Учреждение образования
«Полоцкий государственный университет
имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Проректор по учебной работе
учреждения образования
«Полоцкий государственный
университет имени
Евфросинии Полоцкой»

_____ Ю.П. Голубев
«22» 07 2022 г.
Регистрационный №УД-208/22/уч

ПРОГРАММНО-АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
**1-98 01 01 «Компьютерная безопасность
(по направлениям)»
направление специальности
1-98 01 01-01 «Компьютерная безопасность
(математические методы и программные системы)»**

2022 г.

Учебная программа составлена на основе типовой учебной программы для высших учебных заведений по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)», регистрационный № ТД-Р.639/тип. от 20.02.2022, и учебного плана специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)». Регистрационный №13-13/уч. ФИТ от 29.08.2013 г. для дневной формы получения высшего образования.

СОСТАВИТЕЛЬ:
Ирина Брониславовна Бураченок, к.т.н., доцент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет»
(протокол № 6 от «20» июня 2022 г.).

Методической комиссией факультета компьютерных наук и электроники учреждения образования «Полоцкий государственный университет»
(протокол № 10 от «21» июня 2022 г.).

Научно-методическим советом учреждения образования «Полоцкий государственный университет»
(протокол № 7 от «30» июня 2022 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дисциплина «Программно-аппаратные и технические средства защиты информации» ориентирована на обучение студентов знаниям, умениям и навыкам в области построения программных и программно-аппаратных средств защиты информации. Изучаемые темы базируются на использовании современных информационных технологий, новейшего программного, программно-аппаратного и аппаратного (технического) обеспечения средств защиты информации и компьютеров. Дисциплина ориентирована на подготовку специалиста, умеющего проектировать и применять средства защиты информации, выбирать наиболее подходящие программные и программно-аппаратные средства защиты, отвечающие современным требованиям и новейшим технологиям в области защиты информации.

Изучение данной дисциплины является необходимым этапом в профессиональном развитии «специалиста по защите информации, математика».

Целью изучения дисциплины «Программно-аппаратные и технические средства защиты информации» является подготовка специалистов, владеющих знаниями, навыками и умениями в области обеспечения безопасности информации, обрабатываемой на компьютерах и в информационно-телекоммуникационных сетях.

Задачи изучения дисциплины «Программно-аппаратные и технические средства защиты информации». При изучении данной дисциплины требуется разрешить основные задачи:

– изучение понятийного аппарата дисциплины, основных теоретических положений и принципов обеспечения информационной безопасности, методов и средств защиты программных и аппаратных средств от несанкционированного доступа и копирования, принципов их построения, методов и средств обеспечения информационной безопасности в типовых операционных системах, СУБД и сетях, в том числе с использованием средств криптографической защиты информации, системных вопросов защиты программ и данных.

В результате изучения дисциплины «Программно-аппаратные и технические средства защиты информации» обучаемый должен:

знать:

–методы и аппаратно-программные средства комплексной защиты информационно-телекоммуникационных систем на уровнях защиты программ и данных ПЭВМ, операционных систем, сетей и баз данных;

уметь:

– применять методы и средства защиты ПЭВМ;

– строить решения по защите корпоративных информационно-телекоммуникационных систем;

владеть:

– основными приемами обеспечения информационной безопасности с использованием средств криптографической защиты информации, защиты программ и данных;

–знаниями, навыками и умениями в области обеспечения безопасности информации, обрабатываемой на компьютерах и в информационно-телекоммуникационных сетях.

Требования к уровню освоения содержания учебной дисциплины. При изучении дисциплины «Программно-аппаратные и технические средства защиты информации» у студентов специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «Специалист по защите информации. Математик» обеспечивающих выпускникам по указанной специальности успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

Академические компетенции.

АК-4 Уметь работать самостоятельно;

АК-7 иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером;

Социально-личностные компетенции.

СЛК-3 обладать способностью к межличностным коммуникациям;

Профессиональные компетенции.

Научно-исследовательская деятельность

ПК-1 работать с научной, нормативно-справочной и специальной литературой с целью получения последних сведений о новых методах защиты информации, о стойкости существующих систем защиты информации;

ПК-2 формулировать задачи, возникающие при организации защиты информации;

Организационно-управленческая деятельность

ПК-13 владеть современными средствами телекоммуникаций;

ПК-15 организовывать процесс создания, оценки и эксплуатации средств и систем защиты информации, поддерживать и повышать их безопасность; осуществлять контроль за их использованием;

Проектно-конструкторская деятельность

ПК-17 находить оптимальные проектные решения;

ПК-18 разрабатывать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию;

Производственно-технологическая деятельность

ПК-21 эксплуатировать программные, аппаратно-программные и технические средства и системы защиты информации; осуществлять контроль за их использованием; вести необходимую для этого документацию;

ПК-22 осуществлять поддержку и повышать эффективность эксплуатируемых программные, аппаратно-программные и технические средств и систем защиты информации.

Сформированные компетенции являются базовыми при изучении всех последующих дисциплин, связанных с программированием, а также фундаментальной основой для дальнейшей профессиональной деятельности специалиста в области защиты информации.

Перечень дисциплин, в продолжение и на базе которых изучается дисциплина.

Для изучения учебной дисциплины «Программно-аппаратные и технические средства защиты информации» по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» необходимы знания, полученные при изучении базовых дисциплин: «Операционные системы», «Алгоритмы и структуры данных», «Теоретические основы информационной безопасности» государственного компонента и «Программирование», «Надежность программного обеспечения», «Теория кодирования, сжатия и восстановления информации» компонента учреждения высшего образования.

Перечень дисциплин, которые изучаются на базе дисциплины.

Знания полученные при изучении дисциплины «Программно-аппаратные и технические средства защиты информации» по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» являются основой для дипломного проектирования. Изучение учебной дисциплины позволяет дать студентам знания, необходимые в дальнейшем для успешной работы по специальности.

В соответствии с учебным планом по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» на изучение учебной дисциплины отводится:

Форма получения высшего образования первой ступени	дневная
Курс (курсы)	4
Семестр	7
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	68
В том числе:	
Лекции, часов	34
Лабораторные занятия, часов	34
Самостоятельная работа, часов	40
Форма текущей аттестации	зачет
Трудоёмкость дисциплины, зачетные единицы	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.

Раздел 1 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА УПРАВЛЕНИЯ ДОСТУПОМ, ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ.

Тема 1.1. Программно-аппаратные средства управления доступом.

Модели управления доступом. Показатели защищенности от несанкционированного доступа. Средства доверенной загрузки. Системы защиты информации от несанкционированного доступа.

Тема 1.2. Программно-аппаратные средства идентификации и аутентификации.

Основные понятия идентификации и аутентификации. Парольная защита информации от несанкционированного доступа. Принцип парольной защиты. Возможности обхода парольной защиты. Повышение эффективности парольной защиты. Достоинства и недостатки парольной защиты. Программно-аппаратные системы идентификации и аутентификации.

Тема 1.3. Классификация систем идентификации и аутентификации.

Электронные идентификаторы. Биометрические идентификаторы. Комбинированные системы идентификации и аутентификации. Особенности применения внешних носителей ключевой информации для идентификации и аутентификации.

Раздел 2 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.

Тема 2.1. Программно-аппаратные средства криптографической защиты информации.

Классификация средств криптографической защиты информации. Симметричные криптографические системы. Особенности практического применения симметричных криптографических систем. Асимметричные криптографические системы. Особенности практического применения асимметричных криптографических систем. Применение криптографических систем зашиты информации. Требования к средствам криптографической защиты информации.

Тема 2.2. Средства электронной подписи.

Средства электронной подписи. Назначение электронной подписи. Состав электронной подписи. Способы получения сертификатов. Механизм электронной подписи. Алгоритмы хеширования. Формирование электронной подписи. Виды электронной подписи.

Тема 2.3. Криптопровайдеры.

Понятие криптопровайдера. Известные криптопровайдеры. Программное средство криптографической защиты информации «Криптопровайдер Avest CSP» (криптопровайдер AvCSP) ЗАО «АВЕСТ».

Раздел 3 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА СЕТЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ.

Тема 3.1. Межсетевые экраны.

Технологии межсетевых экранов. Понятие межсетевого экрана. Классификация межсетевых экранов. Структура и функции межсетевого экрана. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Политика межсетевого взаимодействия.

Тема 3.2. Программные и программно-аппаратные межсетевые экраны.

Программные и программно-аппаратные межсетевые экраны. Персональные и распределенные межсетевые экраны. Проблемы безопасности традиционных межсетевых экранов. Показатели защищенности межсетевых экранов.

Тема 3.3. Программные и программно-аппаратные системы обнаружения вторжений.

Системы обнаружения вторжений. Понятие системы обнаружения вторжений. Структура системы обнаружения вторжений. Классификация систем обнаружения вторжений. Методы обнаружения сигнатур. Методы обнаружения аномалий. Проблемы безопасности систем обнаружения вторжений. Развертывание систем обнаружения вторжений. Требования к системам обнаружения вторжений. Программные и программно-аппаратные системы обнаружения вторжений.

Раздел 4 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ.

Тема 4.1. Вредоносное программное обеспечение.

Понятие вредоносного программного обеспечения. Классификация вредоносного программного обеспечения. Компьютерные вирусы. Троянские программы. Сетевые черви. Наименование вредоносного программного обеспечения.

Тема 4.2. Методы и средства защиты от вредоносных программ.

Признаки возможного заражения. Методы обнаружения вредоносных программ. Виды антивирусных программ. Классификация защищенности средств антивирусной защиты информации. Антивирусные программы и комплексы.

Раздел 5 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ БАЗ ДАННЫХ

Тема 5.1. Реализация защиты в некоторых СУБД.

Юридическая защита авторских прав на базы данных. Репликация базы данных. Резервирование и распределение баз данных. Резервное копирование и восстановление баз данных. Защита от атак типа внедрение SQL-кода.

Тема 5.2. Криптографические методы защиты данных в СУБД.

Шифрование (SSL) соединения между браузером и серверным приложением. Атаки man-in-the-middle (MITM). Шифрование (SSL) соединения между серверным приложением и СУБД. Отказоустойчивый и высоконагруженный кластер из СУБД (MySQLCluster).

Раздел 6 ЗАЩИТА ИНФОРМАЦИИ В ТЕХНИЧЕСКИХ КАНАЛАХ УТЕЧКИ.

Тема 6.1. Технические каналы утечки информации.

Классификация технических каналов утечки информации. Понятие речевого сигнала. Каналы утечки речевой акустической информации. Общие сведения о природе и физических

свойствах звука. Механизмы речеобразования и слуховой анализатор. Характеристики речи: понятность, разборчивость, натуральность, качество. Сведения о некоторых методах оценки разборчивости речи.

Тема 6.2. Обзор технических средств негласного съема акустической информации.

Необходимость технической защиты информации. Классификация технических средств съема акустической информации. Закладочные устройства. Технические средства дистанционного съема информации. Технические средства съема информации с линий связи.

Тема 6.3. Технические средства защиты речевой информации.

Типы технических средств защиты информации. Подавители записывающих устройств. Обнаружители закамуфлированных камер. Устройства для активной защиты речевой информации от утечки по акустическому и вибрационному каналам.

Тема 6.4. Методика и порядок проведения мероприятий по выявлению и исследованию каналов утечки информации.

Аттестация объектов информатизации. Методика и порядок проведения мероприятий по выявлению и исследованию КУИ. Специальные проверки. Специальные обследования. Специальные исследования. Методика оценки словесной разборчивости речи W.

Учебно-методическая карта учебной дисциплины «Программно-аппаратные и технические средства защиты информации»

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
	Введение в дисциплину						
1	Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.					Осн. лит.: [2], [3]. Доп. лит.: [1], [13].	Блиц-опрос
	Раздел 1 Программно-аппаратные средства управления доступом, идентификации и аутентификации.	**6**	**4**				
2	**Лекция № 1** ***Тема 1.1. Программно-аппаратные средства управления доступом.*** Модели управления доступом. Показатели защищенности от несанкционированного доступа. Средства доверенной загрузки. Системы защиты информации от несанкционированного доступа.	2				Осн. лит.: [2], [3]. Доп. лит.: [4], [5], [18].	Блиц-опрос
3	**Лекция № 2** ***Тема 1.2. Программно-аппаратные средства идентификации и аутентификации.*** Основные понятия идентификации и аутентификации. Парольная защита информации от несанкционированного доступа. Принцип парольной защиты. Возможности обхода парольной защиты. Повышение эффективности парольной защиты. Достоинства и недостатки парольной защиты. Программно-аппаратные системы идентификации и аутентификации.	2				Осн. лит.: [2], [3]. Доп. лит.: [4], [5], [18].	Блиц-опрос

1	2	3	4	5	6	7	8
4	**Лабораторная работа №1** ***Принципы, повышающие стойкость парольных методов опознания.*** *(Знакомство с методикой выбора оптимальных параметров парольной системы защиты для определения минимально необходимой длины пароля, удовлетворяющей заданным условиям. Знакомство с методиками определения: вероятности подбора пароля злоумышленником с первой попытки (за n попыток); вероятности подбора пароля за время указанное время; вероятности появления двух одинаковых паролей при общем количестве субъектов.)*		2			Методические указания	Защита отчета по лабораторной работе № 1
5	**Лекция № 3** ***Тема 1.3. Классификация систем идентификации и аутентификации.*** Электронные идентификаторы. Биометрические идентификаторы. Комбинированные системы идентификации и аутентификации. Особенности применения внешних носителей ключевой информации для идентификации и аутентификации.	2				Осн. лит.: [2], [3]. Доп. лит.: [6], [7], [10].	Блиц-опрос
6	**Лабораторная работа №2** ***Определение требуемой вероятности правильного опознания для биометрических средств аутентификации.*** *(Знакомство с методикой определения вероятности подбора аутентификатора с первой попытки для средства аутентификации:* – *по отпечатку пальца при заданных условиях;* – *по образцу голоса при заданных условиях;* – *по радужной оболочке глаза при заданных условиях.)*		2			Методические указания	Защита отчета по лабораторной работе № 2
	Раздел 2 Программно-аппаратные средства криптографической защиты информации.	**6**	**6**				
7	**Лекция № 4** ***Тема 2.1. Программно-аппаратные средства криптографической защиты информации.*** Классификация средств криптографической защиты информации. Симметричные криптографические системы. Особенности практического применения симметричных криптографических систем.	2				Осн. лит.: [2], [5], [6]. Доп. лит.: [12], [16].	Блиц-опрос

1	2	3	4	5	6	7	8
	Асимметричные криптографические системы. Особенности практического применения асимметричных криптографических систем. Применение криптографических систем зашиты информации. Требования к средствам криптографической защиты информации.						
8	**Лабораторная работа №3** ***Криптографические методы защиты данных в БД.*** *(Знакомство с основными криптографическими методами защиты данных, знакомство с особенностями хранения пароля и проверки пароля.)*		2			Методические указания	Защита отчета по лабораторной работе № 3
9	**Лекция № 5** ***Тема 2.2. Средства электронной подписи.*** Средства электронной подписи. Назначение электронной подписи. Состав электронной подписи. Способы получения сертификатов. Механизм электронной подписи. Алгоритмы хеширования. Формирование электронной подписи. Виды электронной подписи.	2				Осн. лит.: [2], [5], [6]. Доп. лит.: [1], [4], [5], [6].	*Контрольное тестирование №1
10	**Лабораторная работа №4** ***Работа с Центром управления безопасностью. Применение цифровой подписи к базам данных.*** *(Знакомство со способами защиты информации, реализованными в СУБД Microsoft ACCESS. Получение навыков работы с Центром управления безопасностью базы данных. Создание самозаверяющего сертификата помощью средства SelfCert. Подписание базы данных программным способом.)*		2			Методические указания	Защита отчета по лабораторной работе № 4
11	**Лекция № 6** ***Тема 2.3 Криптопровайдеры.*** Понятие криптопровайдера. Известные криптопровайдеры. Программное средство криптографической защиты информации «Криптопровайдер Avest CSP» (криптопровайдер AvCSP) ЗАО «АВЕСТ».	2				Осн. лит.: [2], [3], [5]. Доп. лит.: [1], [4], [5], [6].	***Контрольная работа №1***
12	**Лабораторная работа №5** ***Организация защиты баз данных в СУБД Microsoft Access.*** *(Знакомство со способами зашиты информации в базе данных на примере СУБД Microsoft Access. Получение навыков парольной защиты базы данных.)*		2			Методические указания	Защита отчета по лабораторной работе № 5

1	2	3	4	5	6	7	8
	Раздел 3 Программно-аппаратные средства сетевой защиты информации.	**6**	**6**				
13	**Лекция № 7** ***Тема 3.1. Межсетевые экраны.*** Технологии межсетевых экранов. Понятие межсетевого экрана. Классификация межсетевых экранов . Структура и функции межсетевого экрана. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Политика межсетевого взаимодействия.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [4], [8], [11], [15].	Блиц-опрос
14	**Лабораторная работа №6** ***Шифрование (SSL) соединения между браузером и серверным приложением.*** *(Знакомство с основными свойствами протокола SSL, видами SSL-соединения, двусторонней SSL-аутентификацией и видами шифрования.)*		2			Методические указания	Защита отчета по лабораторной работе № 6
15	**Лекция №8** ***Тема 3.2. Программные и программно-аппаратные межсетевые экраны.*** Программные и программно-аппаратные межсетевые экраны. Персональные и распределенные межсетевые экраны. Проблемы безопасности традиционных межсетевых экранов. Показатели защищенности межсетевых экранов.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [2], [4], [8], [11], [15].	Блиц-опрос
16	**Лабораторная работа №7** ***Настройка системы предотвращения вторжений (IPS)*** *(Знакомство с процессом настройки имен хостов, IP-адресов интерфейсов и паролей для доступа. Знакомство с настройкой статической маршрутизации.)*		2			Методические указания	Защита отчета по лабораторной работе № 7
17	**Лекция №9** ***Тема 3.3. Программные и программно-аппаратные системы обнаружена вторжений.*** Системы обнаружения вторжений. Понятие системы обнаружения вторжений. Структура системы обнаружения вторжений. Классификация систем обнаружения вторжений. Методы обнаружения сигнатур. Методы обнаружения аномалий. Проблемы безопасности систем обнаружения вторжений. Развертывание систем обнаружения вторжений. Требования к системам обнаружения вторжений. Программные и программно-аппаратные системы обнаружения вторжений.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [4], [8], [9], [11], [15].	*Контрольное тестирование №3

1	2	3	4	5	6	7	8
18	**Лабораторная работа №8** ***Настройка системы предотвращения вторжений (IPS)*** *(Настройкой IPS с помощью Cisco IOS CLI, проверкой на работоспособность IPS. Выполнение сигнатурного и эвристического анализа. Обнаружение аномалий.)*		2			Методические указания	Защита отчета по лабораторной работе № 8
	Раздел 4 Программно-аппаратные средства защиты от вредоносных программ	**4**	**4**				
19	**Лекция №10** ***Тема 4.1. Вредоносное программное обеспечение.*** Понятие вредоносного программного обеспечения. Классификация вредоносного программного обеспечения. Компьютерные вирусы. Троянские программы. Сетевые черви. Наименование вредоносного программного обеспечения.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [6], [10], [11], [12], [19].	Блиц-опрос
20	**Лабораторная работа №9.** ***Репликация базы данных. Резервирование и распределение баз данных.*** *(Знакомство с основными способами репликации базы данных, резервирования и распределение баз данных.)*		2			Методические указания	Защита отчета по лабораторной работе № 9
21	**Лекция №11** ***Тема 4.2. Методы и средства защиты от вредоносных программ.*** Признаки возможного заражения. Методы обнаружения вредоносных программ. Виды антивирусных программ. Классификация защищенности средств антивирусной зашиты информации. Антивирусные программы и комплексы.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [11], [12], [18].	*Контрольное тестирование №4
22	**Лабораторная работа №10** ***Защита от атак типа внедрения SQL-кода.*** *(Знакомство с технологией и принципами проведения атаки внедрения SQL-кода.)*		2			Методические указания	Защита отчета по лабораторной работе № 10
	Раздел 5 Программно-аппаратные средства защиты баз данных	**4**	**4**				
23	**Лекция №12** *Тема 5.1. Реализация защиты в некоторых СУБД.* Юридическая защита авторских прав на базы данных. Репликация базы данных. Резервирование и распределение баз данных. Резервное копирование и восстановление баз данных. Защита от атак типа внедрение SQL-кода.	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [17].	Блиц-опрос

1	2	3	4	5	6	7	8
24	**Лабораторная работа №11** ***Резервное копирование и восстановление баз данных.*** *(Знакомство с видами резервного копирования и схемами ротации. Написание скриптов для резервирования базы данных на отдельном HDD.)*		2			Методические указания	Защита отчета по лабораторной работе № 11
25	**Лекция №13** *Тема 5.2. Криптографические методы защиты данных в СУБД.* Шифрование (SSL) соединения между браузером и серверным приложением. Атаки man-in-the-middle (MITM). Шифрование (SSL) соединения между серверным приложением и СУБД. Отказоустойчивый и высоконагруженный кластер из СУБД (MySQLCluster).	2				Осн. лит.: [1], [2], [3]. Доп. лит.: [17].	*Контрольное тестирование №5
26	**Лабораторная работа №12** ***Атаки MITM. Шифрование (SSL) соединения между серверным приложением и СУБД*** *(Знакомство с технологией атаки man-in-the-middle (MITM). Знакомство с настройками соединения SSL между приложением и СУБД. Выполнение анализа защищенности канала с помощью tcpdump.)*		2			Методические указания	Защита отчета по лабораторной работе № 12
	Раздел 6 Защита информации в технических каналах утечки	**8**	**10**				
27	**Лекция №14** ***Тема 6.1. Технические каналы утечки информации*** Классификация технических каналов утечки информации. Понятие речевого сигнала. Каналы утечки речевой акустической информации. Общие сведения о природе и физических свойствах звука. Механизмы речеобразования и слуховой анализатор. Характеристики речи: понятность, разборчивость, натуральность, качество. Сведения о некоторых методах оценки разборчивости речи.	2				Осн. лит.: [1], [4]. Доп. лит.: [3], [14], [19].	Блиц-опрос
28	**Лекция № 15** ***Тема 6.2. Обзор технических средств негласного съема акустической информации*** Необходимость технической защиты информации. Классификация технических средств съема акустической информации. Закладочные устройства. Технические средства дистанционного съема информации. Технические средства съема информации с линий связи.	2				Осн. лит.: [1], [4]. Доп. лит.: [3], [14], [19].	*Контрольное тестирование №3

1	2	3	4	5	6	7	8
29	**Лабораторная работа №13** ***Мероприятия по выявлению каналов утечки информации.*** *(Знакомство с регламентом проведения специальных проверок; специальных обследований; специальных исследований.)*		2			Методические указания	Защита отчета по лабораторной работе №13
	Лабораторная работа №13 ***Мероприятия по выявлению каналов утечки информации.*** *(Знакомство с регламентом проведения специальных проверок; специальных обследований; специальных исследований.)*		2				
30	**Лекция № 16** ***Тема 6.3. Технические средства защиты речевой информации.*** Типы технических средств защиты информации. Подавители записывающих устройств. Обнаружители закамуфлированных камер. Устройства для активной защиты речевой информации от утечки по акустическому и вибрационному каналам.	2				Осн. лит.: [1], [4]. Доп. лит.: [3], [8], [14], [19].	****Контрольная работа №2***
31	**Лекция № 17** ***Тема 6.4. Методика и порядок проведения мероприятий по выявлению и исследованию каналов утечки информации.*** Аттестация объектов информатизации. Методика и порядок проведения мероприятий по выявлению и исследованию КУИ. Специальные проверки. Специальные обследования. Специальные исследования. Методика оценки словесной разборчивости речи W.	2				Осн. лит.: [1], [4]. Доп. лит.: [3], [4], [8], [14], [19].	*Контрольное тестирование №6
32	**Лабораторная работа №14** ***Оценка первичных признаков элементов речевого сигнала.*** *(Знакомство с методикой оценки тонкой структуры информационных признаков элементов речевого сигнала.)*		2			Методические указания	Защита отчета по лабораторной работе № 14
	Лабораторная работа №14 ***Оценка первичных признаков элементов речевого сигнала.*** *(Знакомство с методикой оценки тонкой структуры информационных признаков элементов речевого сигнала.)*		2				
33	**Лабораторная работа №15** ***Выполнение контрольного задания.***		2			Методические указания	Контрольное задание
	Всего (68 часов)	**34**	**34**				

*** КОНТРОЛЬНЫЕ ТОЧКИ**

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Данилова, О. Т. Технические средства разведки и защита информации : учебное пособие : в 4 частях : [16+] / О. Т. Данилова ; Омский государственный технический университет. – Омск : Омский государственный технический университет (ОмГТУ), 2019. – Часть 1. Технические каналы утечки речевой акустической конфиденциальной информации. – 64 с. : ил., табл., схем., граф. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=682094 (дата обращения: 04.09.2022). – Библиогр. в кн. – ISBN 978-5-8149-2839-9 (Ч. 1). – ISBN 978-5-8149-2838-2. – Текст : электронный.

2. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. – Ростов-на-Дону : Донской ГТУ, 2021. – 228 с. – ISBN 978-5-7890-1878-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/237770 (дата обращения: 04.09.2022). – Режим доступа: для авториз. пользователей.

3. Программно-аппаратные средства защиты информационных систем : учебное пособие : [16+] / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 04.09.2022). – Библиогр.: с. 190. – ISBN 978-5-8265-1737-6. – Текст : электронный.

4. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – Москва : Горячая линия – Телеком, 2021. – 585 с.

5. Раханов, К. Я. Обеспечение конфиденциальности информации в сети Интернет пособие / К. Я. Раханов, Н. А. Раханова. – Новополоцк : Полоц. гос. ун-т 2021. – 192 с.

6. Введение в криптографическую защиту информации объектов : учебник / С.Н. Ильиных, С. Г. Алюшина, Т. И. Калинкина [и др.]. – Москва : МТУСИ, 2021. – 276 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/215231 (дата обращения: 04.09.2022). – Режим доступа: для авториз. пользователей.

Дополнительная:

1. Аверченков, В. И. Служба защиты информации: организация и управление : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов. - 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. : ил., схем. – Режим доступа: по подписке.

2. Вотинов, М. В. Практикум по архитектуре вычислительных машин, комплексам защиты информации и протоколам передачи данных в компьютерных сетях : учебное пособие / М. В. Вотинов. – Мурманск : МГТУ, 2018. – 110 с. – ISBN 978-5-86185-968-4. – Текст : электронный // Лань : электронно-библиотечная система.

3. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А. М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636 (дата обращения: 04.09.2022). – Библиогр.: с. 213. – Текст : электронный.

4. Долозов, Н. Л. Программные средства защиты информации: конспект лекций / Н. Л. Долозов, Т. А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2015. – 63 с. :

Куц Шуклина Е. К.

схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438307 (дата обращения: 11.09.2022). – Библиогр. в кн. – ISBN 978-5-7782-2753-8. – Текст : электронный.

5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. – 312 с. – (Высшее образование). – ISBN 978-5-9916-9043-0. – Текст : электронный // Образовательная платформа Юрайт [сайт].

6. Кондрашин, М. В. Рудановский ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. : ил., схем. – (Организация и технология защиты информации). – Режим доступа: по подписке.

7. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. – 3-е изд., перераб. – Санкт-Петербург : Лань, 2021. – 236 с. – Текст : электронный // Лань : электронно-библиотечная система.

8. Креопалов, В. В. Технические средства и методы защиты информации: учебно-практическое пособие / В. В. Креопалов. – Москва : Евразийский открытый институт, 2011. – 278 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=90753 (дата обращения: 04.09.2022). – ISBN 978-5-374-00507-3. – Текст : электронный.

9. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для вузов / С. Н. Никифоров. – 3-е изд., стер. – Санкт-Петербург : Лань, 2020. – 96 с. – Текст : электронный // Лань : электронно-библиотечная система.

10. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. – 2-е изд., испр. – Санкт-Петербург : Лань, 2020. – 124 с. – Текст : электронный // Лань : электронно-библиотечная система.

11. Пушкарёв, В. В. Защита информационных процессов в компьютерных системах : учебное пособие / В. В. Пушкарёв, В. П. Пушкарёв. – Москва : ТУСУР, 2012. – 131 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/4925 (дата обращения: 04.09.2022). – Режим доступа: для авториз. пользователей.

12. Сергеева, Ю. С. Защита информации: конспект лекций : учебное пособие : [16+] / Ю. С. Сергеева. – Москва : А-Приор, 2011. – 128 с. – (Конспект лекций. В помощь студенту). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=72670 (дата обращения: 04.09.2022). – ISBN 978-5-384-00397-7. – Текст : электронный.

13. Системы защиты информации в ведущих зарубежных странах : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, Г. В.

14. Титов, А. А. Технические средства защиты информации : учебное пособие / А. А. Титов. – Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 194 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=208661 (дата обращения: 04.09.2022). – Текст : электронный.

15. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. – Санкт-Петербург : Лань, 2020. – 184 с. – Текст : электронный // Лань : электронно-библиотечная система.

16. Защита компьютерной информации : учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. – Санкт-Петербург : БГТУ, 2019. – 146 с. – Текст : электронный // Лань : электронно-библиотечная система.

17. Основы построения защищенных баз данных: лабораторный практикум : учебное пособие : [16+] / авт.-сост. Л. Л. Гусева ; Министерство науки и высшего образования Российской Федерации, Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 120 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=563264 (дата обращения: 27.11.2022). – Библиогр. в кн. – Текст : электронный.

18. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. – Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. – 98 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/180093 (дата обращения: 04.09.2022). – Режим доступа: для авториз. пользователей.

19. Технические средства радиоэлектронной защиты : учебное пособие / В. В. Смирнов, Л. Б. Кочин, С. А. Певишев, А. С. Стукалова. – Санкт-Петербург : БГТУ «Военмех» им. Д.Ф. Устинова, 2020. – 62 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/172218 (дата обращения: 04.09.2022). – Режим доступа: для авториз. пользователей.

20. Таненбаум, Э. Компьютерные сети = Computer Networks / [перевод с английского А. Гребеньков]. – 5-е издание. – Санкт-Петербург : Питер, 2021. – 955 с.

21. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. – Благовещенск : АмГУ, 2017. – 240 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/156494 (дата обращения: 04.09.2022). – Режим доступа: для авториз. пользователей.

ГОСТы

1. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.

2. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.

3. Классификация вредоносных программ / Сайт Лаборатории Касперского. URL: https://www.kaspersky.ru/resource-center/threats/malware-classifications (дата обращения: 05.06.2022).

4. СТБ 34.101.1-2014 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

5. СТБ 34.101.2-2014 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

6. СТБ 34.101.3-2014 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности.

7. СТБ 34.101.8-2014 Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования.

8. СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»;

9. СТБ 34.101.79-2019 «Информационные технологии и безопасность. Криптографические токены»;

10. СТБ 34.101.80-2019 «Информационные технологии и безопасность. Расширенные электронные цифровые подписи»;

11. СТБ 34.101.81-2019 «Информационные технологии и безопасность. Протоколы службы заверения данных»;

12. СТБ 34.101.82-2019 «Информационные технологии и безопасность. Протокол постановки штампа времени».

Законы Республики Беларусь

1. Закон Республики Беларусь от 19 июля 2005 г. № 45-З «Об электросвязи».

2. Закон Республики Беларусь от 9 ноября 2009 г. № 59-З «О ратификации Соглашения о сотрудничестве в создании государственных информационных систем

паспортно-визовых документов нового поколения и дальнейшем их развитии и использовании в государствах – участниках СНГ».

3. Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи».

4. Закон Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах».

5. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

6. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных».

Электронные ресурсы:

1. International Organization for Standardization (Международная Организация Стандартизации). [Электрон, ресурс]. – Режим доступа: http://www.iso.org (http://www.iso.ch). – Дата доступа: 19.03.2022.

2. Аппаратные алгоритмы электронных ключей – Системы программно-аппаратной защиты компании Актив. Электронные ключи Guardant Stealth. Internet-ресурс (www.novex.ru).

3. Государственный комитет по стандартизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: http://www.tnpa.by. – Дата доступа: 19.03.2022.

4. Министерство связи и информатизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: http://www.mpt.gov.by. – Дата доступа: 19.03.2022.

5. Научно-исследовательский институт технической защиты информации. [Электрон, ресурс]. – Режим доступа: http://www.niitzi.by. – Дата доступа: 19.03.2018.

6. Национальный правовой портал Республики Беларусь. [Электрон, ресурс]. – http://www.pravo.by. – Дата доступа: 19.03.2022.

7. Национальный центр интеллектуальной собственности. [Электрон, ресурс]. – Режим доступа: http://www.belgospatent.org.by. – Дата доступа: 19.03.2022.

8. Оперативно-аналитический центр при Президенте Республики Беларусь [Электрон, ресурс]. – Режим доступа: http://oac.gov.by. – Дата доступа: 19.03.2022.

9. Система лицензирования NetHASP – С. Груздев «Лицензирование программного обеспечения в сетях» Internet-ресурс (www.aladdin.ru)

Перечень компьютерных программ:

1. Используются пакеты: MatLab, Mathcad, (*любой язык программирования* C++, C#, Java), Microsoft Visio, Oracle, MySQL, Microsoft Server, VMWare/VirtualBox.

ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

Лабораторная работа №1 Принципы, повышающие стойкость парольных методов опознания.
Цель работы – используя методику выбора оптимальных параметров парольной системы защиты определить минимально необходимую длину пароля, удовлетворяющую заданным условиям. Определение вероятности подбора пароля злоумышленником с первой попытки (за *n* попыток); вероятности подбора пароля за время указанное время; вероятности появления двух одинаковых паролей при общем количестве субъектов.

Лабораторная работа № 2 Определение требуемой вероятности правильного опознания для биометрических средств аутентификации.
Цель работы – определение вероятности подбора аутентификатора с первой попытки для средства аутентификации: по отпечатку пальца при заданных условиях; по образцу голоса при заданных условиях; по радужной оболочке глаза при заданных условиях.

Лабораторная работа №3 Криптографические методы защиты данных в базах данных.
Цель работы – изучить основные криптографические методы защиты данных и выполнить хранение пароля и проверку пароля.

Лабораторная работа №4 Работа с Центром управления безопасностью. Применение цифровой подписи к базам данных.
Цель работы – изучение новых возможностей и способов защиты информации в базе данных, реализованных в новых версиях в СУБД Microsoft Access. Получение навыков работы с Центром управления безопасностью базы данных. Создание самозаверяющего сертификата помощью средства SelfCert. Подписание базы данных программным способом.

Лабораторная работа №5 Организация защиты баз данных в СУБД Microsoft Access.

Цель работы – изучить способы зашиты информации в базе данных на примере СУБД Microsoft Access. Получение навыков парольной защиты базы данных.

Лабораторная работа №6 Шифрование (SSL) соединения между браузером и серверным приложением.
Цель работы – изучить основные свойства протокола SSL, виды SSL-соединения, двустороннюю SSL-аутентификацию и виды шифрования.

Лабораторная работа №7. Настройка системы предотвращения вторжений (IPS).
Цель работы – Настройка имен хостов, IP-адресов интерфейсов и паролей для доступа. Настройка статической маршрутизации.

Лабораторная работа №8 Настройка системы предотвращения вторжений (IPS).
Цель работы – Настройка IPS с помощью Cisco IOS CLI, проверка на работоспособность IPS. Сигнатурный анализ. Эвристический анализ. Обнаружение аномалий.

Лабораторная работа №9. Репликация базы данных. Резервирование и распределение баз данных.
Цель работы – изучить основные способы репликации базы данных, резервирования и распределение баз данных.

Лабораторная работа №10 Защита от атак типа внедрения SQL-кода.
Цель работы – изучить технологии и принципы проведения атаки внедрения SQL-кода. Проанализировать способы защиты.

Лабораторная работа №11. Резервное копирование и восстановление баз данных.
Цель работы – изучить виды резервного копирования и схемы ротации. Написать скрипты для резервирования базы данных на отдельном HDD.

Лабораторная работа №12. Атаки MITM. Шифрование (SSL) соединения между серверным приложением и СУБД.
Цель работы – изучить технологию атаки man-in-the-middle (MITM), настроить соединение SSL между приложением и СУБД и выполнить анализ защищенности канала с помощью tcpdump.

Лабораторная работа №13 **Мероприятия по выявлению каналов утечки информации.**
Цель работы – изучить назначение и регламент проведения специальных проверок; изучить назначение и регламент проведения специальных обследований; изучить назначение и регламент проведения специальных исследований.

Лабораторная работа №14 Оценка первичных признаков элементов речевого сигнала.
Цель работы – провести оценку тонкой структуры информационных признаков элементов речевого сигнала.

Лабораторная работа №15 Выполнение контрольного задания.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

1. Какие ставит перед собой цели и задачи дисциплина «Программно-аппаратные и ТС ЗИ?
2. Дайте понятие информационной системы.
3. Что такое безопасность информационной системы?
4. Какие существуют методы и СЗИ?
5. Дайте понятие организационным методам и системам защиты информации?
6. Дайте понятие инженерно-техническим системам защиты информации?
7. Что подразумевается под криптографическими методами и системами защиты информации?
8. Что относят к программно-аппаратным системам защиты информации?
9. Что понимается под понятием модель политики безопасности (модель управления доступом)?
10. Какая основная цель модели управления доступом?
11. Дайте определение понятия доступ к информации.
12. Дайте определение понятия правила разграничения доступа.
13. Дайте определение понятиям объект и субъект доступа.
14. Что такое несанкционированный доступ к информации?
15. Какие вам известны модели управления доступом?
16. Расскажите об особенностях мандатной модели управления доступом.
17. Расскажите об особенностях дискреционной модели управления доступом.
18. Расскажите об особенностях недискреционной модели управления доступом.
19. Расскажите о первой модели политики безопасности, применимой для компьютерных систем.
20. Что понимается под системой разграничения доступом?
21. Особенности систем разграничения доступа, основанных на концепции диспетчера доступа.
22. Укажите основные требования к реализации диспетчера доступа.
23. В чем сущность концепции диспетчера доступа?
24. Что подразумевают под базой данных защиты?
25. Что такое системный журнал? Его основное назначение?
26. С какой целью используется блок очистки памяти?
27. Какие определяют показатели защищенности от несанкционированного доступа?
28. Дайте определение понятиям система и элемент.
29. Какие выделяют классы защищенности СВТ?
30. Что относится к средствам доверенной загрузки?
31. Укажите типы средств доверенной загрузки.
32. Приведите примеры средств доверенной загрузки. Принципы их работы?
33. Приведите классификацию систем защиты.
34. Приведите примеры популярных российских СЗИ от НСД.
35. Приведите примеры популярных зарубежных СЗИ от НСД.
36. Дайте определение идентификации.
37. Дайте определение аутентификации.
38. Дайте определения понятиям авторизация и администрирование.
39. Что такое парольная защита информации от несанкционированного доступа?
40. Укажите основные принципы парольной защиты информации.
41. Укажите возможности обхода парольной защиты.
42. Как повысить эффективность парольной защиты?
43. Укажите достоинства и недостатки парольной защиты.
44. Виды паролей.
45. Приведите меру количественной оценки стойкости парольных систем (формула Андерсона).
46. Как определяется вероятность подбора пароля?

47. Приведите классификацию систем идентификации и аутентификации.
48. Электронные системы идентификации и аутентификации:
    - iButton (Touch Memory);
    - контактные смарт-карты;
    - радиочастотные идентификаторы;
    - бесконтактные смарт-карты;
    - USB-ключи.
49. Основные достоинства биометрических методов идентификации и аутентификации в сравнении с электронными.
50. Расскажите основные этапы развития биометрии.
51. Что лежит в основе биометрической идентификации и аутентификации?
52. Что относится к статическим биометрическим признакам.
53. Особенности систем аутентификации по отпечаткам пальцев.
54. Виды дактилоскопических сканеров.
55. Дактилоскопические сканеры (оптические).
56. Дактилоскопические сканеры (емкостные).
57. Дактилоскопические сканеры (радиочастотные).
58. Дактилоскопические сканеры (давления).
59. Дактилоскопические сканеры (ультразвуковые).
60. Дактилоскопические сканеры (температурные).
61. Системы аутентификации по узору радужной оболочки глаза.
62. Системы аутентификации по сетчатке глаза.
63. Системы аутентификации по геометрической форме руки.
64. Системы аутентификации по геометрии лица.
65. Системы аутентификации по термограмме лица.
66. Динамические биометрические признаки.
67. Системы аутентификации по голосу.
68. Системы аутентификации по динамике рукописной подписи
69. Дактилоскопические сканеры (давления).
70. Системы аутентификации по «клавиатурному почерку».
71. Оценка эффективности биометрических СИА (параметры FAR (False Acceptance Rate), FRR (False Rejection Rate)).
72. Мультифакторная аутентификация, ее применение.
73. Комбинированные (мультимодальные) биометрические системы.
74. Системы на базе радиочастотных идентификаторов и USB-ключей.
75. Системы на базе гибридных смарт-карт.
76. Приведите классификацию средств криптографической защиты информации.
77. Что вам известно о симметричных криптографических системах?
78. Каковы особенности практического применения симметричных криптографических систем?
79. Приведите примеры асимметричных криптографических систем.
80. В чем заключаются особенности практического применения асимметричных криптографических систем?
81. Приведите примеры применения криптографических систем зашиты информации.
82. Перечислите основные нормативные документы описывающие основные требования к средствам криптографической защиты информации в Республике Беларусь.
83. Приведите примеры программно-аппаратных средств криптографической защиты информации.
84. Укажите особенности программных средств криптографической защиты информации.
85. Укажите особенности программно-аппаратных средств криптографической защиты информации.
86. Укажите особенности аппаратных средств криптографической защиты информации.
87. Приведите принципиальное отличие аппаратных от программно-аппаратных СКЗИ.
88. Приведите примеры популярных СКЗИ.

89. Что относят к средствам электронной подписи?
90. Каково основное назначение электронной подписи?
91. Что входит в состав электронной подписи?
92. Какие существуют способы получения сертификатов?
93. Приведите особенности механизма формирования электронной подписи.
94. Что представляет собой алгоритмы хеширования?
95. Как осуществляется процесс формирования электронной подписи?
96. Приведите примеры видов электронной подписи.
97. Дайте понятие криптопровайдер?
98. Каким условиям не удовлетворяет встроенный криптопровайдер Microsoft Base Cryptographic Provider?
99. Приведите примеры известных вам криптопровайдеров.
100. Что вам известно о криптопровайдере AVEST CSP?
101. Укажите известные вам методы сетевой защиты информации.
102. Особенности стандарта ISO/IEC 7498 открытой сетевой модели OSI (Open Systems Interconnection model).
103. Что такое межсетевой экран? Какие основные задачи выполняют межсетевые экраны?
104. Какие используют схемы подключения межсетевых экранов?
105. Приведите классификацию межсетевых экранов:
    - по способу реализации;
    - по охвату контролируемых потоков данных;
    - по используемой технологии;
    - по функционированию на уровнях сетевой модели OSI.
106. Приведите структуру межсетевого экрана. Какие основные функции выполняют межсетевые экраны?
107. В чем основной недостаток схемы единой защиты локальной сети?
108. В чем основное преимущество схемы с раздельной защитой закрытой и открытой подсетей?
109. Туннелирование.
110. Укажите какие возникают проблемы безопасности корпоративной сети при использовании традиционных межсетевых экранов.
111. Показатели защищенности межсетевых экранов.
112. Классы защищенности межсетевых экранов.
113. Приведите примеры программных и программно-аппаратных межсетевых экранов и их применение.
114. Какие сведения представлены в СТБ 34.101.75-2017 Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования?
115. Дайте понятие системы обнаружения вторжений.
116. Основное назначение и функции систем обнаружения вторжений.
117. Приведите структуру системы обнаружения вторжений.
118. Приведите классификацию систем обнаружения вторжений.
119. Расскажите, что такое сигнатура и какие методы обнаружения сигнатур вам известны?
120. Дайте понятие обнаружения аномалии. Какие методы обнаружения аномалий вам известны?
121. Проблемы безопасности систем обнаружения вторжений.
122. Развертывание систем обнаружения вторжений.
123. Какие предъявляют требования к системам обнаружения вторжений?
124. Перечислите известные вам программные и программно-аппаратные системы обнаружена вторжений.
125. Для каких целей применяются программы: Microsoft Network Monitor, IP Sniffer, Ethereal?
126. Дайте понятие идентификации.

127. Дайте понятие аутентификации
128. Что такое можно отнести к средствам аутентификации?
129. Какие существуют три класса опознания?
130. Укажите особенности методов опознания на основе различных принципов.
131. Преимущества и недостатки схемы паролей однократного использования.
132. Преимущества и недостатки динамически изменяющегося пароля.
133. Что относят к методам модификации схемы простых паролей?
134. Укажите особенности метода «запрос-ответ». Варианты реализации данного метода? Достоинства и недостатки?
135. Что относят к методу «рукопожатия»? Укажите его особенности. Достоинства и недостатки?
136. Перечислите известные вам методы защиты от копирования магнитных карт.
137. С какой целью выполняется нанесение магнитного слоя обычного типа поверх второго слоя с более высокой коэрцитивной силой при изготовлении магнитных карт?
138. В каких ситуациях удобно использовать постоянную магнитную разметку ленты (метод «влажной разметки»)?
139. Что представляет собой электронный ключ? Его основные достоинства?
140. Что относят к биометрическим системам аутентификации. Какие выделяют две категории указанных методов?
141. Что лежит в основе метода опознания по отпечатку пальца?
142. Что лежит в основе метода опознания субъекта по лицу?
143. Что лежит в основе метода опознания субъекта по радужной оболочке глаза?
144. Что лежит в основе метода опознания по образцу голоса?
145. Что относят к показателям эффективности средств аутентификации?
146. Как оценивают показатель эффективности средства аутентификации?
147. Как определить вероятность правильного опознания субъекта средством аутентификации?
148. Как определить вероятность пропуска «чужого» субъекта средством аутентификации?
149. Укажите принципы, повышающие стойкость парольных методов опознания?
150. В чем заключается основная идея принципа максимального правдоподобия?
151. В чем заключается основная идея принципа ограничения попыток при опознании субъекта?
152. Особенность принципа цикличности при опознании субъекта?
153. Как определить вероятность подбора пароля с первой попытки?
154. Как определить вероятность подбора PIN-кода с первой попытки?
155. Как определить вероятность подбора битового ключа с первой попытки?
156. В чем заключается принцип ограничения попыток при опознании субъекта?
157. Как определить вероятность подбора пароля за k попыток?
158. Как определить безопасное время действия пароля?
159. Как определить вероятность подбора пароля за безопасное время его действия?
160. Как определить требуемую вероятность правильного опознания для биометрических средств аутентификации? Основные подходы.
161. Какие имеются известные средства аутентификации по отпечатку пальца?
162. Что такое минуция? Когда возникает минуция типа «окончание» папиллярной линии? Когда возникает минуция «раздвоение» папиллярной линии?
163. Какие имеются известные средства аутентификации по образцу голоса?
164. Что понимают под матрицей близости?
165. Какие имеются известные средства аутентификации по радужной оболочке глаза?
166. Расскажите о методах обеспечения конфиденциальности данных.
167. Шифрование данных с неявным заданием ключа.
168. Где может храниться ключевая информация, используемая для шифрования данных?
169. Назвать стадии восстановления базы данных.

170. Перечислить причины утери информации.
171. Перечислить виды резервного копирования.
172. Перечислить схемы ротации.
173. Какой компанией и в каком году был разработан криптографический протокол SSL (Secure Socket Layer)?
174. Какими элементами протокола SSL обеспечивается защищенный обмен данными?
175. Что такое центр сертификации CA (certificate authority)?
176. Назовите наиболее популярные центры сертификации.
177. Назовите виды SSL-соединения.
178. Утилита tcpdump, ее особенности использования для перехвата и анализа сетевого трафика.
179. Что такое HTTPS?
180. Что такое MITM-атака (Man-in-the-Middle)?
181. Какова цель атаки Man-in-the-Middle?
182. В чем заключается атака Man-in-the-Middle?
183. Что такое MitD-атака (Man-in-the-Disk)?
184. Какова цель атаки Man-in-the-Disk?
185. В чем заключается атака Man-in-the-Disk?
186. Можно ли, используя HTTPS-соединение, защитится от атаки?
187. Для каких целей применяются программы: Microsoft Network Monitor, IP Sniffer, Ethereal?
188. Объяснить принципы проведения атаки внедрения SQL.
189. Объяснить внедрение кода в строковые параметры.
190. Объяснить использование UNION.
191. Описать методику проведения атаки типа внедрение SQL-кода.
192. Какие методы защиты от атак типа внедрение SQL-кода вы знаете?

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Программно-аппаратные и технические средства защиты информации» предполагает реализацию следующих форм самостоятельной работы студентов:

– проработка конспекта лекций и учебной литературы;

– изучение печатных источников по теме дисциплины;

– изучение профессиональных электронных ресурсов по теме дисциплины;

– изучение вопросов для самоконтроля;

– подготовка к аудиторному выполнению лабораторных работ (предварительное знакомство с методическими указаниями, программным обеспечением, вариантом индивидуального задания по работе);

– решение индивидуальных задач при подготовке к лабораторным занятиям;

–подготовка к защите лабораторных (оформление отчёта по индивидуальному варианту задания, защита результатов работы и демонстрации степени освоения навыков и умений по конкретной теме);

–углублённое изучение отдельных тем учебной дисциплины для подготовки к устным опросам;

– изучение основной и дополнительной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;

– подготовка к письменным контрольным работам;

–систематизация полученных знаний при подготовке к зачету.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации образовательного процесса, обеспечиваются:

– наличием и использованием в образовательном процессе бизнес-мессенджера для групповой работы и общения Microsoft Teams;

– использованием «облачных» технологий, в частности облачного хранилища файлового хостинга компании Dropbox для размещения материалов по дисциплине;

– наличием и полной доступностью электронных вариантов курса лекций и учебно-методических указаний по основным разделам дисциплины.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещённые в бизнес-мессенджере для групповой работы и общения Microsoft Teams: шифр курса **YFO2I82.**

2. Методические указания к выполнению лабораторных работ по дисциплине «Программно-аппаратные и технические средства защиты информации» для студентов специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)», направления специальности 1-98 01 01-01 «Компьютерная безопасность (математические методы и программные системы)».

Содержание самостоятельной работы студентов

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины при подготовке к контрольным работам	*Тема 1.2 Программно-аппаратные средства идентификации и аутентификации.* Парольная защита информации от несанкционированного доступа. Повышение эффективности парольной защиты. Осн. лит.: [2], [3]. Доп. лит.: [4], [5], [18].	2
	Тема 2.2. Средства электронной подписи. Алгоритмы хеширования. Формирование электронной подписи. Осн. лит.: [2], [5], [6]. Доп. лит.: [1], [4], [5], [6].	2
	Тема 3.3. Программные и программно-аппаратные системы обнаружения вторжений. Системы обнаружения вторжений. Методы обнаружения сигнатур. Методы обнаружения аномалий. Проблемы безопасности систем обнаружения вторжений. Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [4], [8], [9], [11], [15].	2
	Тема 4.2. Методы и средства зашиты от вредоносных программ. Методы обнаружения вредоносных программ. Антивирусные программы и комплексы. Осн. лит.: [1], [2], [3]. Доп. лит.: [11], [12], [18].	2
	Тема 6.2. Обзор технических средств негласного съема акустической информации. Технические средства дистанционного съема информации. Технические средства съема информации с линий связи. Осн. лит.: [1], [4]. Доп. лит.: [3], [14], [19].	2
Подготовка к защите отчетов по лабораторным работам	**Лабораторная работа №1** Принципы, повышающие стойкость парольных методов опознания.	2
	Лабораторная работа №2 Определение требуемой вероятности правильного опознания для биометрических средств аутентификации.	2
	Лабораторная работа №3 Криптографические методы защиты данных в базах данных.	2
	Лабораторная работа №4 Работа с Центром управления безопасностью. Применение цифровой подписи к базам данных.	2

1	2	3
Подготовка к защите отчетов по лабораторным работам	**Лабораторная работа №5** Организация защиты баз данных в СУБД Microsoft Access.	2
	Лабораторная работа №6 Шифрование (SSL) соединения между браузером и серверным приложением.	2
	Лабораторная работа №7 Настройка системы предотвращения вторжений (IPS).	2
	Лабораторная работа №8 Настройка системы предотвращения вторжений (IPS).	2
	Лабораторная работа №9 Репликация базы данных. Резервирование и распределение баз данных.	2
	Лабораторная работа №10 Защита от атак типа внедрения SQL-кода.	2
	Лабораторная работа №11 Резервное копирование и восстановление баз данных.	2
	Лабораторная работа №12 Атаки MITM. Шифрование (SSL) соединения между серверным приложением и СУБД.	2
	Лабораторная работа №13 Мероприятия по выявлению каналов утечки информации.	2
	Лабораторная работа №14 Оценка первичных признаков элементов речевого сигнала.	2
	Лабораторная работа №15 *Выполнение контрольного задания.*	2
	ВСЕГО	**40**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Контроль качества усвоения знаний проводится в соответствии с Положением о рейтинговой системе оценки знаний и компетенций студентов (приказ ректора УО ПГУ № 294 от 06.06.2014 (в редакции, утверждённой приказом № 605 от 17.11.2014) в форме промежуточного контроля и текущей аттестации.

Мероприятия промежуточного контроля проводятся в течение семестра и включают в себя следующие формы контроля:

–устная форма (блиц-опрос на лекциях);

–письменная форма (тесты, контрольные работы, письменные отчёты по лабораторным работам);

–устно-письменная форма (отчёты по лабораторным с их устной защитой);

–техническая форма (электронные тесты, визуальные лабораторные работы).

Лабораторные работы предполагают выполнение и защиту. Последнее лабораторное занятие в семестре предусматривает выполнение и защиту зачётной работы, а также контрольное тестирование. При выполнении лабораторных работ выдаётся индивидуальное задание. Отчёт по лабораторной работе представляется в электронном виде. Содержание отчёта: название работы, вариант задания, анализ задания, ход выполнения работы, основные и промежуточные результаты, выводы по работе. Защита работ проводится индивидуально и оценивается в соответствии установленными правилами.

Результат *промежуточного контроля за семестр* оценивается отметкой в баллах по десятибалльной шкале и выводится, исходя из отметок, выставленных в ходе проведения мероприятий промежуточного контроля в течение семестра по следующей формуле:

$$П = \frac{(КТ_1 + ... + КТ_n) + (ЛР_1 + ЛР_{15}) + (КР_1 + КР_2)}{(17 + n)},$$

где $КТ_1 + ... + КТ_n$ – отметки, выставленные по результатам контрольного тестирования;

n – количество тестов;

$ЛР_1 + ЛР_{15}$ – отметки, выставленные по результатам защит лабораторных работ.

$КР_1$, $КР_2$ – отметки, выставленные по результатам контрольных работ.

Результат промежуточного контроля рассчитывается как округлённое среднее значение. Результат может быть увеличен в соответствии с п.п. 6.8 и 6.9 Положения.

Текущая аттестация проводится в форме зачёта.

Зачёт проводится согласно Положению.

Заключение о *зачёте* формируется на основе накопительного принципа по формуле:

$$З = k \cdot П,$$

где k– весовой коэффициент промежуточного контроля;

П – результат промежуточного контроля за семестр.

Весовой коэффициент k принимается равным 1.

Если полученная отметка $З < 4$ баллов, то проводится устный зачёт отдельно по представленным в программе вопросам.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основные методы (технологии) обучения, отвечающие целям и задачам учебной дисциплины:

– проблемное обучение (проблемное изложение, вариативное изложение), реализуемое на лекционных занятиях;

– учебно-исследовательская деятельность, реализация творческого подхода, реализуемые на лабораторных занятиях.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Программно-аппаратные и технические средства защиты информации» реализуют подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента, проявляющейся в чётком понимании им значимости всех видов выполняемых работ, как с точки зрения важности для профессиональной подготовки, так и с точки зрения оценивания. Подход предполагает использование элементов проблемного обучения и элементов исследовательской деятельности студентов в процессе аудиторной работы, а также при выполнении самостоятельных работ при постоянном рейтинговом контроле.

На лекционных занятиях по дисциплине «Программно-аппаратные и технические средства защиты информации» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных и лабораторных занятиях.

На лекционных занятиях студенты овладевают системой теоретических знаний в области программно-аппаратных средств защиты информации. В ходе лекционного изложения теоретических сведений используются традиционные словесные приёмы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий с опорой на имеющуюся начальную подготовку студентов и их политехнический кругозор, использованием интерактивных методов обучения.

На лабораторных занятиях развиваются и формируются необходимые практические умения и навыки построения программно-аппаратных систем защиты информации.

Применяется индивидуальный, творческий подход. Также во время проведения лабораторных работ особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её выполнения.