раздел 5. Средства и методы ограничения доступа к информации	**12**	**6**
5.1 Подходы к организации разграничения доступа к информации в компьютерных системах. Современные системы защиты ПЭВМ от несанкционированного доступа к информации	1	
Обязательная контрольная работа	1	
5.2 Шифрование данных с использованием программного средства PGP	2	
5.3 Использование ПО для шифрования/дешифрования отдельных файлов, отдельных дисков и всего винчестера	8	**6**
Раздел 6. Технологии обнаружения вторжений	**4**	
6.1 Концепция адаптивного управления безопасностью. Технология анализа защищенности	2	
6.2 Технология обнаружения атак	2	
Раздел 7. Технологии защиты межсетевого обмена данных	**12**	
7.1 Угрозы безопасности ОС. Архитектура подсистемы защищенной ОС	4	
7.2 Методы и средства защиты от удаленных атак через сеть Internet. Особенности функционирования межсетевых экранов	4	
7.3 Защита информации в электронных платежных системах	4	
Итого	**96**	**40**

СОДЕРЖАНИЕ ПРОГРАММЫ

Цель изучения темы	Содержание темы	Результат
Раздел 1. Информационная безопасность компьютерных систем		
Сформировать основные понятия и определения информационной безопасности, с основными угрозами безопасности компьютерных систем и механизмами защиты компьютерных систем. Познакомить с историей развития криптографии	Цели, задачи, содержание дисциплины "Защита компьютерной информации". Основные понятия и определения информационной безопасности. Основные угрозы безопасности компьютерных систем. Классификация и назначение механизмов защиты компьютерных систем. История развития криптографии	Объясняет основные понятия и определения информационной безопасности, излагает основные угрозы безопасности компьютерных систем и механизмы защиты компьютерных систем. Высказывает общее суждение об истории развития криптографии, о целях, задачах, содержании дисциплины
Раздел 2. Криптографическая защита информации		
Познакомить с принципами криптографической защиты информации	Основные термины в сфере криптографической защиты информации. Понятие «криптосистема». Сравнение симметричных и ассиметричных криптосистем. Понятие «криптоаналитические атаки» и их виды. Аппаратно-программные средства защиты информации.	Объясняет основные термины в сфере криптографической защиты информации. Высказывает общее суждение об симметричных и ассиметричных криптосистем
Дать представление про классические симметричные криптосистемы	Классические симметричные криптосистемы: основные понятия и определения. Шифры перестановок, шифры простой замены, шифры сложной замены, шифры гаммирования.	Раскрывает основные понятия и определения классических симметричных криптосистем. Проводит шифрование и дешифрование используя Шифры перестановок, шифры простой замены,

Цель изучения темы	Содержание темы	Результат
		шифры сложной замены, шифры гаммирования.
Формирование умений шифрования с использованием методов шифрующих таблиц и магического квадрата	*Лабораторная работа № 1.* Шифрование с использованием метода шифрующих таблиц и метода магического квадрата	Выполняет шифрование с использованием метода шифрующих таблиц и метода магического квадрата
Формирование умений шифрования с использованием систем Цезаря и системы Трисемуса	*Лабораторная работа № 2* Шифрование с использованием: систем Цезаря и системы Трисемуса	Выполняет шифрование с использованием: систем Цезаря и системы Трисемуса
Формирование умений шифрования с использованием алгоритма шифрования Плейфейра	*Лабораторная работа № 3* Реализация алгоритма шифрования Плейфейра	Выполняет шифрование с помощью алгоритма шифрования Плейфейра
Формирование умений шифрования с использованием системы Вижинера и шифра «двойной квадрат» Уитстона	*Лабораторная работа № 4* Шифрование с использованием системы Вижинера и шифра «двойной квадрат» Уитстона	Выполняет шифрование с использованием системы Вижинера и шифра «двойной квадрат» Уитстона
Дать представление про современные симметричные криптосистемы	Американский стандарт шифрования данных DES. Российский стандарт шифрования данных.	Высказывает общее суждение об шифровании и дешифровании используя американский стандарт шифрования данных DES. Российский стандарт шифрования данных
Дать представление про асимметричные криптосистемы	Концепция криптосистемы с открытым ключом. Однонаправленные функции. Криптосистема RSA. Схема шифрования Эль-Гамаля.	Высказывает общее суждение о криптосистемах с открытом ключом и шифровании используя криптосистему RSA и схема шифрования Эль-Гамаля.

Цель изучения темы	Содержание темы	Результат
Формирование умений шифрования с использованием метода асимметрического шифрования RSA	*Лабораторная работа № 5* Реализация элементов криптосистемы RSA	Выполняет реализацию элементов криптосистемы RSA
Формирование умений шифрования с использованием метода асимметрического шифрования Эль-Гамаля	*Лабораторная работа № 6* Реализация элементов схемы шифрования Эль-Гамаля	Выполняет реализацию элементов схемы шифрования Эль-Гамаля
Формирование умений шифрования с использованием алгоритма шифрования ГОСТ 28147–89	*Лабораторная работа № 7* Реализация элементов схемы шифрования ГОСТ 28147-89	Выполняет реализацию элементов схемы шифрования ГОСТ 28147-89
Раздел 3. Идентификация и проверка подлинности		
Познакомить с основными понятиями и концепциями идентификации и аутентификации пользователей.	Идентификация и аутентификация пользователей. Типовые схемы идентификации и аутентификации пользователей. Особенности применения пароля для аутентификации пользователей. Биометрическая идентификация и аутентификация пользователей.	Раскрывает основные понятия и определения идентификация и аутентификация пользователей.
Познакомить с взаимной проверкой подлинности пользователей, Протоколах идентификации с нулевой передачей знаний	Взаимная проверка подлинности пользователей. Протоколы идентификации с ну левой передачей знаний. Упрощенная схема идентификации с ну левой передачей знаний. Параллельная схема идентификации с ну левой передачей знаний.	Раскрывает основные понятия и определения взаимной проверке подлинности пользователей, протоколах идентификации с нулевой передачей знаний

Цель изучения темы	Содержание темы	Результат
Формирование умений проверки подлинности удаленных пользователей с помощью протокола идентификации с нулевой передачей данных.	*Лабораторная работа № 8* Протокол идентификации с нулевой передачей данных	Выполняет реализацию элементов проверки подлинности удаленных пользователей с помощью протокола идентификации с нулевой передачей данных
Формирование умений проверки подлинности удаленных пользователей с помощью параллельной схемы протокола идентификации с нулевой передачей данных.	*Лабораторная работа № 9* Параллельна схема протокола идентификации с нулевой передачей данных	Выполняет реализацию элементов проверки подлинности удаленных пользователей с помощью параллельной схемы протокола идентификации с нулевой передачей данных
Раздел 4. Электронная цифровая подпись (ЭЦП)		
Познакомить с понятиями ЭЦП и однонаправленными хэш-функциями	ЭЦП и однонаправленная хэш-функция.	Высказывает общее суждение о ЭЦП и однонаправленных хэш-функциях
Сформировать знания об алгоритмах ЭЦП. Научить создавать алгоритмы ЭЦП.	Особенности различных алгоритмов реализации ЭЦП.	Высказывает общее суждение об алгоритмах ЭЦП. Создает алгоритмы ЭЦП.
Формирование умений подписи электронных документов электронной цифровой подписью с помощью алгоритма RSA	*Лабораторная работа № 10* Реализация элементов ЭЦП RSA	Выполняет реализацию элементов электронной цифровой подписью с помощью алгоритма RSA
Формирование умений подписи электронных документов электронной цифровой подписью с помощью алгоритма ГОСТ Р 34.10–94	*Лабораторная работа № 11* Реализация элементов ЭЦП ГОСТ Р 34.10-94	Выполняет реализацию элементов электронной цифровой подписью с помощью алгоритма ГОСТ Р 34.10–94
Раздел 5. Средства и методы ограничения доступа к информации		
Сформировать знания об подходах к организации разграничения доступа к информации в КС	Современные системы защиты ПЭВМ от несанкционированного доступа к информации. Современные концепции построения системы разграничения доступа. Особенности их применения.	Высказывает общее суждение об подходах к организации разграничения доступа к информации в КС

Цель изучения темы	Содержание темы	Результат
Научить шифровать данные с использованием программного средства PGP	Особенности и преимущества системы PGP. История ее создания. Практическое применение.	Производит шифрование данные с использованием программного средства PGP
Научить использовать ПО для блокировки/ограничения доступа к программам, файлам, элементам управления и компьютеру в целом для шифрования данных	ПО для блокировки/ограничения доступа к программам, фай-лам, элементам управления и компьютеру в целом. Рекомендации по применению ПО в определенных условиях. ПО для шифрования данных.	Умеет использовать ПО для блокировки/ограничения доступа к программам, файлам, элементам управления и компьютеру в целом для шифрования данных
Формирование умений шифрования жесткого диска или его частей и работы с виртуальными образами зашифрованной области	*Лабораторная работа № 12* Создание виртуальных зашифрованных дисков (программное средство TrueCrypt)	Выполняет шифрование жесткого диска или его частей и работы с виртуальными образами зашифрованной области
Формирование умений работы с программными средствами, позволяющими скрывать отдельные файлы разных типов на жестком диске	*Лабораторная работа № 13* Скрытие данных на винчестере	Выполняет работы с программными средствами, позволяющими скрывать отдельные файлы разных типов на жестком диске
Раздел 6. Технологии обнаружения вторжений		
Сформировать знания о концепции адаптивного управления безопасностью и технологии анализа защищенности	Адаптивная безопасность сети. Этапы осуществления атаки на КС. Технология управления рисками. Технология анализа защищенности. Средства анализа защищенности.	Высказывает общее суждение о концепции адаптивного управления безопасностью и технологии анализа защищенности
Сформировать знания о технологии обнаружения атак	Методы анализа сетевой информации: статистический метод, экспертные системы, нейронные сети. Классификация систем обнаружения атак IDS. Компоненты и архитектура IDS. Методы реагирования.	Высказывает общее суждение о технологии обнаружения атак

Цель изучения темы	Содержание темы	Результат
Раздел 7. Технологии защиты межсетевого обмена данных		
Сформировать знания об угрозах безопасности ОС. Познакомить с архитектурой подсистемы защищенной ОС.	Угрозы безопасности ОС. Понятием «Защищенная ОС». Подходы к построению защищенных ОС. Адекватная политика безопасности. Основные функции подсистемы защиты ОС. Разграничение доступа к объектам ОС.	Высказывает общее суждение об угрозах безопасности ОС. Излагает основные положения подсистемы защищенной ОС.
Познакомить с методами и средствами защиты от удаленных атак через сеть Internet.	Методы и средства защиты от удаленных атак через сеть Internet. Особенности реализации и функционирования межсетевых экранов.	Излагает основные методы и средства защиты от удаленных атак через сеть Internet.
Познакомить с методами защиты информации в электронных платежных системах	Защита информации в электронных платежных системах. Особенности и сложности, возникающие в этой сфере при защите информации.	Излагает основные методы и средства защиты информации в электронных платежных системах.

КРИТЕРИИ ОЦЕНКИ
РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ УЧАЩИХСЯ

Отметка в баллах	Показатели оценок
1 (один)	Узнавание отдельных объектов изучения программного учебного материала, предъявленных в готовом виде (основных терминов, понятий, определений в области защиты компьютерной информации и т.д.); наличие многочисленных существенных ошибок исправляемых с непосредственной помощью преподавателя.
2 (два)	Различение объектов изучения программного учебного материала, предъявленных в готовом виде (основных терминов, понятий, определений в области защиты компьютерной информации и д.п.); осуществление соответствующих практических действий (использует основные таблицы и схемы шифрования.); наличие существенных ошибок исправляемых с непосредственной помощью преподавателя.
3 (три)	Воспроизведение части программного учебного материала по памяти (фрагментарный пересказ и перечисление методов шифрования, функций, принципов конфигурирования алгоритмов шифрования и т.д.); осуществление умственных и практических действий по образцу (оперирует приемами работы с панелью управления, проводит создание алгоритмов отдельных элементов шифровании и т.д.); наличие отдельных существенных ошибок.
4 (четыре)	Воспроизведение большей части программного учебного материала (описание алгоритмов шифрования, работа с базовыми функциями программ шифрования и т.д.); применение знаний в знакомой ситуации по образцу (работа с оснастками, ЭЦП и т.д.); наличие единичных существенных ошибок.
5 (пять)	Осознанное воспроизведение большей части программного учебного материала (описание типовых задач шифрования, назначения и структуры алгоритмов шифрования, работы со средствами шифрования сообщений, файлов и каталогов и т.д.); применение знаний знакомой ситуации по образцу (составление алгоритмов шифрования блочного и асимметричного типа и т.д.); наличие несущественных ошибок.
6 (шесть)	Полное знание и осознанное воспроизведение всего программного учебного материала; владение программным учебным материалом в знакомой ситуации (описание и объяснение компонентов и основных принципов работы программ шифрования и ЭЦП, выполнение заданий по образцу, на основе предписаний, выбор подходящих средств реализации алгоритма шифрования и т.д.); наличие несущественных ошибок.
7 (семь)	Полное, прочное знание и воспроизведение программного учебного материала; владение программным учебным материалом в знакомой ситуации (развернутое описание и объяснение компонентов и основных принципов работы программ шифрования и ЭЦП, методики разработки программных и аппаратных средств для защиты информации, механизмов защиты информации, формулирование выводов, недостаточно самостоятельное выполнение заданий по разработке программ для защиты информации, контроля защиты ОС и ее приложений и т.д.); 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 методов защиты информации, основных принципов работы программ шифрования информации и защиты ПК и других цифровых устройств, функции защиты файловых систем, защиты ресурсов, методики разработки программ защиты информации, механизмов защиты информации, раскрытие сущности принципов межпрограммного взаимодействия, организации защиты операционных систем и данных, обоснование выбора драйвера для периферийных устройств, самостоятельное выполнение заданий по установке и

Отметка в баллах	Показатели оценок
	настройке, контролю работы ОС и ее приложений и т.д.); наличие единичных несущественных ошибок.
9 (девять)	Полное, прочное, глубокое, системное знание программного учебного материала; оперирование программным учебным материалом в частично измененной ситуации (применение учебного материала при управлении работой компьютера, выборе оптимальных настроек и использовании программ защиты компьютерной информации, выдвижении предположений и гипотез об защите вычислительных систем, наличие действий и операций творческого характера для выполнения заданий по выбору наиболее оптимальной защиты информации в зависимости от круга решаемых задача и т.д.).
10 (десять)	Свободное оперирование программным учебным материалом; применение знаний и умений в незнакомой ситуации (самостоятельное описание, объяснение выбора оптимальных настроек и использования программ защиты компьютерной информации для решения поставленной задачи, демонстрация умений осуществлять все виды защиты компьютерной информации, выполнение творческих работ и заданий и т.д.).

Примечание. При отсутствии результатов учебной деятельности обучающихся в учреждении, обеспечивающем получение среднего специального образования, выставляется «0» (ноль) баллов.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОСНАЩЕНИЯ УЧЕБНОГО КАБИНЕТА

Наименование	Количество
ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ	
Мультимедийный проектор	1
Компьютер	15
Схемы и таблицы	
Латинский алфавит	15
Русский алфавит	15
Таблица Тритемиуса для русского алфавита	15
Таблица Вижинера для русского алфавита	15
Схема шифрования Эль-Гамаля	15
Схема алгоритма RSA	15
Схемы шагов алгоритма в ГОСТе 28147–89	15
Схемы шагов алгоритма в ГОСТе Р34.10–94	15
Программное обеспечение	
ОС Windows или Linux	1
Microsoft Visual Studio	1
Delphi	
ОБОРУДОВАНИЕ ПОМЕЩЕНИЯ	
Стол для преподавателя	1
Столы учебные	16
Стулья	33
Доска классная	1
Экран проекционный	1

ЛИТЕРАТУРА

1. Варфоломеев, А. А. Управление ключами в системах криптографической защиты банковской информации / А. А. Варфоломеев, О. С. Доминина, М. Б. Пеленицын. – М : МИФИ, 1996.

2. Основы информационной безопасности / Е. Б. Белов[и др.]. – М : Горячая линия – Телеком, 2006.

3. Основы криптографии / А. П. Алферов[и др.]. – М : Гелиос АРВ, 2002.

4. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М : Радио и связь, 2001.

5. Хамидуллин, Р. Р. Методы и средства защиты компьютерной информации / Р. Р. Хамидуллин, И. А. Бригаднов, А. В. Морозов. – СПб, 2005.

6. Харин, Ю. С. Математические основы криптологии : учеб. пособие / Ю. С. Харин, В. И. Беоник, Г. В. Матвеев. – Минск : БГУ, 1999.