Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный университет
имени Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«27» 06 2025 г.
Регистрационный № УД –57/25/уч.

ОСНОВЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебная программа учреждения образования
по учебной дисциплине для всех специальностей
общего и специального высшего образования

2025 г.

Учебная программа составлена на основе учебных планов учреждения образования по специальностям общего и специального высшего образования для дневной формы получения образования.

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

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 6 от «27» 05 2025 г.);

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» (протокол № 7 от «27» 06 2025 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

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

Целью изучения дисциплины «Основы безопасности информационных систем» является обучение студентов основам построения и использования современных защищенных информационных компьютерно-коммуникационных систем; подготовка специалистов, умеющих создавать защищенные информационные системы и исследовать защищенность компьютерно-коммуникационных систем.

Изучение данной дисциплины является необходимым этапом в профессиональном развитии специалиста любой из специальностей общего и специального высшего образования

Задачи изучения дисциплины. «Основы безопасности информационных систем». При изучении данной дисциплины требуется разрешить основные задачи:

– сформировать у студентов понимание базовых понятий, связанных с процессом обеспечения информационной безопасности, кибербезопасности и защиты информации;

– сформировать системное понимание проблем безопасности и путей их решения;

– показать основные угрозы безопасности и меры противодействия им, а также показать возможности анализа и управления рисками в сфере информационной безопасности;

– сформировать системное понимание проблем безопасности и путей их решения.

При изучении дисциплины «Основы безопасности информационных систем» у студентов должен сформироваться набор базовых компетенций в области информационной безопасности информационных систем, обеспечивающих выпускникам успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

В результате изучения учебной дисциплины «Основы безопасности информационных систем» формируются следующие **специализированные компетенции:**

Осуществлять поиск, критический анализ информации, применять системный подход для решения поставленных задач в самостоятельной деятельности, вырабатывать стратегию действий, генерировать и реализовывать инновационные идеи, осуществлять социальное взаимодействие и реализовывать свою роль в команде.

В результате изучения дисциплины «Основы безопасности информационных систем» обучаемый должен:

знать:

- системную методологию и правовое обеспечение информационной безопасности информации;
- приоритеты развития информационных технологий, повышающих эффективность защиты информационного пространства Союзного государства Беларуси и России в современных условиях;
- основные понятия в области национальной безопасности и информационной безопасности;
- векторы угроз 5-го поколения;
- как защитить информацию от утечки и разрушения при работе на компьютере и в Интернете;
- что такое разграничение прав доступа;
- в чем отличие понятий: идентификация, аутентификация и авторизация;

- особенности современных компьютерных вирусов и возможности антивирусных программ;
- что такое стеганографические системы защиты информации;

уметь:

- определять возможные каналы утечки информации;
- применять на практике криптографические методы защиты при работе в мессенджерах или с электронной почтой;
- уметь применять на практике методы стеганографии для подтверждения подлинности электронных и других документов;

владеть:

- основными приемами анализа вероятных угроз информационной безопасности для заданных объектов.

Связи с другими учебными дисциплинами.

Для изучения учебной дисциплины «Основы безопасности информационных систем» необходимы знания, полученные при изучении дисциплин, связанных с обработкой данных.

Знания, полученные при изучении дисциплины «Основы безопасности информационных систем», являются основой для дисциплин, в которых используются понятия анализа и обработки данных, персональных данных.

Форма получения высшего образования - дневная

В соответствии с учебными планами специальностей общего и специального высшего образования учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой» на изучение учебной дисциплины отводится:

Курс	3
Семестр	5
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	46
В том числе:	
Лекции, часов	30
Практические занятия, часов	16
Самостоятельная работа, часов	62
Форма промежуточной аттестации	зачет
Трудоёмкость дисциплины, зач. ед	3

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

Цели и задачи изучения дисциплины.

Государственные органы и учреждения, занимающиеся вопросами информационной безопасности 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 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Тема 1.1 Основы безопасности информационных систем.

Отличительные черты информационного общества. Понятие информационной безопасности. Цели и задачи, решение которых должна обеспечивает информационная безопасность. Информационное общество. Безопасность в информационном обществе. Информационная безопасность и ее составляющие. Аспекты информационной безопасности. Место информационной безопасности в системе национальной безопасности. Структура системы безопасности. Общая схема процесса обеспечения безопасности. Положения государственной политики информационной безопасности РБ. Система информационной безопасности РБ. Государственная система защиты РБ.

Тема 1.2. Системная методология информационной безопасности.

Понятие информации. Характеристики информации. Потребители и обладатели информации. Основные формы проявления информации. Информационная безопасность и защита информации. Основные понятия и терминология в области защиты информации.

Тема 1.3. Информационное обеспечение деятельности (бизнеса).

Документоведение. Документационное обеспечение управления. Общая характеристика процессов сбора, передачи, обработки и накопления информации. Управление знаниями. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Охраняемые сведения и демаскирующие признаки. Классификация методов защиты информации.

Тема 1.4. Угрозы информационной безопасности.

Угрозы безопасности информационно-коммуникационных технологий. Классификация умышленных угроз. Общая классификация угроз. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности. Анализ угроз информационной безопасности информационно-коммуникационных технологий. Система дестабилизирующих факторов, влияющих на уязвимость информации. Методология формирования полного множества угроз. Основные методы реализации угроз. Информационная война как угроза национальной безопасности. Понятие информационной войны и ее особенности. Информационное оружие.

Раздел 2. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 2.1. Уровни информационной безопасности.

Законодательный уровень информационной безопасности. Обзор белорусского и российского законодательств. Международные стандарты и спецификации. «Оранжевая

книга». Рекомендации X.800. «Общие критерии». Гармонизированные критерии европейских стран. Административный уровень информационной безопасности. Процедурный уровень информационной безопасности. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Программно-технический уровень информационной безопасности.

Тема 2.2. Политика информационной безопасности.

Понятие политики безопасности. Основные типы и содержание политик безопасности. Принципы государственной политики обеспечения информационной безопасности. Система защиты государственной тайны. Системы менеджмента безопасности информации. Правила и требования. Управление информационной безопасностью. Управление рисками. Аудит информационной безопасности. Стандарты ISO/IEC 17799/27002 и 27001.

РАЗДЕЛ 3 ПРАВОВОЕ ОБЕСПЕЧЕНИЕ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 3.1 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». Указ Президента Республики Беларусь 28 октября 2021 г. № 422 О мерах по совершенствованию защиты персональных данных. Закон РБ от 7 мая 2021 г. № 99-З О защите персональных данных. Указ Президента Республики Беларусь от 14.02.2023 №40 О кибербезопасности.

Тема 3.2 Правовые методы защиты информации.

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

Тема 3.3 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 4 ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема 4.1 Классификация технических каналов утечки информации.

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

Тема 4.2 Звуковые сигналы.

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

Понятие шума. Основные характеристики шума. Применение шумов для маскирования речевых сигналов. Синтез смеси гармонического сигнала и шума с заданным отношением сигнал/шум.

Тема 4.3 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. Типы технических средств защиты информации. Подавители записывающих устройств. Обнаружители закамуфлированных камер. Устройства для активной защиты речевой информации от утечки по акустическому и вибрационному каналам.

РАЗДЕЛ 5 ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 5.1 Стеганографические системы защиты информации.

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

Тема 5.2 Криптографические методы защиты информации.

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

Тема 5.3 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.

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 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.

Учебно-методическая карта учебной дисциплины «Основы безопасности информационных систем»

Дневная форма получения высшего образования

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

1	2	3	4	5	6	7	8
	Раздел 1 Теоретические Основы безопасности информационных систем	**6**	**4**				
2	**Лекция № 2** *Тема 1.1 Основы безопасности информационных систем* Отличительные черты информационного общества. Понятие информационной безопасности. Цели и задачи, решение которых должна обеспечивает информационная безопасность. Информационное общество. Безопасность в информационном обществе. Информационная безопасность и ее составляющие. Аспекты информационной безопасности. Место информационной безопасности в системе национальной безопасности. Структура системы безопасности. Общая схема процесса обеспечения безопасности. Положения государственной политики информационной безопасности РБ. Система информационной безопасности РБ. Государственная система защиты РБ. *Тема 1.2 Системная методология информационной безопасности* Понятие информации. Характеристики информации. Потребители и обладатели информации. Основные формы проявления информации. Информационная безопасность и защита информации. Основные понятия и терминология в области защиты информации.	2				Осн. лит.: [1], [2], [3], [6], [7]. Доп. лит.: [18], [24], [28], [32], [34] Нормативная: [1], [14], [15], [16], [17], [18], [21].	*Тест №1
3	**Практическая работа №1** Изучение Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (утв. Постановлением Совета Министров Республики Беларусь 15.05.2013 № 375).		2				Защита отчёта по практическому занятию № 1
4	**Лекция № 3** *Тема 1.3. Информационное обеспечение деятельности (бизнеса).* Документоведение. Документационное обеспечение управления. Общая характеристика процессов сбора, передачи, обработки и накопления информации. Управление знаниями. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Охраняемые сведения и демаскирующие признаки. Классификация методов защиты информации.	2				Осн. лит.: [1], [2], [3], [6]. Доп. лит.: [18], [24], [28], [32], [34] Нормативная: [2], [3], [4], [5], [11].	Блиц-опрос

1	2	3	4	5	6	7	8
5	**Лекция № 4** *Тема 1.4. Угрозы информационной безопасности.* Угрозы безопасности информационно-коммуникационных технологий. Классификация умышленных угроз. Общая классификация угроз. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности. Анализ угроз информационной безопасности информационно-коммуникационных технологий. Система дестабилизирующих факторов, влияющих на уязвимость информации. Методология формирования полного множества угроз. Основные методы реализации угроз. Информационная война как угроза национальной безопасности. Понятие информационной войны и ее особенности. Информационное оружие.	2				Осн. лит.:[5], [7]. Доп. лит.: [7], [10], [18], [22].	Блиц-опрос
6	**Практическая работа №2** Организация защиты баз данных в СУБД Microsoft ACCESS. Использование пароля для шифрования базы данных в СУБД Microsoft Access.		2				Защита отчёта по практическому занятию № 2
	Раздел 2 Политика информационной безопасности	**4**	**2**				
7	**Лекция № 5** *Тема 2.1. Уровни информационной безопасности.* Законодательный уровень информационной безопасности. Обзор белорусского и российского законодательств. Международные стандарты и спецификации. «Оранжевая книга». Рекомендации X.800. «Общие критерии». Гармонизированные критерии европейских стран. Административный уровень информационной безопасности. Процедурный уровень информационной безопасности. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Программно-технический уровень информационной безопасности.	2				Осн. лит.: [1], [2], [3], [5], [7]. Доп. лит.: [7], [18], [26]. Эл. рес.: [1], [5], [7], [8].	Блиц-опрос
8	**Лекция № 6** *Тема 2.2. Политика информационной безопасности.* Понятие политики безопасности. Основные типы и содержание политик безопасности. Принципы государственной политики обеспечения информационной безопасности. Система защиты государственной тайны. Системы менеджмента безопасности информации. Правила и требования. Управление информационной безопасностью. Управление рисками. Аудит информационной безопасности. Стандарты ISO/IEC 17799/27002 и 27001.	2				Осн. лит.:[5], [7]. Доп. лит.: [7], [18]. Нормативная: [2], [3], [4], [10], [11].	*Тест №2

1	2	3	4	5	6	7	8
9	**Практическая работа №3** Организация защиты баз данных в СУБД Microsoft ACCESS. Работа с Центром управления безопасностью. Организация защиты базы данных в СУБД Microsoft ACCESS.		2				Защита отчёта по практическому занятию № 3
	Раздел 3 Правовое обеспечение и методы защиты информации	**6**	**2**				
10	**Лекция № 7** *Тема 3.1 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». Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 О мерах по совершенствованию защиты персональных данных. Закон РБ от 7 мая 2021 г. № 99-З О защите персональных данных. Указ Президента Республики Беларусь от 14.02.2023 №40 О кибербезопасности.	2				Осн. лит.:[5], [7]. Доп. лит.: [7], [18], [23]. Нормативная: [15], [16], [17], [18], [19], [20], [21], [22], [23].	Блиц-опрос
11	**Лекция № 8** *Тема 3.2 Правовые методы защиты информации.* Правовая защита от компьютерных преступлений. Виды компьютерных преступлений Примеры известных компьютерных преступлений. Виды компьютерных преступлений, мошенничество в интернете. Использование специальных программных средств мошенниками. Полезные советы по компьютерной безопасности.	2				Осн. лит.:[5], [7]. Доп. лит.: [7], [18], [23]. Нормативная: [23].	*Тест №3
12	**Практическая работа №4** Правовое обеспечение информационной безопасности. Выявление и фиксация следов противоправной деятельности на ПЭВМ.		2				Защита отчёта по практическому занятию № 4

1	2	3	4	5	6	7	8
13	**Лекция № 9** *Тема 3.3 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.:[4], [5]. Доп. лит.: [9], [13], [16], [21], [18], [23].	Блиц-опрос
	Раздел 4 Инженерно-техническая защита объектов от несанкционированного доступа	**4**	**2**				
14	**Лекция № 10** *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 Звуковые сигналы* Звуковые сигналы. Пример создания гармонического и полигармонического сигнала. Основные характеристики гармонического сигнала. Энергетический спектр речевого сигнала. Понятие шума. Основные характеристики шума. Применение шумов для маскирования речевых сигналов. Синтез смеси гармонического сигнала и шума с заданным отношением сигнал/шум.	2				Осн. лит.:[4], [5]. Доп. лит.: [9], [13], [16], [21], [18], [23], [29], [30], [31].	Блиц-опрос
15	**Практическая работа №5** Оценка первичных признаков элементов речевого сигнала.		2				Защита отчета по практическому занятию № 5
16	**Лекция № 11** *Тема 4.3 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. Типы технических средств защиты информации. Подавители записывающих устройств. Обнаружители закамуфлированных камер. Устройства для активной защиты речевой информации от утечки по акустическому и вибрационному каналам.	2				Осн. лит.:[4], [5]. Доп. лит.: [9], [13], [16], [21], [18], [23], [29], [30], [31].	*Тест №4

1	2	3	4	5	6	7	8
	Раздел 5 Построение систем защиты информации	**10**	**6**				
17	**Лекция № 12** *Тема 5.1 Стеганографические системы защиты информации.* Понятие стеганографии. Основные достоинства стеганографии. Компьютерная стеганография. Стеганография – эффективная защита печатной продукции. Машиночитаемые технологии для традиционных способов печати. Методы компьютерной стеганографии. Разработка новых машиночитаемых защитных признаков. Производственный контроль.	2				Осн. лит.: [5]. Доп. лит.: [12], [20], [25].	Блиц-опрос
18	**Практическая работа №6** Создание маскирующего шума для имитации виброакустического зашумления.		2				Защита отчета по практическому занятию № 6
19	**Лекция № 13** *Тема 5.2 Криптографические методы защиты информации.* Основные понятия: криптология, криптография, криптоанализ. Коды, шифры и ключи: открытые и закрытые. Основная схема криптографии.	2				Осн. лит.: [5]. Доп. лит.: [33], [25], [27], [28].	*Тест №5
20	**Лекция № 14** *Тема 5.3 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.	2				Доп. лит.: [9], [11].	Блиц-опрос
21	**Практическая работа №7** Изучение методов защиты информации с помощью различных видов шифров, используемых в криптографии.		2				Защита отчёта по практическому занятию № 7
22	**Лекция № 15** *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					*Тест №6

1	2	3	4	5	6	7	8
	Тема 5.5 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.					Осн. лит.: [5], [7]. Доп. лит.: [6], [8], [12], [18], [19], [20], [25], [28], [33]. Нормативная: [12], [24].	*Реферативное выступление с докладом
24	**Практическая работа №8** Штриховое кодирование информации. Анализ реальных штрих-кодов.		2				Защита отчета по практическому занятию № 8
	Всего	**30**	**16**				

*** МЕРОПРИЯТИЯ ТЕКУЩЕГО КОНТРОЛЯ**

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. 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».

2. Системы защиты информации в ведущих зарубежных странах : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, М. В. Рудановский, Г. В. Кондрашин ; 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: 03.09.2025). – Библиогр.: с. 192-193. – ISBN 978-5-9765-1274-0. – Текст : электронный.

3. 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.

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

5. Скулкин, О. Шифровальщики : как реагировать на атаки с использованием программ-вымогателей : [16+] / О. Скулкин ; науч. ред. А. Алексеев ; ред. К. Ахметов ; пер. с англ. А. Власюк. – Москва : Альпина Паблишер, 2023. – 205 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=707831 (дата обращения: 19.03.2024). – ISBN 978-5-206-00080-1. – Текст : электронный.

6. Финансовая кибербезопасность : учебное пособие : [16+] / Е. Н. Макаренко, М. В. Ходорковский, Е. Н. Алифанова [и др.] ; под ред. Е. Н. Макаренко ; Ростовский государственный экономический университет (РИНХ). – Ростов-на-Дону : Издательско-полиграфический комплекс РГЭУ (РИНХ), 2022. – 265 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=711256 (дата обращения: 19.03.2024). – Библиогр. в кн. – ISBN 978-5-7972-3155-4. – Текст : электронный.

7. Шнайер, Б. Взломать всё : как сильные мира сего используют уязвимости систем в своих интересах : практическое пособие : [16+] / Б. Шнайер ; науч. ред. А. Деркач ; ред. Д. Орлов ; пер. с англ. М. Белоголовского. – Москва : Альпина Паблишер, 2023. – 376 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=707381 (дата обращения: 19.03.2024). – ISBN 978-5-9614-8310-9 (рус.). – ISBN 978-0-3938-6666-7 (англ.). – Текст : электронный.

Дополнительная:

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

Гурова Е. В.

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

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

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

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

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

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

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

9. Герасименко, В.А. Основы информационной грамоты. / В.А. Герасименко. – М.: Энергоатомиздат, 1996. –320 с

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс]: учебное пособие / В.А. Сердюк; Высшая Школа Экономики Национальный Исследовательский Университет. – М.: Издательский дом Государственного университета Высшей школы экономики, 2015. – 574 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=440285. – Дата доступа: 19.03.2018.

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

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

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

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

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

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

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

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

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

Нормативная:

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

2. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью. https://files.stroyinf.ru/Index2/1/4293850/4293850664.htm.

3. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

4. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. https://pqm-online.com/assets/files/lib/std/gost-r-iso-mek-27001-2021.pdf.

5. ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. https://protect.gost.ru/v.aspx?control=8&baseC=6&page=280&month=7&year=2016&search=%D1%80&RegNum=1&DocOnPageCount=15&id=230363&pageK=6AC18A47-73C0-4E1E-9792-67CF7F074B94.

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

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

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

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

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

11. СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

12. СТБ РБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи».

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

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

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

16. Закон Республики Беларусь «О Государственных Секретах» №170-З от 19.07.2010. [Электрон, ресурс]. – Режим доступа: http://www.minfin.gov.by/upload/gosznak/acts/zakon_190710_170z.pdf. – Дата доступа: 19.03.2019.

17. Закон Республики Беларусь «Об информации, информатизации и защите информации» № 455-З от 10.11.2008. [Электрон, ресурс]. – Режим доступа: http://www.pravo.by/main.aspx?guid=3871&p0=h10800455&p2={NRPA}. – Дата доступа: 19.03.2019.

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

19. Закон Республики Беларусь «О коммерческой тайне» № 16-З от 05.01.2013. [Электрон, ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=H11300016. — Дата доступа: 19.03.2019.

20. Закон Республики Беларусь 7 мая 2021 г. № 99-З «О защите персональных данных». [Электрон, ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551&p0=H12100099&p1=1. – Дата доступа: 19.03.2022.

21. Указ Президента Республики Беларусь 28 октября 2021 г. № 422 О мерах по совершенствованию защиты персональных данных. – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-422-ot-28-oktyabrya-2021-g. – Дата доступа: 19.02.2022.

22. Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности». – Режим доступа: https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g. – Дата доступа: 19.02.2023.

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

24. Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи». – Режим доступа: https://pravo.by/document/?guid=3961&p0=H10900113. – Дата доступа: 19.02.2022.

Электронные ресурсы:

1. Научно-исследовательский институт технической защиты информации. [Электрон, ресурс]. – Режим доступа: http://www.niitzi.by. – Дата доступа: 19.03.2019.

2. Национальный открытый университет. [Электрон, ресурс]. – Режим доступа: http://www.intuit.ru. – Дата доступа: 19.03.2019.

3. Национальный правовой портал Республики Беларусь. [Электрон, ресурс]. – http://www.pravo.by. – Дата доступа: 19.03.2019.

4. Национальный центр интеллектуальной собственности. [Электрон, ресурс]. – Режим доступа: http://www.belgospatent.org.by. – Дата доступа: 19.03.2019.

5. Оперативно-аналитический центр при Президенте Республики Беларусь [Электрон, ресурс]. – Режим доступа: http://oac.gov.by. – Дата доступа: 19.03.2019.

6. Министерство связи и информатизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: http://www.mpt.gov.by. – Дата доступа: 19.03.2019.

7. International Organization for Standardization (Международная Организация Стандартизации). [Электрон, ресурс]. – Режим доступа: http://www.iso.org (http://www.iso.ch). – Дата доступа: 19.03.2019.

8. Your Private Network (Лаборатория Сетевой Безопасности). [Электрон, ресурс]. – Режим доступа: http://ypn.ru/177/international-standards-of-information-technologies-security. – Дата доступа: 19.03.2019.

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

Перечень компьютерных программ:

Используются пакеты: Microsoft Office Access; Matlab; Mathcad; NI LabView.

ПЕРЕЧЕНЬ ТЕМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

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

Практическая работа №2 Организация защиты баз данных в СУБД Microsoft ACCESS. Использование пароля для шифрования базы данных в СУБД Microsoft Access.

Практическая работа №3 Организация защиты баз данных в СУБД Microsoft ACCESS. Работа с Центром управления безопасностью. Организация защиты базы данных в СУБД Microsoft ACCESS.

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

Практическая работа №5 Оценка первичных признаков элементов речевого сигнала.

Практическая работа №6 Создание маскирующего шума для имитации виброакустического зашумления.

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

Практическая работа №8 Штриховое кодирование информации. Анализ реальных штрих-кодов.

ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

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

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

1. Сформулируйте цель и основные задачи изучения дисциплины «Основы безопасности информационных систем».
2. Государственные органы и учреждения, занимаются вопросами информационной безопасности в РБ?

Раздел 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

3. Назовите основные проблемы информационной безопасности в современном мире.
4. Какие законы РБ в области защиты информации вы знаете? Назовите приоритетные направления в РБ в области защиты информации.
5. Укажите государственные органы и учреждения, занимающиеся вопросами защиты информации в РБ.
6. Назовите отличительные черты информационного общества. Дайте понятие информации.
7. Разделите понятия потребители и обладатели информации.
8. Перечислите основные компоненты безопасности. Что понимается под безопасностью?
9. Приведите основные элементы в структуре системы безопасности.
10. Перечислите аспекты информационной безопасности.
11. Укажете задачи, решение которых должна обеспечивает информационная безопасность.
12. Что включает в себя системная методология информационной безопасности?
13. Сформулируйте основные понятия в области защиты информации.
14. Приведите классификацию угроз. Приведите полную классификацию методов защиты информации.
15. Что относится к охраняемым сведениям? Приведите примеры демаскирующих признаков.
16. Дайте понятие информационной войны и укажите ее особенности.
17. Приведите примеры информационного оружия.
18. Дайте понятия: идентификация, аутентификация, управление доступом.
19. Сформулируйте основные положения государственной политики информационной безопасности РБ.
20. Дайте понятия «Система информационной безопасности РБ», «Государственная система защиты РБ».
21. Перечислите основные функции системы информационной безопасности. Какие проводятся в Республике мероприятия по защите информации?
22. Расскажите, как осуществляется сертификация и аттестация средств защиты информации.
23. Что включают в себя организационно-административные и организационно-технические методы защиты информации?

Раздел 2. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

24. Укажите уровни информационной безопасности.
25. Расскажите, что понимается под законодательным уровнем информационной безопасности?
26. Приведите обзор белорусского и российского законодательств в области информационной безопасности.
27. Приведите примеры международных стандартов и спецификации в области информационной безопасности.
28. Дайте понятие политики безопасности.
29. Приведите примеры основных типов и содержания политик безопасности.

Раздел 3. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

30. Расскажите, что вы знаете о содержании Закона РБ от 6 сентября 1995 г. № 3850-XII «Об информатизации»?
31. Расскажите, что вы знаете о содержании Закона РБ от 29 ноября 1994 г. № 3411-XII «О государственных секретах».
32. Расскажите, что вы знаете о содержании Закона РБ от 3 декабря 1997 г. № 102-З «Об органах государственной безопасности Республики Беларусь».
33. Приведите основное содержание Постановления Совета Министров РБ от 15 февраля 1999 г. № 237 «О служебной информации ограниченного распространения».
34. Приведите основное содержание Постановления Совета Министров РБ от 10 февраля 2000 г. № 186 «О некоторых мерах по защите информации в Республике Беларусь».
35. Что содержится в Указе Президента Республики Беларусь от 12 мая 2004 г. № 231 «Вопросы Государственного центра безопасности информации при Президенте Республики Беларусь»?
36. Приведите основное содержание Указа Президента Республики Беларусь от 14.02.2023 №40 О кибербезопасности.
37. Какую основную задачу призваны решить Указ Президента Республики Беларусь 28 октября 2021 г. № 422 О мерах по совершенствованию защиты персональных данных. и принятый Закон РБ от 7 мая 2021 г. № 99-З О защите персональных данных?
38. Что включает в себя правовая защита от компьютерных преступлений?
39. Перечислите виды компьютерных преступлений. Приведите примеры наиболее известных компьютерных преступлений, принёсших значительный ущерб.
40. Какие существуют виды компьютерных преступлений? Что вам известно о мошенничестве в интернете.
41. Какие специальные программные средства используют мошенники в интернет?
42. Какими правилами следует руководствоваться, чтобы обезопасить себя от мошенничества в интернет?
43. Что вам известно о компьютерных вирусах и антивирусных программах? Приведите наиболее значимые исторические факты о компьютерных вирусах.
44. Дайте понятие вирус. Приведите пример классификации компьютерных вирусов.
45. 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 4. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

46. Что такое технический канал утечки информации. Приведите классификацию технических каналов утечки информации.
47. Дайте понятие речевого сигнала. Какие утечки речевой информации вы знаете? Охарактеризуйте каждый из них.
48. Что вам известно о пассивных и активных методах защиты информации от утечки по техническим каналам?
49. Приведите обзор технических средств негласного съёма акустической информации. Почему возникает необходимость технической защиты информации?
50. Приведите классификацию технических средств съёма акустической информации. Что вам известно о закладочных устройствах?
51. Перечислите технические средства дистанционного съёма информации и технические средства съёма информации с линий связи.
52. Что вам известно о технических средствах защиты речевой информации?
53. Приведите примеры типов технических средств защиты информации. Что вам известно о подавителях записывающих устройств и обнаружителях закамуфлированных камер?
54. Назовите устройства для активной защиты речевой информации от утечки по акустическому и вибрационному каналам.
55. Что такое звуковой сигнал? Приведите пример создания гармонического и полигармонического сигнала. Перечислите основные характеристики гармонического сигнала.
56. Что такое речевой сигнал, в чем заключается особенность энергетического спектра речевого сигнала? С какой основной целью необходимо построение спектров сигналов?
57. 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?
58. Откуда берутся форманты? Дайте определение форманты. Укажите известные вам методы оценки формант?
59. 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?
60. Дайте понятие синтеза смеси гармонического сигнала и гауссово шума с заданным отношением сигнал/шум.
61. Расскажите об особенностях методики и порядка проведения мероприятий по выявлению и исследованию КУИ. Каков порядок проведения аттестации объектов информатизации?
62. Расскажите об особенностях методики и порядка проведения мероприятий по выявлению и исследованию КУИ. Что включают в себя: специальные проверки, специальные обследования, специальные исследования?
63. Приведите пример методики оценки словесной разборчивости речи W.

Раздел 5. ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

64. Что вам известно о стеганографических системах защиты информации?
65. Дайте понятие о стеганографии. В чем заключаются её основные достоинства?

66. Дайте определение компьютерная и цифровая стеганография. Приведите примеры известных вам методов компьютерной стеганографии.
67. Расскажите почему стеганография есть эффективная защита печатной продукции?
68. Расскажите о машиночитаемых технологиях для традиционных способов печати.
69. Что вам известно о разработке новых машиночитаемых защитных признаков. Как осуществляется производственный контроль машиночитаемых защитных признаков?
70. Какие вам известны криптографические методы защиты информации?
71. Дайте основные понятия: криптология, криптография, криптоанализ.
72. Дайте понятия код, шифр и ключ: открытый и закрытый.
73. Приведите основную схему криптографии.
74. Дайте понятие электронного документа и электронной цифровой подписи
75. Придание юридического статуса электронным документам. Юридическая сила оригинала и копии электронного документа.
76. Какие существуют угрозы цифровой подписи. RSA как фундамент электронной цифровой подписи.
77. Приведите примеры уникальной и точной идентификации продуктов и банковских счетов.
78. Особенности использования стандартизированных кодов банков, супермаркетов и других крупных подсистем экономики – кредитные карты. Алгоритм Луна. Понятие и разновидности шрихкодов.
79. Приведите примеры возможных атак автоматизированной банковской системы. Возможные атаки на уровне сети.
80. Какие существуют меры защиты от атак на сетевом уровне.
81. Перечислите основные правила организации защиты АСБ.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Освоение учебной дисциплины «Основы безопасности информационных систем» предполагает следующие формы самостоятельной работы студентов:

– изучение печатных источников по теме дисциплины;

– изучение профессиональных электронных ресурсов по теме дисциплины;

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

– выполнение практических упражнений для закрепления знаний и навыков;

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

–решение индивидуальных задач при подготовке к практическим занятиям;

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

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

–систематизация полученных знаний при подготовке к зачёту.

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.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов дневной формы получения высшего образования

Материалы, размещённые на бесплатном сервисе для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google Класс Room университета: шифр курса **BSJG677Z.**

Методические указания к выполнению практических работ по дисциплине по дисциплине «Основы безопасности информационных систем» для студентов всех специальностей.

Содержание самостоятельной работы студентов
(дневная форма получения высшего образования)

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Углублённое изучение отдельных тем для подготовки к контрольному тестированию	*Тема 1.4 Угрозы информационной безопасности.* Осн. литература: [5], [7]. Доп. литература: [7], [10], [18], [22].	4
	Тема 2.1 Правовое обеспечение защиты информации. Осн. литература:[5], [7]. Доп. литература: [7], [18], [23]. Нормативная: [15], [16], [17], [18], [19], [20], [21], [22], [23].	4
	Тема 2.4 Компьютерные вирусы и антивирусные программы. Осн. литература: [4], [5]. Доп. литература: [9], [16], [21], [18], [23].	4
	Тема 4.2 Звуковые сигналы. Осн. литература:[4], [5]. Доп. литература.: [9], [13], [16], [21], [18], [23], [29], [30], [31].	4
	Тема 5.2 Криптографические методы защиты информации. Осн. литература: [5]. Доп. литература: [33], [25], [27], [28].	4
	Тема 5.3 Уникальная и точная идентификация продуктов и банковских счетов. Доп. литература: [7], [9].	4
	Тема 5.5 Основы защиты автоматизированных систем от несанкционированного доступа. Осн. литература: [5], [7]. Доп. литература: [6], [8], [12], [18], [19], [20], [25], [28], [33].	4
Подготовка к защите отчётов по практическим работам	**Практическая работа №1** Изучение Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (утверждён Постановлением Совета Министров Республики Беларусь 15.05.2013 № 375).	4
	Практическая работа №2 Организация защиты баз данных в СУБД Microsoft ACCESS. Использование пароля для шифрования базы данных в СУБД Microsoft Access.	4
	Практическая работа №3 Организация защиты баз данных в СУБД Microsoft ACCESS. Работа с Центром управления безопасностью. Организация защиты базы данных в СУБД Microsoft ACCESS.	6
	Практическая работа №4 Правовое обеспечение информационной безопасности. Выявление и фиксация следов противоправной деятельности на ПЭВМ.	4
	Практическая работа №5 Оценка первичных признаков элементов речевого сигнала.	4
	Практическая работа № 6. Создание маскирующего шума для имитации виброакустического зашумления.	4
	Практическая работа №7 Изучение методов защиты информации с помощью различных видов шифров, используемых в криптографии.	4
	Практическая работа №8 Штриховое кодирование информации. Анализ реальных штрих-кодов.	4
	ВСЕГО:	**62**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Диагностика качества усвоения знаний проводится в форме текущего контроля и промежуточной аттестации.

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

–устная форма (блиц-опрос на лекциях);

–письменная форма (тесты, письменные отчёты по практическим работам);

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

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

Практикум предполагает выполнение и защиту практических работ. По каждой практической работе выдается индивидуальное задание. Отчет по практической работе представляется в электронном виде. Содержание отчета: 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:

$$Т = \frac{(КТ_1 + ... + КТ_6) + (ПР_1 + ... + ПР_8)}{14}$$

где $КТ_1 + ... + КТ_6$ – отметки, выставленные по результатам контрольного тестирования;
$ПР_1 + ... + ПР_8$ – отметки, выставленные по результатам защиты практических работ.

Результат текущего контроля рассчитывается как округлённое среднее значение.

Для обучающего, пропустившего мероприятие текущего контроля по уважительной причине, кафедрой устанавливаются дополнительные сроки.

Обучающемуся, пропустившему мероприятие текущего контроля без уважительной причины, выставляется 1 (один) балл за данное мероприятие.

Результат текущего контроля может быть повышен:

- за участие обучающего в научно-практических мероприятиях, учебно-исследовательской, научно-исследовательской работе студентов (конференциях, семинарах, олимпиадах, конкурсах, научных кружках и т.п.) по профилю учебной дисциплины (модуля) и может быть повышен до 10 баллов при достижении значимых результатов в этой работе;

- обучающийся в целях повышения отметки по любому мероприятию текущего контроля может воспользоваться правом на дополнительные образовательные услуги (платные консультации, платные дополнительные занятия). Количество и сроки пересдач с целью повышения отметки определяет кафедра.

Промежуточная аттестация проводится в форме зачёта.

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

$$З = k \cdot Т,$$

где k– весовой коэффициент текущего контроля;

Т – результат текущего контроля за семестр.

Весовой коэффициент k принимается равным 1.

Отметка «зачтено» выставляется в случае, если отметка по результатам текущего контроля не ниже 4 (четырех) баллов.

Если, по результатам текущего контроля отметка ниже 4 (четырех) баллов, то проводится устный опрос по вопросам.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

- проблемное обучение (проблемное изложение, вариативное изложение), реализуемое на лекционных занятиях;
- учебно-исследовательская деятельность, реализация творческого подхода, реализуемые на практических занятиях.

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

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

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