Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Проректор по учебной работе
учреждения образования
«Полоцкий государственный университет
имени Евфросинии Полоцкой»
_____ Е.И. Галешова
«18» 12 2023 г.
Регистрационный №УД-473/23/уч

МОДУЛЬ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

ЛАБОРАТОРНЫЙ СПЕЦПРАКТИКУМ «ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ»

учебная программа учреждения образования
по учебным дисциплинам для специальности
1-31 04 08 «Компьютерная физика»

2023 г.

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 1-31 04 08-2018 и учебного плана специальности 1-31 04 08 «Компьютерная физика». Регистрационный №06-20/уч. ФКНиЭ от 28.12.2020 г. для дневной формы получения высшего образования.

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

Кухта Сергей Васильевич, старший преподаватель кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 11 от «16» 11 2023 г.).

Методической комиссией факультета компьютерных наук и электроники учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 4 от «14» 12 2023 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Интенсивное внедрение информационных технологий во все области деятельности человека позволяет обеспечить оперативный обмен сведениями между службами, отделами предприятия и организациями в целом за счет оптимизации информационных потоков, что позволяет ускорить и сделать более качественным процесс их взаимодействия. Сведения, которыми обмениваются такие партнеры, как правило, носят конфиденциальный характер и относятся к категориям служебной или государственной тайны, что требует подготовки современных специалистов, обладающих не только специальными знаниями по их профилю обучения, но и владением основами защиты информации.

Учебный модуль «Компьютерная безопасность» включает в себя дисциплину «Основы защиты информации» и Лабораторный спецпрактикум «Основы защиты информации», которые относятся к дисциплинам специализации 1-31 04 08 03 «Компьютерное моделирование физических процессов» специальности 1-31 04 08 «Компьютерная физика» и ориентированы на обучение студентов по указанной специальности базовым знаниям, умениям и навыкам в области защиты информации. Изучаемые темы по модулю представляются на основе современной нормативной регулятивной базы и национального законодательства.

Цель изучения учебного модуля.

Целью изучения дисциплин «Основы защиты информации» и «Лабораторный спецпрактикум «Основы защиты информации» является формирование у студентов базовых знаний в области информационной безопасности и вопросов обеспечения защиты информации в условиях различных по виду, происхождению и характеру возникновения угроз. Изучение дисциплин «Основы защиты информации» и «Лабораторный спецпрактикум «Основы защиты информации» является необходимым этапом в профессиональном развитии «Физика. Программиста».

Задачи изучения учебного модуля.

При изучении дисциплин «Основы защиты информации» и «Лабораторный спецпрактикум «Основы защиты информации» требуется разрешить основные задачи:

– сформировать у студентов понимание базовых понятий, связанных с процессом обеспечения информационной безопасности;

– показать основные угрозы информационной безопасности;

– сформировать системное понимание проблем безопасности и путей их решения;

– изучить методы и средства защиты информации;

– получить знания о принципах организации и построения комплексных систем защиты информации.

В результате изучения дисциплин «Основы защиты информации» и «Лабораторный спецпрактикум «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;

– основные 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 приемами анализа вероятных угроз информационной безопасности для заданных объектов;

– методами построения надежных криптосистем и функций хеширования;

– методами построения криптосистем с открытым ключом и систем электронной цифровой подписи;

– способами введения объектов интеллектуальной собственности в гражданский оборот;

– способами передачи прав на использование объектов интеллектуальной собственности.

Требования к уровню освоения содержания учебного модуля.

При изучении дисциплин «Основы защиты информации» и «Лабораторный спецпрактикум «Основы защиты информации» у студентов специальности 1-31 04 08 «Компьютерная физика» должен сформироваться набор ***специализированных компетенций***, соответствующих присваиваемой по завершению высшего образования квалификации «Физик. Программист» обеспечивающих выпускникам по указанной специальности успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности.

СК-9. Быть способным разрабатывать физико-математическую модель явлений, процессов или систем при организации защиты информации; выполнять оценку эффективности методов защиты информации.

Сформированная компетенция является основополагающей при изучении всех последующих дисциплин, связанных с обработкой и защитой информации, а также фундаментальной основой для дальнейшей профессиональной деятельности физика-программиста.

Перечень дисциплин, в продолжение и на базе которых изучается учебный модуль.

Основой для изучения учебных дисциплин «Основы защиты информации» и «Лабораторный спецпрактикум «Основы защиты информации» по специальности 1-31 04 08 «Компьютерная физика» является предмет «Информатика», изучаемый при получении общего базового и общего среднего образования, а также необходимы знания, полученные при изучении дисциплин «Программирование», «Программно-аппаратные интерфейсы информационных систем», «Объектно-ориентированное программирование».

Перечень дисциплин, которые изучаются на базе учебного модуля.

Знания, полученные при изучении дисциплин «Основы защиты информации» и «Лабораторный спецпрактикум «Основы защиты информации» непосредственно связаны с учебными дисциплинами «Системы управления базами данных», «Компьютерные методы статистического анализа данных», «Программирование на суперкомпьютерах», «Программные методы автоматизации эксперимента», «Лабораторный спецпрактикум «Современные технологии программирования», а также другими дисциплинами, предусмотренными учебным планом по специальности.

Изучение учебного модуля «Компьютерная безопасность» позволяет дать студентам базу, необходимую для успешного усвоения материала перечисленных выше учебных дисциплин, а также получить знания, необходимые в дальнейшем для успешной работы.

В соответствии с учебным планом по специальности 1-31 04 08 «Компьютерная физика» на изучение учебной дисциплины отводится:

Форма получения высшего образования	дневная
Курс (курсы)	3
Семестр	6
Всего часов по модулю, часов	216
Всего аудиторных часов по модулю, часов	120
Трудоёмкость модуля «Компьютерная безопасность», з.е.	6
В том числе:	
Дисциплина «Основы защиты информации»	
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	60
Лекции, часов	32
Практические занятия, часов	28
Самостоятельная работа по дисциплине, часов	48
Форма промежуточной аттестации по дисциплине	диф. зачет
Трудоёмкость дисциплины, з.е.	3
Лабораторный спецпрактикум «Основы защиты информации»	
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	60
Лабораторные занятия, часов	60
Самостоятельная работа по дисциплине, часов	48
Форма промежуточной аттестации по дисциплине	зачет
Трудоёмкость дисциплины, з.е.	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Учебная дисциплина «Основы защиты информации»

ВВЕДЕНИЕ

Цели и задачи изучения модуля. 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. Виды компьютерных преступлений. Примеры известных компьютерных преступлений. Использование специальных программных средств мошенниками. Полезные советы по компьютерной безопасности.

Тема 2.3 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 (КУИ). 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 Программно-аппаратные системы защиты информации

Системы охранно-пожарной сигнализации. Системы видеонаблюдения. Системы контроля и управления доступом.

Тема 4.7 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.

РАЗДЕЛ 5 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

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.

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 (АСБ) 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. Промышленная собственность. Коммерческое использование объектов интеллектуальной собственности. Государственное управление интеллектуальной собственностью. Защита прав авторов и правообладателей.

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.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Учебная дисциплина «Лабораторный спецпрактикум «Основы защиты информации»»

РАЗДЕЛ 1 ОСНОВЫ ТЕОРИИ ЧИСЕЛ

Тема 1.1 Использование алгоритмов теории чисел в криптографии.

РАЗДЕЛ 2 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Тема 2.1 Шифрование данных криптоалгоритмом перестановки.
Тема 2.2 Шифрование данных криптоалгоритмом простой замены.
Тема 2.3 Шифрование данных криптоалгоритмом многоалфавитной замены.
Тема 2.4 Программная реализация сети Фейстеля.
Тема 2.5 Исследование криптосистемы DES.
Тема 2.6 Исследование криптосистемы ГОСТ 28147.
Тема 2.7 Анализ генераторов псевдослучайной последовательности.
Тема 2.8 Исследование шифра гаммирования.
Тема 2.9 Реализация арифметики больших чисел.
Тема 2.10 Программная реализация генератора простых чисел.
Тема 2.11 Реализация алгоритмов модульной арифметики.
Тема 2.12 Реализация алгоритма Евклида, расширенного алгоритма Евклида.
Тема 2.13 Анализ односторонних функций.
Тема 2.14 Реализация программы шифрования асимметричной криптосистемы.
Тема 2.15 Реализация программы дешифрования асимметричной криптосистемы.

РАЗДЕЛ 3 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА С ПОМОЩЬЮ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ

Тема 3.1 Исследование криптографических хеш-функций.
Тема 3.2 Генерация электронной цифровой подписи в документе.
Тема 3.3 Верификации электронной цифровой подписи документа.
Тема 3.4 Исследование показателей эффективности парольных средств аутентификации.
Тема 3.5 Исследование показателей эффективности биометрических средств аутентификации.
Тема 3.6 Исследование методов компьютерной стеганографии.
Тема 3.7 Программная реализация протокола простой аутентификации.
Тема 3.8 Программная реализация протокола многофакторной аутентификации.

РАЗДЕЛ 4 МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 4.1 Использование программной систем PGP и TrueCrypt для обеспечения конфиденциальности и целостности информационных ресурсов
Тема 4.2 Получение практических навыков программного восстановления данных при помощи программы TestDisk
Тема 4.3 Реализация политики безопасности в защищенных версиях операционной системы Windows. Создание и удаление учетной записи пользователя, групп пользователей
Тема 4.4 Разграничение прав пользователей в защищенных версиях операционной системы Windows. Тема 4.5 Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows
Тема 4.6 Аудит информационных процессов в операционной системе Windows. Аудит реестра в операционной системе Windows

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	**2**	**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.: [1], [2], [7]. Доп. лит.: [11]. Норм. докум.: [1], [2], [3] [12], [17]. Эл. рес.: [1], [5], [6], [7], [10].	
2	**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			Методические указания	Защита отчёта по практической работе № 1

1	2	3	4	5	6	7	8
	Раздел 1 Системная методология информационной безопасности	**2**	**2**				
3	**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				Осн. лит.: [2], [4], [5]. Доп. лит.: [2], [10]. Норм. докум.: [8], [17], [18]. Эл. рес.: [2], [6], [11].	*Контрольное тестирование №1
4	**Практическая работа №2** Изучение Закона Республики Беларусь 19 июля 2010 г. №170-З «О Государственных Секретах». Государственное регулирование и управление в области информации, информатизации и защиты информации. Изучение Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».		2			Методические указания	Защита отчета по практической работе № 2
	Раздел 2 Правовое обеспечение и методы защиты информации	**4**	**4**				
5	**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». *Тема 2.2 Правовые методы защиты информации* Правовая защита от компьютерных преступлений. Виды компьютерных преступлений. Примеры известных компьютерных преступлений. Использование специальных программных средств мошенниками. Полезные советы по компьютерной безопасности.	2				Осн. лит.: [4], [6], [7]. Норм. докум.: [1], [12], [13], [14], [15] [17], [18]. Эл. рес.: [3]. Осн. лит.: [7]. Доп. лит.: [11]. Норм. докум.: [15].	

1	2	3		5	6	7	8
6	**Практическая работа №3** Изучение концепции национальной безопасности Республики Беларусь. Указ Президента Республики Беларусь №440 от 9 декабря 2019 г. Указ Президента №40 от 14 февраля 2023 г.		2			Методические указания	Защита отчета по практической работе № 3
7	**Лекция № 4** *Тема 2.3 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				Осн. лит.: [2], [3]. Доп. лит.: [6], [10]. Норм. докум.: [9].	*Контрольное тестирование №2
8	**Практическая работа №4** Правовое обеспечение информационной безопасности. Выявление и фиксация следов противоправной деятельности на ПЭВМ.		2			Методические указания	Защита отчета по практической работе № 4
	Раздел 3 Организационные методы защиты информации	**4**	**4**				
9	**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				Осн. лит.: [4], [6], [7]. Доп. лит.: [2], [10], [11]. Норм. докум.: [13], [14], [16].	
10	**Практическая работа №5** Администрирование Windows 10. Управление системными службами и процессами Windows.		2			Методические указания	Защита отчета по практической работе № 5
11	**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-административные и организационно-технические методы защиты информации. Страхование как метод защиты информации.	2				Осн. лит.: [7]. Доп. лит.: [12], [8].	

1	2	3		5	6	7	8
12	**Практическая работа №6** Организация защиты в Microsoft EXCEL.		2			Методические указания	Защита отчета по практической работе № 6
	Раздел 4 Инженерно-техническая защита объектов от несанкционированного доступа	**8**	**8**				
13	**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				Осн. лит.: [1], [2]. Доп. лит.: [3], [4], [5], [7].	*Контрольное тестирование №3
14	**Практическая работа №7** Оценка первичных признаков элементов речевого сигнала.		2			Методические указания	Защита отчета по практической работе № 7
15	**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				Осн. лит.: [1], [2]. Доп. лит.: [3], [4], [5], [7].	
16	**Практическая работа №8** Создание маскирующего шума для имитации виброакустического зашумления.		2			Методические указания	Защита отчета по практической работе № 8

1	2	3	4	5	6	7	8
17	**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				Осн. лит.: [1], [2]. Доп. лит.: [5].	
18	**Практическая работа №9** Применение маскирующего шума для имитации виброакустического зашумления.		2			Методические указания	Защита отчета по практической работе № 9
19	**Лекция № 10** *Тема 4.6 Программно-аппаратные системы защиты информации* Системы охранно-пожарной сигнализации. Системы видеонаблюдения. Системы контроля и управления доступом. *Тема 4.7 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.	2				Осн. лит.: [1], [2]. Доп. лит.: [4], [7].	*Контрольное тестирование №4
20	**Практическая работа №10** Мероприятия по выявлению каналов утечки информации (специальные проверки, специальные обследования, специальные исследования).		2			Методические указания	Защита отчета по практической работе № 10
	Раздел 5 Защита информации в информационных системах	**8**	**6**				
21	**Лекция № 11** *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.	2				Осн. лит.: [1], [2]. Доп. лит.: [2], [12].	
22	**Практическая работа №11** Изучение методов защиты информации с помощью различных видов шифров, используемых в криптографии.		2			Методические указания	Защита отчета по практической работе № 11

1	2	3	4	5	6	7	8
23	**Лекция № 12** *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.	2				Осн. лит.: [5], [8], [9-10]. Доп. лит.: [1], [4], [7], [8]. Доп. лит.: [1], [12]. Норм. докум.: [5], [6].	*Контрольное тестирование №5
24	**Практическая работа №12** Организация защиты баз данных в СУБД Microsoft ACCESS.		2			Методические указания	Защита отчета по практической работе № 12
25	**Лекция № 13** *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				Осн. лит.: [5], [8], [9-10]. Доп. лит.: [4], [8].	
26	**Лекция № 14** *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				Доп. лит.: [12].	
27	**Практическая работа №13** Штриховое кодирование информации. Анализ реальных штрих-кодов.		2			Методические указания	Защита отчета по практической работе № 13

1	2	3	4	5	6	7	8
	Раздел 6 Защита интеллектуальной собственности	**4**	**2**				
28	**Лекция № 15** *Тема 6.1 Объекты интеллектуальной собственности* Мир вещей и результаты интеллектуальной деятельности. Объекты интеллектуальной собственности. Базы данных. Промышленная собственность. Авторское право и смежные права. Промышленная собственность. Коммерческое использование объектов интеллектуальной собственности. Государственное управление интеллектуальной собственностью. Защита прав авторов и правообладателей.	2				Осн. лит.: [3], [7].	*Контрольное тестирование №6
29	**Лекция № 16** *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.	2				Осн. лит.: [3], [7], [9]. Доп. лит.: [12].	*Реферативное выступление с докладом
30	**Практическая работа №14** Поиск патентной информации в электронных базах: Патентного ведомства Республики Беларусь. Роспатента. Европейского патентного ведомства. Патентного ведомства США.		2				Защита отчета по практической работе № 14
	Всего	**32**	**28**				

*** МЕРОПРИЯТИЯ ТЕКУЩЕГО КОНТРОЛЯ**

Учебно-методическая карта учебной дисциплины «Лабораторный спецпрактикум «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
	Раздел 1 Основы теории чисел			**2**			
1	**Лабораторная работа №1** Использование алгоритмов теории чисел в криптографии			2		Осн. лит.: [5], [9]. Методические указания	Защита отчёта по лабораторной работе № 1
	Раздел 2 Криптографическая защита информации			**30**			
2	**Лабораторная работа №2** Шифрование данных криптоалгоритмом перестановки			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчёта по лабораторной работе № 2
3	**Лабораторная работа №3** Шифрование данных криптоалгоритмом простой замены			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 3
4	**Лабораторная работа №4** Шифрование данных криптоалгоритмом многоалфавитной замены			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 4

1	2	3	4	5	6	7	8
5	**Лабораторная работа №5** Программная реализация сети Фейстеля			**2**		Осн. лит.: [5], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 5
6	**Лабораторная работа №6** Исследование криптосистемы DES			2		Осн. лит.: [5], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 6
7	**Лабораторная работа №7** Исследование криптосистемы ГОСТ 28147			2		Осн. лит.: [5], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 7
8	**Лабораторная работа №8** Анализ генераторов псевдослучайной последовательности			2		Осн. лит.: [3], [9]. Методические указания	Защита отчета по лабораторной работе № 8
9	**Лабораторная работа №9** Исследование шифра гаммирования			2		Осн. лит.: [3], [9]. Методические указания	Защита отчета по лабораторной работе № 9
10	**Лабораторная работа №10** Реализация арифметики больших чисел			2		Осн. лит.: [5], [9], [10]. Методические указания	Защита отчета по лабораторной работе № 10
11	**Лабораторная работа №11** Программная реализация генератора простых чисел			2		Осн. лит.: [5], [9], [10]. Методические указания	Защита отчета по лабораторной работе № 11
12	**Лабораторная работа №12** Реализация алгоритмов модульной арифметики			2		Осн. лит.: [3], [9], [10]. Методические указания	Защита отчета по лабораторной работе № 12
13	**Лабораторная работа №13** Реализация алгоритма Евклида, расширенного алгоритма Евклида			2		Осн. лит.: [3], [9], [10]. Методические указания	Защита отчета по лабораторной работе № 13

1	2	3	4	5	6	7	8
14	**Лабораторная работа №14** Анализ односторонних функций			2		Осн. лит.: [5], [9], [10]. Методические указания	Защита отчета по лабораторной работе № 14
15	**Лабораторная работа №15** Реализация программы шифрования асимметричной криптосистемы			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 15
16	**Лабораторная работа №16** Реализация программы дешифрования асимметричной криптосистемы			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 16
	Раздел 3 Обеспечение безопасности информационного обмена с помощью криптографических протоколов			**16**			
17	**Лабораторная работа №17** Исследование криптографических хеш-функций			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 17
18	**Лабораторная работа №18** Генерация электронной цифровой подписи в документе			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 18
19	**Лабораторная работа №19** Верификации электронной цифровой подписи документа			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 19
20	**Лабораторная работа №20** Исследование показателей эффективности парольных средств аутентификации			2		Осн. лит.: [8], [10]. Методические указания	Защита отчета по лабораторной работе № 20
21	**Лабораторная работа №21** Исследование показателей эффективности биометрических средств аутентификации			2		Осн. лит.: [8], [10]. Методические указания	Защита отчета по лабораторной работе № 21
22	**Лабораторная работа №22** Исследование методов компьютерной стеганографии			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 22

1	2	3	4	5	6	7	8
23	**Лабораторная работа №23** Программная реализация протокола простой аутентификации			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 23
24	**Лабораторная работа №24** Программная реализация протокола многофакторной аутентификации			2		Осн. лит.: [3], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 24
	Раздел 4 Механизмы обеспечения информационной безопасности			**12**			
25	**Лабораторная работа №25** Использование программной систем PGP и TrueCrypt для обеспечения конфиденциальности и целостности информационных ресурсов			2		Осн. лит.: [10]. Методические указания	Защита отчета по лабораторной работе № 25
26	**Лабораторная работа №26** Получение практических навыков программного восстановления данных при помощи программы TestDisk			2		Осн. лит.: [10]. Методические указания	Защита отчета по лабораторной работе № 26
27	**Лабораторная работа №27** Реализация политики безопасности в защищенных версиях операционной системы Windows. Создание и удаление учетной записи пользователя, групп пользователей			2		Осн. лит.: [5], [10]. Методические указания	Защита отчета по лабораторной работе № 27
28	**Лабораторная работа №28** Разграничение прав пользователей в защищенных версиях операционной системы Windows. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows			2		Осн. лит.: [5], [10]. Методические указания	Защита отчета по лабораторной работе № 28
29	**Лабораторная работа №29** Аудит информационных процессов в операционной системе Windows. Аудит реестра в операционной системе Windows			2		Осн. лит.: [5], [10]. Методические указания	Защита отчета по лабораторной работе № 29
30	**Лабораторная работа №30** Выполнение зачётной итоговой работы			2		Осн. лит.: [3], [5], [8], [10]. Методические указания	Защита отчета по лабораторной работе № 30
	Всего			**60**			

Примечание: в соответствии с рейтинговой системой для определения результата текущего контроля за семестр в виде отметки в баллах по десятибалльной шкале используются отметки, полученные за мероприятия текущего контроля в течение семестра, обозначенные в графе «Форма контроля знаний»

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Белоус, А. И. Программные и аппаратные трояны – способы внедрения и методы противодействия : первая техническая энциклопедия : в 2 книгах / А. И. Белоус, В. А. Солодуха, С. В. Шведов. – Москва : Техносфера, 2019. – Книга 1. – 1318 с. : ил., схем., табл. – (Мир электроники). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=597000 (дата обращения: 11.10.2023). – ISBN 978-5-94836-524-4. – Текст : электронный.

2. Белоус, А.И. Кибероружие и кибербезопасность: о сложных вещах простыми словами: монография / А. И. Белоус, В. А. Солодуха. – Москва; Вологда: Инфра-Инженерия, 2020. – 690 с.

3. Васильева, И.Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. – Москва: Юрайт, 2023. – 349 с. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника и практикума для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.

4. Государственная политика информационной безопасности и информационное противоборство: учебное пособие / В. Ю. Арчаков [и др.]; Академия управления при Президенте Республики Беларусь ; [авторы: В.Ю. Арчаков, А.Л. Баньковский, А.В. Ивановский, О.С. Макаров]. – 2-е издание, стереотипное. – Минск : Академия управления при Президенте Республики Беларусь, 2020 ; 2021. – 227 с. – Допущено Министерством образования Республики Беларусь в качестве учебного пособия для слушателей системы дополнительного образования взрослых по специальностям переподготовки «Информационно-аналитическая работа в системе органов государственного управления».

5. Деза, Е.И. Введение в криптографию. Теоретико-числовые основы защиты информации: учебное пособие / Е. И. Деза, Л. В. Котова. - издание стереотипное. – Москва : ЛЕНАНД, 2022. – 368 с. – (Основы защиты информации. № 14).

6. Петренко, В. И. Защита персональных данных в информационных системах. Практикум [Электронный ресурс]: учебное пособие для вузов / В. И. Петренко, И. В. Мандрица ; Петренко В. И., Мандрица И. В. – 2-е изд., стер. – Санкт-Петербург: Лань, 2020. – 108 с. // ЭБС «Лань». – Режим доступа: по подписке: URL: https://e.lanbook.com/book/149364.

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

8. Романьков, В.А. Введение в криптографию: курс лекций / В. А. Романьков. – 2 издание, исправленное и дополненное. – Москва: ИНФРА-М, 2023. – 234 с. – Рекомендовано в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям подготовки 01.03.01 «Математика», 02.03.01 «Математика и компьютерные технологии», 01.03.02 «Прикладная математика и информатика» (квалификация (степень) «бакалавр»).

9. Фомичев, В.М. Криптографические методы защиты информации: учебник для вузов: в 2 частях / В. М. Фомичев, Д. А. Мельников; под редакцией В.М. Фомичева. – Москва: Юрайт, 2023. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям. Часть 1 : Математические аспекты. – 2023. – 209 с.

10. Фомичев, В.М. Криптографические методы защиты информации: учебник для вузов: в 2 частях / В. М. Фомичев, Д. А. Мельников; под редакцией В.М. Фомичева. – Москва: Юрайт, 2023. – (Высшее образование). – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям. Часть 2: Системные и прикладные аспекты. – 2023. – 245 с. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.

Гурнова Е.В.

Дополнительная:

1. Внуков, А.А. Защита информации в банковских системах: учебное пособие для вузов / А. А. Внуков. – 2-е издание, исправленное и дополненное. – Москва: Юрайт, 2021. – 245 с. – Рекомендовано Учебно-методическим отделом высшего образования в качестве учебного пособия для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям.

2. Гультяева, Т. А. Основы защиты информации : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730 (дата обращения: 29.09.2023). – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст : электронный.

3. 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: 29.01.2024). – Библиогр. в кн. – ISBN 978-5-8149-2839-9 (Ч. 1). – ISBN 978-5-8149-2838-2. – Текст : электронный.

4. Долозов, Н. Л. Программные средства защиты информации : конспект лекций : [16+] / Н. Л. Долозов, Т. А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2015. – 63 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438307 (дата обращения: 29.09.2023). – Библиогр. в кн. – ISBN 978-5-7782-2753-8. – Текст : электронный.

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

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

7. Каторин, Ю.Ф. Защита информации техническими средствами: учебное пособие. / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. – СПб.: НИУ ИТМО, 2012. – 416с.

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

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

10. Новиков, В.К. Средства, технологии, системы и технические каналы утечки информации для осуществления киберслежки за человеком и его деятельностью: монография / В.К. Новиков, М.Г. Краснов, И.С. Рекунков. – Москва: Горячая линия-Телеком, 2021. – 160 с.

11. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. – 2-е изд., испр. – Санкт-Петербург : Лань, 2020. – 124 с. – ISBN 978-5-8114-4404-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/133924 (дата обращения: 19.08.2022). – Режим доступа: для авториз. пользователей.

12. Системы защиты информации в ведущих зарубежных странах : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, Г. В. 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. – URL: https://biblioclub.ru/index.php?page=book&id=93351 (дата обращения: 29.09.2023). – Библиогр.: с. 192-193. – ISBN 978-5-9765-1274-0. – Текст : электронный.

13. Гультяева, Т. А. Основы защиты информации : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730 (дата обращения: 29.09.2023). – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст : электронный.

14. Долозов, Н. Л. Программные средства защиты информации : конспект лекций : [16+] / Н. Л. Долозов, Т. А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2015. – 63 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=438307 (дата обращения: 29.09.2023). – Библиогр. в кн. – ISBN 978-5-7782-2753-8. – Текст : электронный.

15. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. – 2-е изд., испр. – Санкт-Петербург : Лань, 2020. – 124 с. – ISBN 978-5-8114-4404-5. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/133924 (дата обращения: 19.08.2022). – Режим доступа: для авториз. пользователей.

Нормативные документы:

1. Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY): постановление Совета Министров Республики Беларусь от № 375 от 15.05.2013 г.: в ред. постановления Совета Министров Республики Беларусь № 145 от 12.03.2020 г.

2. Концепция информационной безопасности: утв. постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь».

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

4. СТБ 34.101.8-2006 Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования: введен 01.07.2006.

5. СТБ 34.101.9-2004 Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы: введен 01.09.2004.

6. СТБ 34.101.10-2004 Информационные технологии. Средства защиты информации от несанкционированного доступа в автоматизированных системах. Общие требования: введен 01.09.2004.

7. СТБ 34.101.11-2009 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в доверенной зоне корпоративной сети: введен 01.09.2009.

8. СТБ 34.101.12-2007 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества: введен 01.10.2007.

9. СТБ 34.101.15-2007 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Типовая программа и методика испытаний: введен 01.11.2007.

10. СТБ 34.101.31-2011 Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности: введен 01.07.2011.

11. Закон Республики Беларусь «О Государственных Секретах» №170-З от 19.07.2010 г.: в ред. Закона Республики Беларусь № 124-З от 17.07.2018.

12. Закон Республики Беларусь «Об информации, информатизации и защите информации» № 455-З от 10.11.2008 г.: в ред. Закона Республики Беларусь № 362-З от 11.05.2016 г.

13. Закон Республики Беларусь «О коммерческой тайне» № 16-З от 05.01.2013: в ред. Закона Республики Беларусь № 132-З от 17.07.2018 г.

14. Закон Республики Беларусь «О защите персональных данных» №99-З от 07.05.2023.

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

16. Указ Президента Республики Беларусь «О кибербезопасности». № 40 от 14.02.2023 г.

17. Указ Президента Республики Беларусь «О некоторых мерах по совершенствованию защиты информации» № 196 от 16.04.2013 г.: в ред. Указа Президента Республики Беларусь № 449 от 9.12.2019 г.

18. Указ Президента Республики Беларусь «О совершенствовании государственного регулирования в области защиты информации» № 449 от 9.12.2019 г.

Электронные ресурсы:

1. Научно-исследовательский институт технической защиты информации. [Электрон, ресурс]. – Режим доступа: http://www.niitzi.by. – Дата доступа: 19.03.2023.

2. Национальный открытый университет. [Электрон, ресурс]. – Режим доступа: http://www.intuit.ru. – Дата доступа: 19.03.2023.

3. Национальный правовой портал Республики Беларусь. [Электрон, ресурс]. – http://www.pravo.by. – Дата доступа: 19.03.2023.

4. Национальный центр интеллектуальной собственности. [Электрон, ресурс]. – Режим доступа: http://www.belgospatent.org.by. – Дата доступа: 19.03.2023.

5. Оперативно-аналитический центр при Президенте Республики Беларусь [Электрон, ресурс]. – Режим доступа: http://oac.gov.by. – Дата доступа: 19.03.2023.

6. Министерство связи и информатизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: http://www.mpt.gov.by. – Дата доступа: 19.03.2023.

7. International Organization for Standardization (Международная Организация Стандартизации). [Электрон, ресурс]. – Режим доступа: http://www.iso.org (http://www.iso.ch). – Дата доступа: 19.03.2023.

8. Your Private Network (Лаборатория Сетевой Безопасности). [Электрон, ресурс]. – Режим доступа: http://ypn.ru/177/international-standards-of-information-technologies-security. – Дата доступа: 19.03.20239.

9. Государственный комитет по стандартизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: http://www.tnpa.by. – Дата доступа: 19.03.2019.

10. Государственный комитет по стандартизации. [Электрон, ресурс]. – Режим доступа: http://www.gosstandart.goy.by. – Дата доступа: 19.03.2023.

11. Отчет о деятельности Национального центра защиты персональных данных за 2022 год – Национальный центр защиты персональных данных Республики Беларусь (cpd.by) – Режим доступа: https://cpd.by/otchet-o-dejatelnosti-nacionalnogo-centra-zashhity-personalnyh-dannyh-za-2022-god/ – Дата доступа: 19.03.2023.

Перечень компьютерных программ:

Используются пакеты: Microsoft Office Access; Matlab; Mathcad; NI LabView и программные среды для разработки программного обеспечения и др.

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

По учебной дисциплине «Основы защиты информации»

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
Изучение Закона Республики Беларусь 19 июля 2010 г. №170-З «О Государственных Секретах». Государственное регулирование и управление в области информации, информатизации и защиты информации. Изучение Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

Практическая работа №3
Изучение концепции национальной безопасности Республики Беларусь. Указ Президента Республики Беларусь №440 от 9 декабря 2019 г. Указ Президента №40 от 14 февраля 2023 г.

Практическая работа №4
Правовое обеспечение информационной безопасности. Выявление и фиксация следов противоправной деятельности на ПЭВМ.

Практическая работа №5
Администрирование Windows 10. Управление системными службами и процессами Windows.

Практическая работа №6
Организация защиты в Microsoft EXCEL.

Практическая работа №7
Оценка первичных признаков элементов речевого сигнала.

Практическая работа №8
Создание маскирующего шума для имитации виброакустического зашумления.

Практическая работа №9
Применение маскирующего шума для имитации виброакустического зашумления.

Практическая работа №10
Мероприятия по выявлению каналов утечки информации (специальные проверки, специальные обследования, специальные исследования).

Практическая работа №11
Изучение методов защиты информации с помощью различных видов шифров, используемых в криптографии.

Практическая работа №12
Организация защиты баз данных в СУБД Microsoft ACCESS.

Практическая работа №13
Штриховое кодирование информации. Анализ реальных штрих-кодов.

Практическая работа №14
Поиск патентной информации в электронных базах: Патентного ведомства Республики Беларусь. Роспатента. Европейского патентного ведомства. Патентного ведомства США.

ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

по учебной дисциплине «Лабораторный спецпрактикум «Основы защиты информации»»

Лабораторная работа №1
Использование алгоритмов теории чисел в криптографии

Лабораторная работа №2
Шифрование данных криптоалгоритмом перестановки

Лабораторная работа №3
Шифрование данных криптоалгоритмом простой замены

Лабораторная работа №4
Шифрование данных криптоалгоритмом многоалфавитной замены

Лабораторная работа №5
Программная реализация сети Фейстеля

Лабораторная работа №6
Исследование криптосистемы DES

Лабораторная работа №7
Исследование криптосистемы ГОСТ 28147

Лабораторная работа №8
Анализ генераторов псевдослучайной последовательности

Лабораторная работа №9
Исследование шифра гаммирования

Лабораторная работа №10
Реализация арифметики больших чисел

Лабораторная работа №11
Программная реализация генератора простых чисел

Лабораторная работа №12
Реализация алгоритмов модульной арифметики

Лабораторная работа №13
Реализация алгоритма Евклида, расширенного алгоритма Евклида

Лабораторная работа №14
Анализ односторонних функций

Лабораторная работа №15
Реализация программы шифрования асимметричной криптосистемы

Лабораторная работа №16
Реализация программы дешифрования асимметричной криптосистемы

Лабораторная работа №17
Исследование криптографических хеш-функций

Лабораторная работа №18
Генерация электронной цифровой подписи в документе

Лабораторная работа №19
Верификации электронной цифровой подписи документа

Лабораторная работа №20
Исследование показателей эффективности парольных средств аутентификации

Лабораторная работа №21
Исследование показателей эффективности биометрических средств аутентификации

Лабораторная работа №22
Исследование методов компьютерной стеганографии

Лабораторная работа №23
Программная реализация протокола простой аутентификации

Лабораторная работа №24
Программная реализация протокола многофакторной аутентификации

Лабораторная работа №25
Использование программной систем PGP и TrueCrypt для обеспечения конфиденциальности и целостности информационных ресурсов

Лабораторная работа №26
Получение практических навыков программного восстановления данных при помощи программы TestDisk

Лабораторная работа №27
Реализация политики безопасности в защищенных версиях операционной системы Windows. Создание и удаление учетной записи пользователя, групп пользователей

Лабораторная работа №28
Разграничение прав пользователей в защищенных версиях операционной системы Windows. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

Лабораторная работа №29
Аудит информационных процессов в операционной системе Windows. Аудит реестра в операционной системе Windows

Лабораторная работа №30
Выполнение зачётной итоговой работы

ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

По учебной дисциплине «Основы защиты информации»

1. Виртуальные частные сети.
2. Деструктивные возможности современных вредоносных программ.
3. Защита от атак на сетевом уровне. Межсетевые экраны.
4. Защита персональных данных.
5. Инструменты проверки целостности содержимого дисков.
6. Исторические события факты в области информационной безопасности.
7. Компьютерная стеганография в нашей жизни.
8. Понятие SQL-инъекции и меры борьбы.
9. Порядок действий в случае несанкционированного взлома вашего аккаунта.
10. Приемы безопасного использования личной и корпоративной электронной почты.
11. Приемы навыки безопасного использования мобильных устройств.
12. Примеры использования электронной цифровой подписи в Республике Беларусь.
13. Примеры стандартизированных кодов банков, супермаркетов и других крупных подсистем экономики.
14. Системы обнаружения уязвимостей сетей и анализаторы сетевых атак.
15. Современные криптосистемы.
16. Средства антивирусной защиты.
17. Средства идентификации и аутентификации пользователей (комплекс ЗА).
18. Средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям.
19. Существующие в мире механические системы защиты.
20. Цифровая грамотность.
21. Разновидности систем охранно-пожарной сигнализации.
22. Наиболее распространенные системы видеонаблюдения.
23. Современные системы контроля и управления доступом.
24. Что необходимо знать при использовании паролей.

ТЕМЫ КОНТРОЛЬНЫХ РАБОТ

По учебной дисциплине «Основы защиты информации»

Вариант №1 – Предложения для обеспечения безопасности пользователей в социальных сетях.

Вариант №2 – Построение BI-платформы в контексте информационной безопасности.

Вариант №3 – Построение биометрической системы для обеспечения информационной безопасности.

Вариант №4 – Защита от вредоносных файлов различных типов.

Вариант №5 – Обнаружение вирусов в PDF-файлах с использованием методов машинного обучения.

Вариант №6 – Механизмы реализации удаленных атак в глобальной сети INTERNET.

Вариант №7 – Средства управления безопасностью в архитектуре операционных систем WINDOWS.

Вариант №8 – Основы безопасности операционных систем семейства UNIX.

Вариант №9 – Модели реконфигурируемой стеганографической системы с применением технологии блокчейн.

Вариант №10 – Защита авторских прав на электронные документы методами стеганографии.

Вариант №11 – Модели защиты информации. Модель Харрисона-Рузо-Ульмана. Модель Белла-ЛаПадулы.

Вариант №12 – Модель многоуровневой защиты. Модель Lifecycle Security.

Вариант №13 – Методика управления рисками, предлагаемая Microsoft.

Вариант №14 – Защита с помощью систем обнаружения и предотвращения вторжений при помощи NIPS/NIDS: Snort.

Вариант №15 – Программное восстановления данных при помощи программы TestDisk.

Вариант №16 – Сканирования сети с помощью Honeypot, Nmap.

Вариант №17 – Системы PGP и TrueCrypt для обеспечения конфиденциальности и целостности информационных ресурсов.

Вариант №18 – Системы идентификации голоса.

Вариант №19 – Технологии синтеза речи из текста (Text-to-Speech, TTS) и клонирования существующего голоса (voice cloning).

Вариант №20 – Приложения Zao, Reface «Дипфейк» от VK.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ДИФФЕРЕНЦИРОВАННОГО ЗАЧЕТА

По учебной дисциплине «Основы защиты информации»

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?

Раздел 5 Защита информации в информационных системах

56. Что вам известно о стеганографических системах защиты информации?

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

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

59. Расскажите почему стеганография есть эффективная защита печатной продукции?

60. Расскажите о машиночитаемых технологиях для традиционных способов печати.

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

62. Какие вам известны криптографические методы защиты информации?

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

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

65. Приведите основную схему криптографии.

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

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

68. Перечислите основные правила организации защиты АСБ.

69. Дайте понятие электронного документа и электронной цифровой подписи

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

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

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

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

Раздел 6 Защита интеллектуальной собственности

74. Приведите примеры объектов интеллектуальной собственности.

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

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

77. Как осуществляется поиск патентной информации в Интернет?

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

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

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

По учебной дисциплине Лабораторный спецпрактикум «Основы защиты информации»

Раздел 1 Основы теории чисел

1. Дать определение понятий: целое число, натуральное число, делимость чисел, собственный делитель, НОД.
2. Сформулировать основную теорему арифметики. Представить примеры ее применения.
3. Пояснить сущность проблемы факторизации и ее с вязь с прикладной криптографией.
4. Найти НОД: пар чисел: 333 и 100; 56 и 200; 99 и 200; 61 и 987; 123 и 456; трех чисел: 21, 43, 342; 57, 31, 200; 42, 11, 98.
5. Записать каноническое разложение чисел: 2770; 3780; 6224.
6. Записать соотношение Безу. Показать пример его практического использования.
7. Подсчитать число взаимно простых чисел с числами 2770, 3780, 6224.
8. Сформулировать малую теорему Ферма. Показать примеры ее практического применения.
9. Сформулировать основные свойства модулярной арифметики.
10. Пояснить порядок операций на основе расширенного алгоритма Евклида.
11. Найти числа, обратные к a по модулю n: a= 41, n= 143; a= 13, n= 71.

Раздел 2 Криптографическая защита информации

12. В чем заключается основная идея криптографических преобразований на основе шифров перестановки?
13. Привести классификационные признаки и дать сравнительную характеристику разновидностям перестановочных шифров.
14. Оцените количество возможных простых перестановок текста, состоящего из пяти символов? Из десяти символов? Из n символов?
15. Охарактеризовать криптостойкость перестановочных и подстановочных шифров.
16. Привести примеры и дать характеристику перестановочным шифрам, не рассмотренным в материалах к данной лабораторной работе.
17. Имеются ли предпочтения в выборе размеров используемой таблицы для перестановочных шифров?
18. Охарактеризовать основные методы взлома перестановочных шифров.
19. В чем заключается основная идея криптографических преобразований на основе шифров замены?
20. Привести классификационные признаки и дать сравнительную характеристику разновидностям подстановочных шифров.
21. Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языков?
22. Найти ключ шифра, с помощью которого получен шифртекст: «byajhvfwbjyyfzgjcktljdfntkmyjcnm».
23. Расшифровать (с демонстрацией каждого шага алгоритма) текст Ci= «qrscqcocqclc», зашифрованный аффинным шифром Цезаря при N= 26, a= 3, b= 5.
24. Зашифровать и расшифровать свою фамилию (на основе кириллицы), используя аффинный шифрЦезаря.

25. Можно ли использовать в качестве ключевого в шифре Виженера слово, равное по длине открытому тексту? Обосновать ответ.

26. По какому признаку можно определить, что текст зашифрован шифром Плейфера?

27. Имеются ли предпочтения в выборе размеров таблицы Трисемуса для виртуального алфавита мощностью 40: 4×10; 10×4; 5×8; 8×5; 2×20; 20×2?

28. Охарактеризовать основные виды атак на шифры.

29. Сравнить криптостойкость шифра Цезаря и шифра Виженера.

30. Опишите принцип работы шифра Виженера.

31. Опишите принцип работы одноразовой системы шифрования.

32. Отличия метода посимвольного шифрования и шифрования текста биграммами.

33. Чем отличаются шифрование биграммами и шифрование биграммами с двойным квадратом?

34. Охарактеризовать основные методы взлома подстановочных шифров.

35. В чем состоит принципиальная разница моноалфавитных и полиалфавитных шифров замены?

36. В каких случаях частотный анализ может эффективно применяться для дешифрования шифров?

37. Какие меры практической стойкости шифра относительно метода криптоанализа вы можете выделить?

38. Что такое псевдослучайная последовательность?

39. Как определяется период псевдослучайной последовательности?

40. Привести классификационные признаки и дать сравнительную характеристику генераторов псевдослучайной последовательности.

41. Охарактеризовать конгруэнтные генераторы случайной последовательности чисел.

42. Каким способом чаще всего осуществляется гаммирование?

43. Гаммирование: основные определения.

44. Двоичное гаммирование: основные особенности.

45. Назовите преимущества и недостатки использования скремблера.

46. Укажите свойства, которыми должна обладать псевдослучайная последовательность, генерируемая скремблером.

47. Для каких целей используют скремблеры и дескремблеры?

48. Опишите алгоритм сети Фейстеля.

49. Какова структура классической сети Фейстеля?

50. Что такое раунд в сети Фейстеля?

51. Какими свойствами обладает сеть Фейстеля?

52. Каким образом используется материал ключа при шифровании?

53. В чем отличие процессов шифрования и дешифрования?

54. Назовите достоинстваи недостатки блочных шифров.

55. Опишите основные шаги алгоритма DES и режимы его работы.

56. Опишите основные шаги алгоритма ГОСТ 28147-89 и режимы его работы.

57. Какова длина ключа и блока в алгоритмах блочного симметричного шифрования?

58. Сколько циклов шифрования выполняется в алгоритмах блочного симметричного шифрования?

59. Что является преимуществом симметричного шифрования?

60. Как иначе называется асимметричное шифрование?

61. Что является преимуществом асимметричного шифрования?

62. Что такое однонаправленные функции?

63. Основные свойства однонаправленных функций с потайным ходом.

64. Опишите основные шаги алгоритма RSA?

65. На чем основана безопасность системы RSA?

66. Как реализуется программное возведение в степень для больших чисел?

67. Опишите основные шаги схемы Эль-Гамаля и ее надежность?

68. Отличие шифра Эль-Гамаля от шифра RSA?

Раздел 3 Обеспечение безопасности информационного обмена с помощью криптографических протоколов

69. Что лежит в основе криптографического контроля целостности?

70. Для чего используется хэш-функция?

71. Что такое хэш-функция? Когда она является криптографически стойкой? Что такое лавинный эффект?

72. Опишите алгоритм MD5.

73. Опишите семейство алгоритмов SHA.

74. Опишите семейство алгоритмов RIPEMD.

75. Что называют коллизией хэш-функции, каковы причины возникновения коллизии?

76. Способы взлома хэш-функции MD5.

77. Приведите примеры использования хэш-функции MD5.

78. Опишите протокол Диффи–Хеллмана?

79. Оцените надежность протокола Диффи–Хеллмана?

80. Какую роль выполняет электронная цифровая подпись?

81. Какие криптоалгоритмы используются для создания электронной цифровой подписи?

82. 2.Что такое криптографическая хэш-функция, какими свойствами она должна обладать?

83. Как содержание сообщение влияет на электронную цифровую подпись?

84. Где используется ЭЦП?

85. В каком случае электронная цифровая подпись при проверке отвергается?

86. Опишите основные шаги алгоритма ЭЦП RSA?

87. В чем отличие применения асимметричных алгоритмов для зашифровывания и для формирования ЭЦП?

88. Зависит ли длина хэш-значения сообщения от длины открытого текста?

89. С помощью какого ключа – открытого или закрытого – подписывается сообщение при использовании ЭЦП?

90. Что может быть идентификатором при аутентификации?

91. Что такое идентификация субъекта?

92. Что такое аутентификация субъекта?

93. Классификация средств аутентификации.

94. Как оценивается эффективность парольного средства аутентификации?

95. Какие виды парольных атак вы знаете?

96. Перечислите основные рекомендации по выбору пароля.

97. Как оценить время жизни пароля?

98. Что такое комбинированные пароли?

99. Что такое «парадокс дня рождения»?

100.В чем особенность биометрических средств аутентификации?

101.Как оценивается эффективность биометрического средства аутентификации?

102.Что собой представляет стеганография?

103.Перечислите области применения стеганографических алгоритмов.

104.От чего зависит стойкость стегосистем?

105.Каковы особенности встраивания и извлечения информации из стегоконтейнера?

Раздел 4 Механизмы обеспечения информационной безопасности

106.Охарактеризовать основные методы разграничения доступа.

107.Каким образом представляются полномочия субъекта информационной системы?

108.Какие действия нужно выполнить при шифровании симметричным алгоритмом с использованием криптографических библиотек PGP и TrueCrypt?

109.Какие действия нужно выполнить при шифровании асимметричным алгоритмом с использованием криптографических библиотек PGP и TrueCrypt?

110.Какие действия нужно выполнить при вычислении и проверке электронной цифровой подписи с использованием криптографических библиотек PGP и TrueCrypt?

111.Какие действия нужно выполнить при хэшировании с использованием криптографических библиотек PGP и TrueCrypt?

112.Каково назначение и возможности оснастки «Групповая политика»?

113.2.Способ запуска оснастки «Групповая политика», принудительное обновление групповых политик из командной строки.

114.3.Способ запуска оснастки «Локальная политика безопасности», примеры параметров.

115.4.Область и время начала действия параметров из разделов «Конфигурация компьютера» и «Конфигурация пользователя» в групповой политике.

116.Назначение и способ запуска оснастки «Результирующая политика».

117.Для чего необходимо создавать резервную копию?

118.Какие способы создания резервной копии вам известны?

119.Какова цель резервного копирования данных?

120.Перечислите виды резервного копирования данных?

121.Какие предъявляют требования к системе резервного копирования?

122.Назовите журналы, используемые в ОС Windows.

123.Что отражается в журналах ОС Windows?

124.Какие категории пользователей имеют возможность доступа к журналам ОС Windows?

125.Как производится включение и настройка аудита в ОС Windows?

126.Какие категории событий могут отслеживаться в Windows?

127.Как производится настройка аудита обращений к файлам?

128.Какие события, связанные с обращением к файлам, могут отслеживаться?

129.Какая информация приводится в журналах?

130.Прокомментируйте записи в журнале безопасности, соответствующие входу в систему.

131.Прокомментируйте записи в журнале безопасности, соответствующие аудиту управления учетными записями.

132.Прокомментируйте записи в журнале безопасности, соответствующие изменению политики.

133.Прокомментируйте записи в журнале безопасности, соответствующие использованию привилегий.

134.Как можно определить время работы пользователя с определенным приложением или файлом данных?

135.Какие типы учетных записей используются в Windows? Какие права предоставляет каждый тип?

136.Каковы основные ветви реестра?

137.Что такое куст?

138.Где и как хранится реестр?

139.Что хранится в основных кустах реестра?

140.Как обеспечивается целостность данных в реестре?

141.Какие вы можете дать рекомендации по усилению защиты реестра?

142.Как установить аудит реестра?

143.Какие события можно отследить с помощью аудита реестра?

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

по учебной дисциплине «Основы защиты информации»

Обучение дисциплине «Основы 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;
- выполнение практических упражнений (работа с тренажерами) для закрепления знаний и навыков;
- решение во внеурочное время контрольных задач, получаемых на лекциях;
- углублённое изучение отдельных тем учебной дисциплины для подготовки к устным опросам;
- изучение основной и дополнительной и научной литературы в процессе подготовки к анализу и решению проблемных задач, реализации элементов исследовательской деятельности;
- подготовка к контрольному тестированию;
- систематизация полученных знаний при подготовке к дифференцируемому зачету;

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

- наличием и использованием в образовательном 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;
- 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 **4R8VVLN.**
2. Материалы, размещённые на бесплатном сервисе для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google Класс Room университета: шифр курса **4Z6MV6P**.
3. Методические указания к выполнению лабораторных работ по дисциплине «Основы защиты информации» для студентов специальности 1-31 04 08 «Компьютерная физика».

Содержание самостоятельной работы студентов
(дневная форма получения высшего образования)

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины	*Тема 2.3 Компьютерные вирусы и антивирусные программы* Понятие вирус. История компьютерных вирусов. Деструктивные возможности и пути проникновения вирусов. Методы защиты от вирусов. Осн. лит.: [2], [3]. Доп. лит.: [6], [10].	4
	Тема 4.2 Обзор технических средств негласного съёма акустической информации Закладочные устройства. Технические средства дистанционного съёма информации. Технические средства съёма информации с линий связи. Осн. лит.: [1], [2]. Доп. лит.: [3], [4], [5], [7].	4
	Тема 4.6 Программно-аппаратные системы защиты информации Системы охранно-пожарной сигнализации. Системы видеонаблюдения. Системы контроля и управления доступом. Осн. лит.: [1], [2]. Доп. лит.: [3], [4], [5], [7].	4
	Тема 5.1 Стеганографические системы защиты информации Компьютерная стеганография. Методы компьютерной стеганографии. Разработка новых машиночитаемых защитных признаков. Осн. лит.: [1], [2]. Доп. лит.: [2], [12].	4
	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. Доп. лит.: [12].	4
Выполнение контрольной работы		10
Подготовка к реферативному выступлению		8
Систематизация полученных знаний при подготовке к дифференцированному зачету		10
	ИТОГО:	**48**

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

По учебной дисциплине «Лабораторный спецпрактикум «Основы защиты информации»»

Обучение «Лабораторному спецпрактикуму «Основы защиты информации»» предполагает реализацию следующих форм самостоятельной работы студентов:

– проработка учебной литературы;

– изучение печатных источников по теме дисциплины;

–изучение вопросов для самоконтроля;

– выполнение практических заданий по лабораторным работам для закрепления умений и навыков;

–углублённое изучение отдельных тем для подготовки к защите лабораторных работ;

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

–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 СДО Moodle, доступной пользователям через Интернет в любое удобное для них время;

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

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещённые в СДО Moodle для групповой работы и общения s: режим доступа **https://study.psu.by/course/edit.php?id=588**.

Содержание самостоятельной работы студентов
(дневная форма получения высшего образования)

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Подготовка к защите отчетов по лабораторным работам	**Лабораторная работа №1** Использование алгоритмов теории чисел в криптографии	1
	Лабораторная работа №2 Шифрование данных криптоалгоритмом перестановки	1
	Лабораторная работа №3 Шифрование данных криптоалгоритмом простой замены	2
	Лабораторная работа №4 Шифрование данных криптоалгоритмом многоалфавитной замены	2
	Лабораторная работа №6 Исследование криптосистемы DES	2
	Лабораторная работа №7 Исследование криптосистемы ГОСТ 28147	2
	Лабораторная работа №8 Анализ генераторов псевдослучайной последовательности	1
	Лабораторная работа №9 Исследование шифра гаммирования	1
	Лабораторная работа №10 Реализация арифметики больших чисел	2
	Лабораторная работа №11 Программная реализация генератора простых чисел	1
	Лабораторная работа №12 Реализация алгоритмов модульной арифметики	1
	Лабораторная работа №13 Реализация алгоритма Евклида, расширенного алгоритма Евклида	1
	Лабораторная работа №14 Анализ односторонних функций	1
	Лабораторная работа №15 Реализация программы шифрования асимметричной криптосистемы	2
	Лабораторная работа №16 Реализация программы дешифрования асимметричной криптосистемы	2
	Лабораторная работа №17 Исследование криптографических хеш-функций	2
	Лабораторная работа №18 Генерация электронной цифровой подписи в документе	1
	Лабораторная работа №19 Верификации электронной цифровой подписи документа	1
	Лабораторная работа №20 Исследование показателей эффективности парольных средств аутентификации	1
	Лабораторная работа №21 Исследование показателей эффективности биометрических средств аутентификации	1

1	2	3
	Лабораторная работа №22 Исследование методов компьютерной стеганографии	2
	Лабораторная работа №23 Программная реализация протокола простой аутентификации	2
	Лабораторная работа №24 Программная реализация протокола многофакторной аутентификации	2
	Лабораторная работа №25 Использование программной систем PGP и TrueCrypt для обеспечения конфиденциальности и целостности информационных ресурсов	2
	Лабораторная работа №26 Получение практических навыков программного восстановления данных при помощи программы TestDisk	2
	Лабораторная работа №27 Реализация политики безопасности в защищенных версиях операционной системы Windows. Создание и удаление учетной записи пользователя, групп пользователей	2
	Лабораторная работа №28 Разграничение прав пользователей в защищенных версиях операционной системы Windows. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows	2
	Лабораторная работа №29 Аудит информационных процессов в операционной системе Windows. Аудит реестра в операционной системе Windows	2
	Лабораторная работа №30 Выполнение зачётной итоговой работы	2
	ИТОГО:	**48**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

по учебной дисциплине «Основы защиты информации»

Учебном планом специальности в качестве формы промежуточной аттестации по учебной дисциплине «Основы защиты информации» предусмотрен дифференцированный зачет. Оценка учебных достижений студента производится по десятибалльной шкале.

Диагностика 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) (далее – Положение) в форме текущего контроля и промежуточной аттестации.

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

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

– устная форма (блиц-опрос на лекциях, реферативные выступления);

– письменная форма (тесты, контрольные опросы, контрольные работы, письменные отчеты по практическим работам, рефераты);

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

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

Практические работы предполагают выполнение и защиту. Последнее практическое занятие в семестре предусматривает выполнение и защиту зачётной итоговой 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.

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

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_n) + (\text{ПР}_1 + \ldots + \text{ПР}_{14}) + (\text{КР}_1))}{(15 + n)},$$

где $\text{КТ}_1 + \ldots + \text{КТ}_n$ – отметки, выставленные по результатам контрольного тестирования;

$\text{ПР}_1 + \ldots + \text{ПР}_{14}$ – отметки, выставленные по результатам защит практических работ;

n – количество тестов;

КР_1 – отметка, выставленная по результатам контрольной работы.

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

В таблице 2 представлены составляющие, формирующие отметку текущего контроля Т по дисциплине.

Таблица 2 – Составляющие отметки текущего контроля Т по дисциплине

Мероприятия текущего контроля	**Содержание мероприятий текущего контроля – название раздела (темы)**	**Задания мероприятия текущего контроля**	**Отметка мероприятий текущего контроля** (КР), (КТ), (ПР)
Контрольная работа	См. темы контрольных работ	Предлагается выполнить контрольную работу по указанной теме согласно варианту.	Максимальная отметка 10 (десять) баллов
Контрольный тест	Темы и планируемые контрольные тесты указаны в учебно-методической карте дисциплины	Тест ориентирован на прохождение в online-режиме и оформлен в **Google Forms** и размещен в **Google Класс Room**	Максимальная отметка 10 (десять) баллов

Промежуточная аттестация проводится в форме дифференцированного зачёта.

Дифференцированный зачет проводится согласно Положению.

Итоговая отметка по дифференцированному зачету (ИДЗ) учитывает отметку по результатам текущего контроля (Т) и отметку дифференцированному зачету (ДЗ). Весовой коэффициент k принимается равным 0,5. Информация о весовом коэффициенте доводится до студентов па первом занятии в семестре. Составляющие для формирования итоговой отметки по дисциплине и их весовые коэффициенты представлены в таблице 3.

Таблица 3 – Составляющие итоговой отметки по дисциплине

Составляющие (ИДЗ)	k	Т	$1-k$	ДЗ
	0,5	Представлены в таблице 2	0,5	*

*Отметка, полученная студентом на дифференцированном зачете за письменный ответ по билету.

Итоговая отметка по дисциплине определяется по формуле:

$$ИЭ = 0{,}5Т + 0{,}5ДЗ.$$

Положительной является отметка не ниже 4 баллов.

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

по учебной дисциплине «Лабораторный спецпрактикум «Основы защиты информации»»

Учебном планом специальности в качестве формы промежуточной аттестации по «Лабораторному спецпрактикуму «Основы защиты информации»» предусмотрен зачет.

Диагностика 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) (далее – Положение) в форме текущего контроля и промежуточной аттестации.

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

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

–письменная форма (письменные отчеты по лабораторным работам);

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

Лабораторные работы предполагают выполнение и защиту. Последнее лабораторное занятие в семестре предусматривает выполнение и защиту зачётной итоговой работы. 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 *текущего контроля за семестр* оценивается отметкой в баллах по десятибалльной шкале и выводится, исходя из отметок, выставленных в ходе проведения мероприятий текущего контроля в течение семестра по следующей формуле:

$$\text{Т} = \frac{(\text{ЛР}_1 + \ldots + \text{ЛР}_n)}{n},$$

где $\text{ЛР}_1 + \ldots + \text{ЛР}_n$ – отметки, выставленные по результатам защит лабораторных работ;

n – количество лабораторных работ, предусмотренных к выполнению к дате текущего контроля.

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

Промежуточная аттестация проводится в форме зачёта. Зачёт проводится согласно Положению.

Заключение о *зачёте* формируется по формуле:

$$\text{З} = k \cdot \text{Т},$$

где k– весовой коэффициент текущего контроля;

Т – результат текущего контроля за семестр.

Для выставления зачета весовой коэффициент k принимается равным 1. Отметка «зачтено» выставляется студентам, получившим по результатам текущего контроля 4 балла и выше.

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

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНООГО МОДУЛЯ

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

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

– учебно-исследовательская деятельность.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплин «Основы защиты информации» и «Лабораторного спецпрактикума «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 занятиях, на которых студенты овладевают системой теоретических знаний в области защиты информации и информационной безопасности и формируют системное понимание проблем защиты информации и информационной безопасности и путей их решения и практических занятиях, на которых развиваются и формируются необходимые практические умения и навыки.

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.

Во время проведения практических работ по дисциплине «Основы защиты информации» и лабораторных занятий по учебной дисциплине «Лабораторного спецпрактикума «Основы защиты информации»» особое внимание уделяется формированию у студентов умения планировать свою работу и определять эффективную последовательность её выполнения.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, по которой требуется согласование	**Название кафедры**	**Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине**	**Решение, принятое кафедрой, разработавшей учебную программу**
«Системы управления базами данных»	Кафедра физики	предложений и дополнений нет	
«Компьютерные методы статистического анализа данных»	Кафедра физики	предложений и дополнений нет	
«Программирование на суперкомпьютерах»	Кафедра физики	предложений и дополнений нет	
«Программные методы автоматизации эксперимента»	Кафедра физики	предложений и дополнений нет	
«Лабораторный спецпрактикум «Современные технологии программирования»»	Кафедра физики	предложений и дополнений нет	

Заведующий кафедрой физики, к.ф.-м.н., доцент С.А. Вабищевич