Учреждение образования «Полоцкий государственный университет»

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

_____ Н.А. Борейко
«28» 12 2020 г.
Регистрационный №УД-220/20/уч

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

(включая модуль «Основы управления интеллектуальной собственностью»)

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
1-28 01 02 «Электронный маркетинг»

2020 г.

Учебная программа составлена на основе типовой учебной программы для высших учебных заведений для направлениий образования 28; 39; 40; 41; 45; группы специальностей 36 04; специальностей 1-53 01 02; 1-53 01 07; 1-58 01 01; 1-98 01 02. Регистрационный № ТД-I.1347/тип. от 05.04.2016 и учебного плана по специальности 1-28 01 02 «Электронный маркетинг». Регистрационный №07-17/уч. ФЭФ от 30.06.2017 г.

СОСТАВИТЕЛЬ:
Ирина Брониславовна Бураченок, доцент кафедры технологий программирования учреждения образования «Полоцкий государственный университет», к.т.н.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования учреждения образования «Полоцкий государственный университет»
(протокол № 11 от « 11 » ноября 2020 г.);

Методической комиссией финансово-экономического факультета учреждения образования «Полоцкий государственный университет»
(протокол № 10 от « 30 » ноября 2020 г.);

Научно-методическим советом учреждения образования «Полоцкий государственный университет»
(протокол № 2 от « 28 » декабря 2020 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Основы защиты информации» ориентирована на обучение студентов базовым знаниям, умениям и навыкам в области защиты информации. Изучаемые темы представляются на основе современной нормативной регулятивной базы и национального законодательства. При построении учебной дисциплины «Основы защиты информации» использовались современные представления о процессах жизненного цикла защищённых информационных систем и парадигма их информационной безопасности.

Целью изучения учебной дисциплины «Основы защиты информации» является обучение студентов основам построения и использования современных защищённых информационных компьютерно-коммуникационных систем; подготовка специалистов, умеющих создавать защищённые информационные системы и исследовать защищённость компьютерно-коммуникационных систем.

Изучение данной дисциплины является необходимым этапом в профессиональном развитии «маркетолога-программиста».

Задачи изучения учебной дисциплины «Основы защиты информации». При изучении данной учебной дисциплины требуется разрешить две основные задачи: во-первых, дать студентам базовые знания в области защиты информации и информационной безопасности и, во-вторых, сформировать системное понимание проблем безопасности и путей их решения.

В результате изучения учебной дисциплины «Основы защиты информации» обучаемый должен:

знать:

–системную методологию и правовое обеспечение защиты информации;

–организационно-технические методы и технические средства защиты информации;

–основы криптографической защиты информации;

–особенности защиты информации в автоматизированных системах;

–основы положения международного и национального законодательства в области интеллектуальной собственности;

–порядок оформления и защиты прав на объекты интеллектуальной собственности;

уметь:

–определять возможные каналы утечки информации и обоснованно выбирать средства их блокирования;

–разрабатывать рекомендации по защите объектов различного типа от несанкционированного доступа;

–проводить патентные исследования;

–составлять заявки на выдачу охранных документов на объекты промышленной собственности;

–оформлять договора на передачу имущественных прав на объекты интеллектуальной собственности;

владеть:

–основными приёмами анализа вероятных угроз информационной безопасности для заданных объектов;

–способами введения объектов интеллектуальной собственности в гражданский оборот;

–способами передачи прав на использование объектов интеллектуальной собственности.

Требования к уровню освоения содержания учебной дисциплины. При изучении дисциплины «Основы защиты информации» у студентов 1-28 01 02 «Электронный маркетинг» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «маркетолог-программист», обеспечивающих выпускникам по указанной специальности успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

Академические компетенции.

АК-1 уметь применять базовые научно-теоретические знания для решения теоретических и практических задач;

АК-2 владеть системным и сравнительным анализом;

АК-3 владеть исследовательскими навыками;

АК-4 уметь работать самостоятельно;

АК-5 быть способным порождать новые идеи (обладать креативностью);

АК-6 владеть междисциплинарным подходом при решении проблемы;

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

АК-8 обладать навыками устной и письменной коммуникации;

АК-9 уметь учиться, повышать свою квалификацию в течение всей жизни;

АК-10 использовать основные законы естественнонаучных дисциплин в профессиональной деятельности;

АК-11 владеть основными методами, способами и средствами получения, хранения, переработки информации с использованием компьютерной техники;

АК-14 на научной основе организовывать свой труд, самостоятельно оценивать результаты своей деятельности.

Социально-личностные компетенции.

СЛК-1 обладать качествами гражданственности;

СЛК-2 быть способным к социальному взаимодействию;

СЛК-3 обладать способностью к межличностным коммуникациям;

СЛК-5 быть способным к критике и самокритике;

СЛК-6 уметь работать в команде.

Профессиональные компетенции.

Организационно-управленческая деятельность.

ПК-29 работать с юридической литературой и трудовым законодательством;

ПК-35 пользоваться глобальными информационными ресурсами;

Сформированные компетенции в области защиты информации являются базовыми при изучении всех последующих дисциплин специальности, при выполнении курсовых и дипломных работ.

Перечень дисциплин, в продолжение и на базе которых изучается дисциплина «Основы защиты информации». Учебная дисциплина «Основы защиты информации» непосредственно связана с изучаемой дисциплиной по специальности: «Основы алгоритмизации и программирования».

Перечень дисциплин, которые изучаются на базе дисциплины «Основы защиты информации». Материалы используются в дальнейшем при изучении дисциплин по специальности: «Распределённые системы обработки информации».

В соответствии с учебным планом по специальности 1-28 01 02 «Электронный маркетинг» на изучение учебной дисциплины отводится:

Форма получения высшего образования	дневная
Курс	2
Семестр	4
Всего часов	94
Всего аудиторных часов	52
В том числе:	
Лекции, часов	34
Практические (семинарские) занятия, часов	18
Самостоятельная работа, часов	42
Форма текущей аттестации	зачёт
Трудоёмкость дисциплины, зач. ед	2,5

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

Цели и задачи изучения дисциплины. Основные проблемы информационной безопасности. Законодательство РБ в области ЗИ. Приоритетные направления в РБ в области защиты информации.

Государственные органы и учреждения, занимающиеся вопросами защиты информации в РБ: Министерство связи и информатизации Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь, Научно-исследовательский институт технической защиты информации, Национальный центр интеллектуальной собственности, Государственный комитет по стандартизации Республики Беларусь, Белорусский государственный институт стандартизации и сертификации.

РАЗДЕЛ 1 СИСТЕМНАЯ МЕТОДОЛОГИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 1.1 Основы информационной безопасности

Отличительные черты информационного общества. Понятие информации. Потребители и обладатели информации. Компоненты безопасности. Общее понимание безопасности. Структура системы безопасности. Аспекты информационной безопасности. Цели и задачи, решение которых должна обеспечивает информационная безопасность.

Тема 1.2 Системная методология информационной безопасности

Основные понятия и терминология в области защиты информации. Классификация угроз. Охраняемые сведения и демаскирующие признаки. Классификация методов защиты информации.

РАЗДЕЛ 2 ПРАВОВОЕ ОБЕСПЕЧЕНИЕ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 2.1 Правовое обеспечение защиты информации

Закон РБ от 6 сентября 1995 г. № 3850-XII «Об информатизации». Закон РБ от 29 ноября 1994 г. № 3411-XII «О государственных секретах». Закон РБ от 3 декабря 1997 г. № 102-З «Об органах государственной безопасности Республики Беларусь». Постановление Совета Министров РБ от 15 февраля 1999 г. № 237 «О служебной информации ограниченного распространения». Постановление Совета Министров РБ от 10 февраля 2000 г. № 186 «О некоторых мерах по защите информации в Республике Беларусь». Указ Президента Республики Беларусь от 12 мая 2004 г. № 231 «Вопросы Государственного центра безопасности информации при Президенте Республики Беларусь».

Тема 2.2 Правовые методы защиты информации

Правовая защита от компьютерных преступлений.

Тема 2.3 Виды компьютерных преступлений

Примеры известных компьютерных преступлений. Виды компьютерных преступлений, мошенничество в интернете. Использование специальных программных средств мошенниками. Полезные советы по компьютерной безопасности.

Тема 2.4 Компьютерные вирусы и антивирусные программы

Понятие вирус. История компьютерных вирусов. Классификация компьютерных вирусов. Особенности алгоритмов работы вирусов. Деструктивные возможности и пути проникновения вирусов. Методы защиты от вирусов.

РАЗДЕЛ 3 ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 3.1 Государственное регулирование в области защиты информации

Положения государственной политики информационной безопасности РБ. Система информационной безопасности РБ. Государственная система защиты РБ. Основные функции системы информационной безопасности. Мероприятия по защите информации.

Тема 3.2 Лицензирование деятельности юридических и физических лиц в области защиты информации

Основные виды лицензируемой деятельности. Основные требования к организациям, претендующим на получение лицензий на работы в области защиты информации. Сертификация и аттестация средств защиты информации. Организационно-административные и организационно-технические методы защиты информации. Страхование как метод защиты информации.

РАЗДЕЛ 4 ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема 4.1 Классификация технических каналов утечки информации

Классификация каналов утечки информации. Понятие речевого сигнала. Каналы утечки речевой информации. Пассивные и активные методы защиты информации от утечки по техническим каналам.

Тема 4.2 Обзор технических средств негласного съёма акустической информации

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

Тема 4.3. 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 4.4 Звуковые сигналы

Звуковые сигналы. Пример создания гармонического и полигармонического сигнала. Основные характеристики гармонического сигнала. Энергетический спектр речевого сигнала.

Тема 4.5 Применение шумов для маскирования речевых сигналов

Маскирование речевых сообщений. Понятие шума. Основные характеристики шума. Примеры построения гистограммы распределения плотности вероятности шума. Синтез смеси гармонического сигнала и шума с заданным отношением сигнал/шум.

Тема 4.6 Методика и порядок проведения мероприятий по выявлению и исследованию КУИ

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

Тема 4.7 Использование вейвлетов в задачах обработки и распознавания речи

Возможности вейвлет-анализа. Особенности комплексного вейвлета Морле.

РАЗДЕЛ 5 МАШИНОЧИТАЕМЫЕ ТЕХНОЛОГИИ – МОЩНАЯ СОВРЕМЕННАЯ ЗАЩИТА

Тема 5.1 Стеганографические системы защиты информации

Понятие стеганографии. Основные достоинства стеганографии. Компьютерная стеганография. Стеганография – эффективная защита печатной продукции. Машиночитаемые технологии для традиционных способов печати. Методы компьютерной стеганографии. Разработка новых машиночитаемых защитных признаков. Производственный контроль.

Тема 5.2 Криптографические методы защиты информации

Основные понятия: криптология, криптография, криптоанализ. Коды, шифры и ключи: открытые и закрытые. Основная схема криптографии.

Тема 5.3 Основы защиты автоматизированных систем от несанкционированного доступа

Автоматизированная банковская система глазами хакера. Возможные атаки автоматизированной банковской системы. Возможные атаки на уровне сети. Меры защиты от атак на сетевом уровне. Основные правила организации защиты АСБ. Основные нормативные документы по оценке безопасности.

Тема 5.4 Электронный документ и электронная цифровая подпись

Понятие электронного документа. Придание юридического статуса электронным документам. Юридическая сила оригинала и копии электронного документа. Электронная цифровая подпись. Сертификат открытого ключа. Удостоверяющий центр. Угрозы цифровой подписи. RSA как фундамент электронной цифровой подписи.

Тема 5.5 Уникальная и точная идентификация продуктов и банковских счетов

Основа современного общества стандартизированные коды банков, супермаркетов и других крупных подсистем экономики –кредитные карты. Алгоритм Луна. Шрихкоды.

РАЗДЕЛ 6 ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Тема 6.1 Объекты интеллектуальной собственности

Мир вещей и результаты интеллектуальной деятельности. Объекты интеллектуальной собственности. Базы данных. Промышленная собственность. Авторское право и смежные права. Коммерческое использование объектов интеллектуальной собственности. Государственное управление интеллектуальной собственностью.

Тема 6.2 Патентная информация

Источники патентной информации. Международная патентная классификация. Патентный документ. Примеры патентных документов. Поиск патентной информации в Интернет.

Тема 6.3 Товарные знаки

Товарные знаки: определение. Виды товарных знаков. Права на товарный знак. Нарушение прав на товарные знаки.

Учебно-методическая карта учебной дисциплины «Основы защиты информации»
Дневная форма получения высшего образования

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	Практические занятия	Лабораторные занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
	Введение в дисциплину	**2**					
1	**Лекция № 1** Цели и задачи изучения дисциплины. Основные проблемы информационной безопасности. Законодательство РБ в области ЗИ. Приоритетные направления в РБ в области защиты информации. Государственные органы и учреждения, занимающиеся вопросами защиты информации в РБ: Министерство связи и информатизации Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь, Научно-исследовательский институт технической защиты информации, Национальный центр интеллектуальной собственности, Государственный комитет по стандартизации Республики Беларусь, Белорусский государственный институт стандартизации и сертификации.	2				Осн. лит.: [3], [5], [12]. Эл. рес.: [1], [3], [4], [6], [9], [13] Online библ.: [5]	

1	2	3
	Раздел 1 Системная методология информационной безопасности	**2**
2	**Лекция № 2** *Тема 1.1 Основы информационной безопасности* Отличительные черты информационного общества. Понятие информации. Потребители и обладатели информации. Компоненты безопасности. Общее понимание безопасности. Структура системы безопасности. Аспекты информационной безопасности. Цели и задачи, решение которых должна обеспечивает информационная безопасность. *Тема 1.2 Системная методология информационной безопасности* Основные понятия и терминология в области защиты информации. Классификация угроз. Охраняемые сведения и демаскирующие признаки. Классификация методов защиты информации.	2
3	**Практическая работа №1** Изучение Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (утверждён Постановлением Совета Министров Республики Беларусь 15.05.2013 № 375).	
	Раздел 2 Правовое обеспечение и методы защиты информации	**4**
4	**Лекция № 3** *Тема 2.1 Правовое обеспечение защиты информации* Закон РБ от 6 сентября 1995 г. № 3850-XII «Об информатизации». Закон РБ от 29 ноября 1994 г. № 3411-XII «О государственных секретах». Закон РБ от 3 декабря 1997 г. № 102-З «Об органах государственной безопасности РБ». Постановление Совета Министров РБ от 15 февраля 1999 г. № 237 «О служебной информации ограниченного распространения». Постановление Совета Министров РБ от 10 февраля 2000 г. № 186 «О некоторых мерах по защите информации в РБ». Указ Президента РБ от 12 мая 2004 г. № 231 «Вопросы Государственного центра безопасности информации при Президенте РБ».	2

	4	5	6	7	8
	2				
				Осн. лит.: [3], [5], [7], [12], [14], [15]-[19], [21], [22]. Доп. лит.: [6], [18]. Эл. рес.: [1], [3], [5], [9], [15]. Online библ.:[4], [5].	*Контрольное тестирование №1
	2				Защита отчёта по практическому занятию № 1
	2				
				Осн. лит.: [3], [5], [14]. Эл. рес.: [1], [2], [11].	

1	2	3	4
	Тема 2.2 Правовые методы защиты информации Правовая защита от компьютерных преступлений. *Тема 2.3 Виды компьютерных преступлений* Примеры известных компьютерных преступлений. Виды компьютерных преступлений, мошенничество в интернете. Использование специальных программных средств мошенниками. Полезные советы по компьютерной безопасности.		
5	**Лекция № 4** *Тема 2.4 Компьютерные вирусы и антивирусные программы* Понятие вирус. История компьютерных вирусов. Классификация компьютерных вирусов. Особенности алгоритмов работы вирусов. Деструктивные возможности и пути проникновения вирусов. Методы защиты от вирусов.	2	
6	**Практическая работа №2** Правовое обеспечение информационной безопасности.		
	Раздел 3 Организационные методы защиты информации	**4**	
7	**Лекция № 5** *Тема 3.1 Государственное регулирование в области защиты информации* Положения государственной политики информационной безопасности РБ. Система информационной безопасности РБ. Государственная система защиты РБ. Основные функции системы информационной безопасности. Мероприятия по защите информации.	2	
8	**Лекция № 6** *Тема 3.2 Лицензирование деятельности юридических и физических лиц в области защиты информации* Основные виды лицензируемой деятельности. Основные требования к организациям, претендующим на получение лицензий на работы в области защиты информации. Сертификация и аттестация средств защиты информации. Организационно-	2	

4	5	6	7	8
			Осн. лит.: [4], [10], [13], [23]. Доп. лит.: [11]. Эл. рес.: [9], [11]. Online библ.: [4].	
			Осн. лит.: [4], [10], [13]. Доп. лит.: [7].	*Контрольное тестирование №2
2				Защита отчёта по практическому занятию № 2
2				
			Осн. лит.: [3], [14], [16]. Доп. лит.: [2].	
			Осн. лит.: [3], [14]. Доп. лит.: [1], [9], [18].	*Контрольное тестирование №3

	административные и организационно-технические методы защиты информации. Страхование как метод защиты информации.		
9	**Практическая работа №3** Выявление и фиксация следов противоправной деятельности на ПЭВМ.		2
1	2	3	4
	Раздел 4 Инженерно-техническая защита объектов от несанкционированного доступа	**10**	**4**
10	**Лекция № 7** *Тема 4.1 Классификация технических каналов утечки информации* Классификация каналов утечки информации. Понятие речевого сигнала. Каналы утечки речевой информации. Пассивные и активные методы защиты информации от утечки по техническим каналам. *Тема 4.2 Обзор технических средств негласного съёма акустической информации* Необходимость технической защиты информации. Классификация технических средств съёма акустической информации. Закладочные устройства. Технические средства дистанционного съёма информации. Технические средства съёма информации с линий связи.	2	
11	**Лекция № 8** *Тема 4.3. 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 4.4 Звуковые сигналы* Звуковые сигналы. Пример создания гармонического и полигармонического сигнала. Основные характеристики гармонического сигнала. Энергетический спектр речевого сигнала.	2	
12	**Практическая работа №4** Оценка первичных признаков элементов речевого сигнала.		2

			Защита отчёта по практическому занятию № 3
5	6	7	8
		Осн. лит.: [9], [24]. Доп. лит.: [2], [15]. Осн. лит.: [9], [2], [3]. Доп. лит.: [2], [12]. Online библ.: [2], [3], [4].	
		Осн. лит.: [1], [2], [7], [9], [11]. Доп. лит.: [18]. Осн. лит.: [1]. Доп. лит.: [13], [14]. Online библ.: [3], [4].	*Контрольное тестирование №4
			Защита отчета по практическому занятию № 4

13	**Лекция № 9** *Тема 4.5 Применение шумов для маскирования речевых сигналов* Маскирование речевых сообщений. Понятие шума. Основные характеристики шума. Примеры построения гистограммы распределения плотности вероятности шума. Синтез смеси гармонического сигнала и шума с заданным отношением сигнал/шум.	2	
1	2	3	4
14	**Лекция № 10** *Тема 4.6 Методика и порядок проведения мероприятий по выявлению и исследованию КУИ* Аттестация объектов информатизации. Методика и порядок проведения мероприятий по выявлению и исследованию КУИ. Специальные проверки. Специальные обследования. Специальные исследования. Методика оценки словесной разборчивости речи.	2	
15	**Практическая работа №5** Создание маскирующего шума для имитации виброакустического зашумления.		2
16	**Лекция № 11** *Тема 4.7 Использование вейвлетов в задачах обработки и распознавания речи* Возможности вейвлет-анализа. Особенности комплексного вейвлета Морле.	2	
	Раздел 5 Машиночитаемые технологии – мощная современная защита	**8**	4
17	**Лекция № 12** *Тема 5.1 Стеганографические системы защиты информации* Понятие стеганографии. Основные достоинства стеганографии. Компьютерная стеганография. Стеганография – эффективная защита печатной продукции. Машиночитаемые технологии для традиционных способов печати. Методы компьютерной стеганографии. Разработка новых машиночитаемых защитных признаков. Производственный контроль.	2	
18	**Практическая работа №6** Мероприятия по выявлению каналов утечки информации (специальные проверки, специальные обследования, специальные исследования).		1

			Осн. лит.: [1], [2], [8]. Доп. лит.: [18].	
4	5	6	7	8
			Осн. лит.: [8]. Доп. лит.: [18].	*Контрольное тестирование №5
2				Защита отчета по практическому занятию № 5
			Осн. лит.: [8], [11]. Доп. лит.: [10], [17].	
4				
			Осн. лит.: [11]. Доп. лит.: [4], [7].	
2				Защита отчета по практическому занятию № 6

19	**Лекция № 13** *Тема 5.2 Криптографические методы защиты информации* Основные понятия: криптология, криптография, криптоанализ. Коды, шифры и ключи: открытые и закрытые. Основная схема криптографии.	2	
1	2	3	4
	Тема 5.3 Основы защиты автоматизированных систем от несанкционированного доступа Автоматизированная банковская система глазами хакера. Возможные атаки автоматизированной банковской системы. Возможные атаки на уровне сети. Меры защиты от атак на сетевом уровне. Основные правила организации защиты АСБ. Основные нормативные документы по оценке безопасности.		
20	**Лекция № 14** *Тема 5.4 Электронный документ и электронная цифровая подпись* Понятие электронного документа. Придание юридического статуса электронным документам. Юридическая сила оригинала и копии электронного документа. Электронная цифровая подпись. Сертификат открытого ключа. Удостоверяющий центр. Угрозы цифровой подписи. RSA как фундамент электронной цифровой подписи.	2	
21	**Практическая работа №7** Изучение методов защиты информации с помощью различных видов шифров, используемых в криптографии.		2
22	**Лекция № 15** *Тема 5.5 Уникальная и точная идентификация продуктов и банковских счётов* Основа современного общества стандартизированные коды банков, супермаркетов и других крупных подсистем экономики – кредитные карты. Алгоритм Луна. Шрихкоды.	2	
	Раздел 6 Защита интеллектуальной собственности	**4**	4
23	**Лекция № 16** *Тема 6.1 Объекты интеллектуальной собственности*	2	

			Осн. лит.: [6], [7], [12]. Доп. лит.: [18], [22].	
4	5	6	7	8
			Осн. лит.: [6], [2]. Доп. лит.: [1], [5], [12]. Online библ.: [1], [7]. Эл. рес.: [14].	
			Осн. лит.: [6], [7], [12], [24] Доп. лит.: [18], [22]. Online библ.: [1], [7].	*Контрольное тестирование №6
2				Защита отчёта по практическому занятию № 7
			Осн. лит.: [7], [12]. Online библ.: [6].	
4				
			Осн. лит.: [25], [26].	

	Мир вещей и результаты интеллектуальной деятельности. Объекты интеллектуальной собственности. Базы данных. Промышленная собственность. Авторское право и смежные права. Коммерческое использование объектов интеллектуальной собственности. Государственное управление интеллектуальной собственностью.					Доп. лит.: [18]. Online библ.: [8].	
	Тема 6.2 Патентная информация Источники патентной информации. Международная патентная классификация. Патентный документ. Примеры патентных документов. Поиск патентной информации в Интернет.					Осн. лит.: [9]. Online библ.: [8].	
1	2	3	4	5	6	8	9
24	**Лекция № 17** *Тема 6.3 Товарные знаки* Товарные знаки: определение. Виды товарных знаков. Права на товарный знак. Нарушение прав на товарные знаки.	2				Осн. лит.: [9]. Доп. лит.: [18]. Online библ.: [8].	*Реферативное выступление с докладом
25	**Практическая работа №8** Исследование разборчивости речи методом артикуляционных измерений при защите речевой информации различными видами маскирующих сигналов.		2				Защита отчета по практическому занятию № 8
26	**Практическая работа №9** Поиск патентной информации в электронных базах: Патентного ведомства Республики Беларусь. Роспатента. Европейского патентного ведомства. Патентного ведомства США.		2				Защита отчета по практическому занятию № 9
	Всего	**34**	**18**				

* мероприятия промежуточного контроля

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Богуш, В.А. Электромагнитные излучения. Методы и средства защиты. / В.А. Богуш, Т.В. Борботько, А.В. Гусинский. / Под ред. Л.М. Лынькова. – Мн.: Бестпринт, 2003.

2. Бузов Г.А. Выявление специальных технических средств несанкционированного получения информации/ Г.А. Бузов, М.: Горячая линия – Телеком, 2019 – 204 с.

3. Герасименко, В.А. Основы защиты информации. / В.А. Герасименко, А.А. Малюк – М.: МИФИ, 1997 – 537 с.

4. Гладких, А.А. Мошенничество в интернете. / А.А. Гладких. – М.: Litres, 2012. – 62 с.

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Взамен: ГОСТ Р 50922-96; введ. 2008-02-01. – М.: Стандартинформ, 2007. – 12 с.

6. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / А. А. Внуков. – 2-е изд., испр. и доп. – Москва: Издательство Юрайт, 2021. – 246 с.

7. Домарев, В.В. Безопасность информационных технологий. Методология создания систем защиты. / В.В. Домарев. – К.:000 ТИД «ДС», 2001. – 688 с.

8. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк. – СПб.: ГУАП, 2006. – 188 с.

9. Зайцев, А.П. Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. – Москва: Горячая линия-Телеком, 2017 – 442 с.

10. Касперский, Крис Компьютерные вирусы внутри и снаружи. / Крис Касперский. – СПб.: ПИТЕР, 2006. – 526с.

11. Каторин, Ю. Ф. Защита информации техническими средствами [Электронный ресурс]: учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак. – Санкт-Петербург: НИУ ИТМО, 2012. – 416 с. // Электронно-библиотечная система «Лань» – Режим доступа: по подписке: URL: https://e.lanbook.com/book/40850.

12. Куприянов, А.И. Основы защиты информации. / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. – М.: Радиоэлектроника, 2006. – 256 с.

13. Михайлов, Д.М. Защита мобильных телефонов от атак. / Д.М. Михайлов, И.Ю. Жуков. / Под ред. А.М. Ивашко. – М.: Фойлис, 2011. – 189 с.

14. «Об информатизации»: Закон Республики Беларусь от 6 сентября 1995г. № 3850-XII // Ведомости Верховного Совета Республики Беларусь. Ноябрь 1995 г. № 33(179), ст. 428.

15. СТБ 34.101.1-2004 (ИСО/МЭК 15408.1-99) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

16. СТБ 34.101.2-2004 (ИСО/МЭК 15408.2-99) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

17. СТБ 34.101.28-2011 «Информационные технологии. Средства защиты речевой информации виброакустические. Классификация и общие технические требования».

18. СТБ 34.101.3-2004 (ИСО/МЭК 15408.3-99) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности.

19. СТБ II ИСО/МЭК 17799-2000/2004 Информационные технологии и безопасность. Правила управления информационной безопасностью.

20.СТБ ISO/IEC 27001 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

21.СТБ П ИСО/МЭК 27001-2008 Информационные технологии. Технологии безопасности. Системы управления зашитой информации. Требования.

22.ТР 2013/027/BY – Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность».

23.Уголовный Кодекс Республики Беларусь // Национальный реестр правовых актов Республики Беларусь. 15 октября 1999г. № 76.

24.Халяпин, Д.Б. Защита информации. Вас подслушивают? Защищайтесь! /Д.Б. Халяпин. – М.: НОУ ШО «Баярд», 2004 – 432 с.

25.Якимахо, А.П. Управление интеллектуальной собственностью в Республике Беларусь / под ред. Г.Е. Ясникова. – Минск: Дикта, 2011. – 323 с.

26.Кудашов, В.И. Основы управления интеллектуальной собственностью: учебник. – Минск: ИВЦ Минфина, 2013. – 407 с. – Утверждено Министерством образования Республики Беларусь в качестве учебника для студентов учреждений высшего образования по естественнонаучным, экономическим и техническим специальностям.

Дополнительная:

1.Астахов, А.М. Искусство управления информационными рисками. / А.М. Астахов. – М.: ДМК Пресс, 2010. – 312с.

2.Галатенко, В.А. Основы информационной безопасности: курс лекций. / В.А. Галатенко. – М.: Интернет-Университет Информационных Технологий, 2003. – 280 с.

3.Герасименко, В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. Кн.1. / В.А. Герасименко. – М.: Энергоатомиздат, 1994. – 400 с.

4.Герасименко, В.А. Основы информационной грамоты. / В.А. Герасименко. – М.: Энсргоатомиздат, 1996. –320 с

5.Голдовский, И. Безопасность платежей в Интернете. / И. Голдовский. – СПб.: Питер, 2001. – 240с.

6.Гостехкомиссия России. Руководящий документ. Положение по аттестации объектов информатизации по требованиям безопасности информации. – М. : Изд-во стандартов, 1994. – 31 с.

7.Девянин, П.Н. Теоретические основы компьютерной безопасности: учебное пособие для вузов. / П.Н.Девянин, О.О. Михальский, Д.И. Правиков, А.Ю. Щербаков. – М.: Радио и связь, 2000. – 192с.

8.Конеев, И.Р. Информационная безопасность предприятия. / И.Р. Конеев – СПб.: БХВ-Петербург, 2003. – 752 с.

9.Курило, А.И. Аудит информационной безопасности. / А.И. Курило, СЛ. Зефиров, В.Б. Голованов и др. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.

10.Петухов, А.П. Введение в теорию базисов всплесков. / А.П. Петухов. – СПб.: Изд-во СПбГТУ. – 1999. – 132 с.

11.Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие. / Ю.А. Родичев. – СПб.: Питер, 2008.

12.Семкин, С.И. Основы организационного обеспечения информационной безопасности объектов информатизации. / С.И. Семкин, Э.В. Беляков, С.В. Гребнев, В.И. Козачок. – М.: Гелиос АРВ, 2005. – 192с.

13.Фант, Г. Акустическая теория речеобразования / Г. Фант. – М. : Наука, 1964. – 283 с.

14.Фланаган, Дж. Анализ, синтез и восприятие речи / Дж. Фланаган ; пер. с англ. под ред. А. А. Пирогова. – М. : Связь, 1968. – 396 с.

15. Цирлов, В. Л. Основы информационной безопасности: краткий курс. / В. Л. Цирлов. – Ростов н/Д: Феникс, 2008. – 253с. – (Профессиональное образование).

16. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. / В.Ф. Шаньгин. – М.: ИД «Форум»: ИНФРА-М, 2009. – 416 с. (Профессиональное образование).

17. Штарк, Г.Г. Применение вейвлетов для ЦОС. / Г.Г. Штарк. – М.: Техносфера, 2007. –192 с.

18. Ярочкин, В.И. Информационная безопасность: учебник для ВУЗов. Изд. 2. / В.И. Ярочкин. – Мн.: Академический проект, 2005. – 544 с.

19. Голенда, К. Защита информации : Учеб. пособие / Л. К. Голенда, М. А. Челноков, Л. А. Попкова. - Мн. : БГЭУ, 2000. – 35с.

20. Арутюнов, В.В. Защита информации : учеб.-метод. пособие / В. В. Арутюнов. –М. : ЛИБЕРЕЯ-БИБИНФОРМ, 2008. – 55 с.

21. Лукашов, А.И. Конфиденциальная информация и коммерческая тайна : правовое регулирование и организация защиты / А. И. Лукашов, Г. Н. Мухин. – Мн. : Тесей, 1998. –128с.

22. Богуш, Р.П. Основы защиты информации : учеб.-метод. комплекс для слушателей ИПК спец. 1-40 01 73 «Программное обеспечение информационных систем» / Р. П. Богуш, А. В. Курилович ; М-во образования РБ, Полоцкий гос. ун-т. – Новополоцк : ПГУ, 2009. –95 с. – Библиогр.: с 94. – См. также эл. копию. – Adobe Acrobat Document.

Университетская библиотека онлайн:

1. Аверченков, В.И. Защита персональных данных в организации [Электронный ресурс] : монография / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин ; В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – 3-е изд., стер. – Москва: Издательство «Флинта», 2016. – 124 с. – Библиогр. в кн. // Университетская библиотека онлайн. Режим доступа: https://biblioclub.ru.

2. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс] : учебное пособие / А. М. Голиков ; А.М. Голиков; Министерство образования и науки Российской Федерации; Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Библиогр. в кн. // Университетская библиотека онлайн. Режим доступа: https://biblioclub.ru.

3. Голиков, А.М. Защита информации от утечки по техническим каналам [Электронный ресурс] : учебное пособие / А. М. Голиков ; А.М. Голиков; Министерство образования и науки Российской Федерации; Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. - Библиогр.: // Университетская библиотека онлайн. Режим доступа: https://biblioclub.ru.

4. Смирнов, В. И. Защита информации [Электронный ресурс] : лабораторный практикум / В. И. Смирнов ; В.И. Смирнов; Поволжский государственный технологический университет. – Йошкар-Ола : ПГТУ, 2017. – 67 с. : ил. – Библиогр. в кн. // Университетская библиотека онлайн. Режим доступа: https://biblioclub.ru.

5. Диогенес, Ю. Кибербезопасность. Стратегия атак и обороны [Электронный ресурс] / Ю. Диогенес, Э. Озкайя; перевод с английского Д. А. Беликова. – Москва: ДМК Пресс, 2020. – 326 с.// Электронно-библиотечная система «Лань» – Режим доступа: по подписке: URL: https://e.lanbook.com/book/131717

6. Мошенничество в платежной сфере: бизнес-энциклопедия [Электронный ресурс]. – Москва : Интеллектуальная Литература, 2016. – 345 с. : табл., схем. – Режим доступа: по подписке: URL: http://biblioclub.ru/index.php?page=book&id=430951

7. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии [Электронный ресурс]: учебник / М. В. Тумбинская, М. В. Петровский. – Санкт-Петербург: Лань, 2019. – 344 с. // Электронно-библиотечная система Лань :. – URL: https://e.lanbook.com/book/125739

8. Сычев, А. Н. Защита интеллектуальной собственности и патентоведение [Электронный ресурс] : учебное пособие / А.Н. Сычев. – Томск : Эль Контент, 2012. – 160 с. – Допущено Министерством образования Российской Федерации в качестве учебника для студентов высших учебных заведений. – Режим доступа: по подписке: URL: http://biblioclub.ru/index.php?page=book&id=208697

Электронные ресурсы:

1. International Organization for Standardization (Международная Организация Стандартизации). [Электрон, ресурс]. – Режим доступа: http://www.iso.org (http://www.iso.ch). – Дата доступа: 19.03.2018.

2. Your Private Network (Лаборатория Сетевой Безопасности). [Электрон, ресурс]. – Режим доступа: http://ypn.ru/177/international-standards-of-information-technologies-security. – Дата доступа: 19.03.2018.

3. Государственный комитет по стандартизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: http://www.tnpa.by. – Дата доступа: 19.03.2018.

4. Государственный комитет по стандартизации. [Электрон, ресурс]. – Режим доступа: http://www.gosstandart.goy.by. – Дата доступа: 19.03.2018.

5. Закон Республики Беларусь 19 июля 2010 г. №170-З «О Государственных Секретах». [Электрон, ресурс]. – Режим доступа: http://www.minfin.gov.by/upload/gosznak/acts/zakon_190710_170z.pdf. – Дата доступа: 19.03.2018.

6. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации». [Электрон, ресурс]. – Режим доступа: http://www.pravo.by/main.aspx?guid=3871&p0=h10800455&p2={NRPA}. – Дата доступа: 19.03.2018.

7. Креопалов, В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебно-практическое пособие / В.В. Креопалов. – М.: Евразийский открытый институт, 2011. – 278 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=90753. – Дата доступа: 19.03.2018.

8. Министерство связи и информатизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: http://www.mpt.gov.by. – Дата доступа: 19.03.2018.

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

10. Национальный открытый университет. [Электрон, ресурс]. – Режим доступа: http://www.intuit.ru. – Дата доступа: 19.03.2018.

11. Национальный правовой портал Республики Беларусь. [Электрон, ресурс]. – http://www.pravo.by. – Дата доступа: 19.03.2018.

12. Национальный центр интеллектуальной собственности. [Электрон, ресурс]. – Режим доступа: http://www.belgospatent.org.by. – Дата доступа: 19.03.2018.

13. Оперативно-аналитический центр при Президенте Республики Беларусь [Электрон, ресурс]. – Режим доступа: http://oac.gov.by. – Дата доступа: 19.03.2018.

14. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс]: учебное пособие / В.А. Сердюк; Высшая Школа Экономики Национальный Исследовательский Университет. – М.: Издательский дом Государственного

университета Высшей школы экономики, 2015. – 574 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=440285. – Дата доступа: 19.03.2018.

15. Системы защиты информации в ведущих зарубежных странах [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 4-е изд., стер. – М.: Флинта, 2016. – 224 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=93351. – Дата доступа: 19.03.2018.

Перечень компьютерных программ:

Используются пакеты: Matlab; Mathcad; NI LabView.

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическая работа №1 Изучение Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (утверждён Постановлением Совета Министров Республики Беларусь 15.05.2013 № 375).

Практическая работа №2 Правовое обеспечение информационной безопасности.

Практическая работа №3 Выявление и фиксация следов противоправной деятельности на ПЭВМ.

Практическая работа №4 Оценка первичных признаков элементов речевого сигнала

Практическая работа №5 Создание маскирующего шума для имитации виброакустического зашумления.

Практическая работа №6 Мероприятия по выявлению каналов утечки информации (специальные проверки, специальные обследования, специальные исследования).

Практическая работа №7 Изучение методов защиты информации с помощью различных видов шифров, используемых в криптографии.

Практическая работа №8 Исследование разборчивости речи методом артикуляционных измерений при защите речевой информации различными видами маскирующих сигналов.

Практическая работа №9 Поиск патентной информации в электронных базах: Патентного ведомства Республики Беларусь. Роспатента. Европейского патентного ведомства. Патентного ведомства США.

ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

1. Понятие SQL-инъекции и меры борьбы.
2. Примеры использования электронной цифровой подписи в Республике Беларусь.
3. Шумы в нашей жизни и их влияние на здоровье человека.
4. Шумовое оружие.
5. Что необходимо знать при использовании паролей.
6. Компьютерная стеганография в нашей жизни.
7. Существующие в мире механические системы защиты.
8. Приёмы безопасного использования личной и корпоративной электронной почты.
9. Защита от атак на сетевом уровне.
10. Приёмы навыки безопасного использования мобильных устройств.
11. Порядок действий в случае несанкционированного взлома вашего аккаунта.
12. Понятие клиппирования сигнала и области применения.
13. Виды маскирующих шумов и способы их применения.
14. Примеры стандартизированных кодов банков, супермаркетов и других крупных подсистем экономики.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

Введение

1. Сформулируйте цель и основные задачи изучения дисциплины «Основы защиты информации».

2. Назовите основные проблемы информационной безопасности в современном мире.

3. Какие законы РБ в области защиты информации вы знаете? Назовите приоритетные направления в РБ в области защиты информации.

4. Укажите государственные органы и учреждения, занимающиеся вопросами защиты информации в РБ.

5. Назовите отличительные черты информационного общества. Дайте понятие информации.

6. Разделите понятия потребители и обладатели информации.

7. Перечислите основные компоненты безопасности. Что понимается под безопасностью?

8. Приведите основные элементы в структуре системы безопасности.

9. Перечислите аспекты информационной безопасности.

10. Укажете задачи, решение которых должна обеспечивает информационная безопасность.

Раздел 1 Системная методология информационной безопасности

11. Что включает в себя системная методология информационной безопасности?

12. Сформулируйте основные понятия в области защиты информации.

13. Приведите классификацию угроз. Приведите полную классификацию методов защиты информации.

14. Что относится к охраняемым сведениям? Приведите примеры демаскирующих признаков.

Раздел 2 Правовое обеспечение и методы защиты информации

15. Расскажите, что вы знаете о содержании Закона РБ от 6 сентября 1995 г. № 3850-XII «Об информатизации»?

16. Расскажите, что вы знаете о содержании Закона РБ от 29 ноября 1994 г. № 3411-XII «О государственных секретах».

17. Расскажите, что вы знаете о содержании Закона РБ от 3 декабря 1997 г. № 102-З «Об органах государственной безопасности Республики Беларусь».

18. Приведите основное содержание Постановления Совета Министров РБ от 15 февраля 1999 г. № 237 «О служебной информации ограниченного распространения».

19. Приведите основное содержание Постановления Совета Министров РБ от 10 февраля 2000 г. № 186 «О некоторых мерах по защите информации в Республике Беларусь».

20. Что содержится в Указе Президента Республики Беларусь от 12 мая 2004 г. № 231 «Вопросы Государственного центра безопасности информации при Президенте Республики Беларусь»?

21. Что включает в себя правовая защита от компьютерных преступлений?

22. Перечислите виды компьютерных преступлений. Приведите примеры наиболее известных компьютерных преступлений, принёсших значительный ущерб.

23. Какие существуют виды компьютерных преступлений? Что вам известно о мошенничестве в интернете.

24. Какие специальные программные средства используют мошенники в интернет?

25. Какими правилами следует руководствоваться, чтобы обезопасить себя от мошенничества в интернет?

26. Что вам известно о компьютерных вирусах и антивирусных программах? Приведите наиболее значимые исторические факты о компьютерных вирусах.

27. Дайте понятие вирус. Приведите пример классификации компьютерных вирусов.

28. Расскажите об особенностях алгоритмов работы наиболее распространённых вирусов, вредоносного программного обеспечения. Деструктивные возможности и пути проникновения вирусов. Какие существуют методы защиты от компьютерных вирусов?

Раздел 3 Организационные методы защиты информации

29. Что означает Государственное регулирование в области защиты информации?

30. Сформулируйте основные положения государственной политики информационной безопасности РБ.

31. Дайте понятия «Система информационной безопасности РБ», «Государственная система защиты РБ».

32. Перечислите основные функции системы информационной безопасности. Какие проводятся в Республике мероприятия по защите информации?

33. Что вам известно о лицензировании деятельности юридических и физических лиц в области защиты информации.

34. Перечислите основные виды лицензируемой деятельности и основные требования к организациям, претендующим на получение лицензий на работы в области защиты информации.

35. Расскажите, как осуществляется сертификация и аттестация средств защиты информации.

36. Что включают в себя организационно-административные и организационно-технические методы защиты информации?

37. Расскажите о страховании как методе защиты информации.

Раздел 4 Инженерно-техническая защита объектов от несанкционированного доступа

38. Что такое технический канал утечки информации. Приведите классификацию технических каналов утечки информации.

39. Дайте понятие речевого сигнала. Какие утечки речевой информации вы знаете? Охарактеризуйте каждый из них.

40. Что вам известно о пассивных и активных методах защиты информации от утечки по техническим каналам?

41. Приведите обзор технических средств негласного съёма акустической информации. Почему возникает необходимость технической защиты информации?

42. Приведите классификацию технических средств съёма акустической информации. Что вам известно о закладочных устройствах?

43. Перечислите технические средства дистанционного съёма информации и технические средства съёма информации с линий связи.

44. Что вам известно о технических средствах защиты речевой информации?

45. Приведите примеры типов технических средств защиты информации. Что вам известно о подавителях записывающих устройств и обнаружителях закамуфлированных камер?

46. Назовите устройства для активной защиты речевой информации от утечки по акустическому и вибрационному каналам.

47. Что такое звуковой сигнал? Приведите пример создания гармонического и полигармонического сигнала. Перечислите основные характеристики гармонического сигнала.

48. Дайте определения прямому и обратному преобразованиям Фурье. Как осуществляется процедура дискретного преобразования Фурье? В чем заключается основная идея быстрого алгоритма преобразования Фурье?

49. Что такое речевой сигнал, в чем заключается особенность энергетического спектра речевого сигнала? С какой основной целью необходимо построение спектров сигналов?

50. Дайте определение речевого сигнала. Какими основными признаками характеризуется речевой сигнал? Какие методы оценки основного тона вам известны? Особенности частоты основного тона для мужского и женского голосов?

51. Откуда берутся форманты? Дайте определение форманты. Укажите известные вам методы оценки формант?

52. Дайте понятие шума. Приведите основные характеристики шума. Расскажите о применении шумов для маскирования речевых сообщений. Какие основные характеристики можно оценить по гистограмме распределения плотности вероятности шума?

53. Дайте понятие синтеза смеси гармонического сигнала и гауссово шума с заданным отношением сигнал/шум.

54. Расскажите об особенностях методики и порядка проведения мероприятий по выявлению и исследованию КУИ. Каков порядок проведения аттестации объектов информатизации?

55. Расскажите об особенностях методики и порядка проведения мероприятий по выявлению и исследованию КУИ. Что включают в себя: специальные проверки, специальные обследования, специальные исследования?

56. Приведите пример методики оценки словесной разборчивости речи W.

57. С какой целью используют вейвлеты в задачах обработки и распознавания речи? Расскажите об основных возможностях вейвлет-анализа.

58. В чем заключаются особенности комплексного вейвлета Морле? Какие ещё вейвлет функции вам известны?

Раздел 5 Машиночитаемые технологии – мощная современная защита

59. Что вам известно о стеганографических системах защиты информации?

60. Дайте понятие о стеганографии. В чем заключаются её основные достоинства?

61. Дайте определение компьютерная и цифровая стеганография. Приведите примеры известных вам методов компьютерной стеганографии.

62. Расскажите почему стеганография есть эффективная защита печатной продукции?

63. Расскажите о машиночитаемых технологиях для традиционных способов печати.

64. Что вам известно о разработке новых машиночитаемых защитных признаков. Как осуществляется производственный контроль машиночитаемых защитных признаков?

65. Какие вам известны криптографические методы защиты информации?

66. Дайте основные понятия: криптология, криптография, криптоанализ.

67. Дайте понятия код, шифр и ключ: открытый и закрытый.

68. Приведите основную схему криптографии.

69. Приведите примеры возможных атак автоматизированной банковской системы. Возможные атаки на уровне сети.

70. Какие существуют меры защиты от атак на сетевом уровне.

71. Перечислите основные правила организации защиты АСБ.

72. Дайте понятие электронного документа и электронной цифровой подписи

73. Придание юридического статуса электронным документам. Юридическая сила оригинала и копии электронного документа.

74. Какие существуют угрозы цифровой подписи. RSA как фундамент электронной цифровой подписи.

75. Приведите примеры уникальной и точной идентификации продуктов и банковских счетов.

76. Особенности использования стандартизированных кодов банков, супермаркетов и других крупных подсистем экономики – кредитные карты. Алгоритм Луна. Понятие и разновидности шрихкодов.

Раздел 6 Защита интеллектуальной собственности

77. Приведите примеры объектов интеллектуальной собственности.

78. Что вам известно о Международной патентной классификации? Где размещаются источники патентной информации?

79. Что представляет собой патентный документ? Приведите примеры патентных документов.

80. Как осуществляется поиск патентной информации в Интернет?

81. Что представляет собой товарный знак? Дайте определение товарного знака.

82. Какие виды товарных знаков вам известны? Как оформить права на товарный знак? Последствия нарушения прав на товарные знаки.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Основы защиты информации» предполагает реализацию следующих видов самостоятельной работы студентов:

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

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

– решение индивидуальных задач при подготовке к практическим занятиям;

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

– подготовку к промежуточной и текущей диагностике компетенций;

– углублённое изучение отдельных тем учебной дисциплины для подготовки к контрольному тестированию;

– систематизация полученных знаний при подготовке к зачёту.

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

– наличием и использованием в учебном процессе открытых систем автоматизированного тестирования при использовании бесплатного сервиса для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google – Google Класс, которые доступны пользователям через Интернет в любое удобное для них время;

– использованием бизнес-мессенджера для групповой работы и общения Microsoft Teams;

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

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

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещённые на бесплатном сервисе для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google Класс Room университета: шифр курса **MESJ5ER**.

2. Материалы, размещённые в бизнес-мессенджере для групповой работы и общения Microsoft Teams: шифр курса **UUWNV6V**.

3. Методические указания к выполнению практических работ по дисциплине «Основы защиты информации» для студентов специальности 1-28 01 02 «Электронный маркетинг».

Содержание самостоятельной работы студентов (дневная форма получения высшего образования)

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
	Тема 2.4 Компьютерные вирусы и антивирусные программы Осн. литература: [4], [10], [13]. Доп. литература: [7].	2
	Тема 4.1 Классификация технических каналов утечки информации Осн. литература: [9], [24]. Доп. литература: [2], [15].	2

1	2	3
Углублённое изучение отдельных тем для подготовки к контрольному тестированию	*Тема 4.2 Обзор технических средств негласного съёма акустической информации* Осн. литература: [2], [3], [9]. Доп. литература: [2], [12], [21].	2
	Тема 4.3. Технические средства защиты речевой информации Осн. литература: [1], [2], [7], [9], [11]. Доп. литература: [18].	2
	Тема 4.4 Звуковые сигналы Осн. литература: [1]. Доп. литература: [13], [14].	2
	Тема 4.5 Применение шумов для маскирования речевых сигналов Осн. литература: [1], [2], [8]. Доп. литература: [18].	2
	Тема 5.2 Криптографические методы защиты информации Осн. литература: [6], [7], [12]. Доп. литература: [18].	2
	Тема 5.4 Электронный документ и электронная цифровая подпись Осн. литература: [6], [7], [12], [24] Доп. литература: [18].	2
	Тема 5.3 Основы защиты автоматизированных систем от несанкционированного доступа Осн. литература: [2], [6]. Доп. литература: [1], [5], [12].	2
	Тема 5.5 Уникальная и точная идентификация продуктов и банковских счётов Осн. литература: [7], [12]. Доп. литература: [18].	2
	Тема 6.3 Товарные знаки Осн. литература: [9], [25], [26]. Доп. литература: [18].	2
Подготовка к защите отчётов по практическим работам	**Практическая работа №1** Изучение Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (утверждён Постановлением Совета Министров Республики Беларусь 15.05.2013 № 375).	2
	Практическая работа №2 Правовое обеспечение информационной безопасности.	2
	Практическая работа №3 Выявление и фиксация следов противоправной деятельности на ПЭВМ.	2
	Практическая работа № 4. Оценка первичных признаков элементов речевого сигнала.	2
	Практическая работа №5 Создание маскирующего шума для имитации виброакустического зашумления.	2
	Практическая работа № 6. Мероприятия по выявлению каналов утечки информации (специальные проверки, специальные обследования, специальные исследования).	2
	Практическая работа №7 Изучение методов защиты информации с помощью различных видов шифров, используемых в криптографии.	2
	Практическая работа №8 Исследование разборчивости речи методом артикуляционных измерений при защите речевой информации различными видами маскирующих сигналов.	2
	Практическая работа №9 Поиск патентной информации в электронных базах: Патентного ведомства Республики Беларусь. Роспатента. Европейского патентного ведомства. Патентного ведомства США.	4
	ВСЕГО:	42

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Средствами диагностики результатов учебной деятельности являются мероприятия промежуточного контроля, которые проводятся в течение семестра и включают в себя следующие формы контроля:

– контрольное тестирование;

– защита отчётов по практическим работам;

– зачёт.

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.

Для оценивания самостоятельной и аудиторной работы студентов в рамках учебной дисциплины используется накопительная система оценивания знаний, которая предполагает суммирование отметок, выставляемых в электронный журнал за все виды работ в течение прохождения для определения среднеарифметических показателей успеваемости.

Практические занятия предполагают выполнение и защиту. Последнее практическое занятие в семестре предусматривает выполнение и защиту зачётной работы, а также контрольное тестирование. При выполнении практических работ выдаётся индивидуальное задание. Отчёт по практической 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.

Промежуточная (аттестационная) диагностика компетенции студентов осуществляется на основании индивидуального рейтинга студента на момент аттестации. Для положительной аттестации (промежуточного контроля успеваемости) необходимо согласно календарному плану выполнить все практические работы и индивидуальные задания, а также иметь положительную отметку по промежуточному контролю освоения теоретической части.

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:

$$П = \frac{(КТ_1 + ... + КТ_6) + (ПР_1 + ... + ПР_9)}{15}$$

где $КТ_1 + ... + КТ_6$ – отметки, выставленные по результатам контрольного тестирования;
$ПР_1 + ... + ПР_9$ – отметки, выставленные по результатам защиты практических работ.

Результат промежуточного контроля рассчитывается как округлённое среднее значение.

Текущая аттестация проводится в форме зачёта.

Зачёт проводится согласно Положению.

Заключение о выставлении отметки «зачтено» 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 учебной программе вопросам.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Основы 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 «Основы защиты информации» возможно использование элементов проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Изучение учебной дисциплины осуществляется на лекционных и практических занятиях. На лекционных занятиях студенты овладевают системой теоретических знаний в области защиты информации. В ходе лекционного изложения теоретических сведений используются традиционные словесные приёмы и методы, которые активизируются постановкой проблемных вопросов и заданий, организацией учебных дискуссий в опоре на имеющуюся начальную подготовку студентов и их политехнический кругозор, использованием интерактивных методов обучения.

На практических занятиях развиваются и формируются необходимые практические умения и навыки по оценке защищённости компьютерных систем и технических каналов утечки. Во время проведения практических работ особое внимание уделяется формированию у студентов умения планировать работу, определять эффективную последовательность её выполнения.