Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный университет
имени Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«30» 06 2023 г.
Регистрационный №УД-407/23/уч

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

2023 г.

Учебная программа составлена на основе типовой учебной программы для высших учебных заведений по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)», регистрационный № ТД-Р.633/тип. от 03.05.2016, образовательного стандарта по специальности высшего образования ОСВО 1-98 01 01-2021 и учебного плана специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)». Регистрационный №21-21/уч. ФКНиЭ от 26.07.2021 г. для очной дневной формы получения высшего образования.

СОСТАВИТЕЛЬ:
Ирина Брониславовна Бураченок, к.т.н., доцент, доцент 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 № 6 от «30» 05 2023 г.).

Методической комиссией факультета компьютерных наук и электроники учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 10 от «22» 06 2023 г.).

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 6 от «30» 06 2023 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Теоретические основы информационной безопасности» ориентирована на обучение студентов базовым знаниям, умениям и навыкам в области защиты информации и ориентирована на подготовку специалиста, умеющего создавать защищенные информационные системы и исследовать защищенность компьютерно-коммуникационных систем. Изучаемые темы представляются на основе современной нормативной регулятивной базы и национального законодательства.

Целью изучения дисциплины «Теоретические основы информационной безопасности» является формирование у студентов базовых знаний в области информационной безопасности, обучение основам построения и особенностям использования современных защищенных информационных компьютерно-коммуникационных систем.

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

Задачи изучения дисциплины «Теоретические основы информационной безопасности». При изучении данной дисциплины требуется разрешить основные задачи:

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

– 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.

В результате изучения дисциплины «Теоретические основы информационной безопасности» обучаемый должен:

знать:

– основные проблемы обеспечения защищенности информации в информационно-коммуникационных системах;

– современные методы исследования и научно-технические решения по обеспечению защиты информации в корпоративных компьютерно-коммуникационных системах;

– математические и инженерные основы построения и функционирования защищенных компьютерно-коммуникационных систем и средств защиты, эффективные методы анализа их защищенности;

уметь:

– проводить исследования проблем информационной безопасности с использованием современных методов;

– применять современные методы и технологии для создания и оценки защищенных систем;

владеть:

– основными подходами к анализу задач информационной безопасности.

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

универсальные компетенции:

УК-1 Владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации;

УК-2 Решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий;

базовые профессиональные компетенции:

БПК-5 Использовать основные понятия и нормативные правовые акты информационной безопасности для описания и классификации теоретических, правовых,

организационных и инженерно-технических методов обеспечения конфиденциальности, целостности и доступности информации.

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

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

Основой для изучения учебной дисциплины «Теоретические основы информационной безопасности» по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» является предмет «Информатика», изучаемый при получении общего базового и общего среднего образования, а также необходимы знания, полученные при изучении базовых дисциплин по специальности государственного компонента «Основы и методологии программирования», «Алгоритмы и структуры данных», «Операционные системы» и дисциплин компонента учреждения высшего образования «Арифметические и алгебраические основы криптографии».

Перечень дисциплин, которые изучаются на базе дисциплины.

Знания, полученные при изучении дисциплины «Теоретические основы информационной безопасности», непосредственно связаны с учебными дисциплинами: «Программно-аппаратные и технические средства защиты информации», «Методы и стандарты оценки защищенности компьютерных систем», «Криптографические протоколы», необходимы также при изучении ряда дисциплин специализации: «Защита информации в операционных системах и компьютерных сетях», «Компьютерная защита финансовой информации», а также другими дисциплинами, предусмотренными учебным планом по специальности. Изучение учебной дисциплины позволяет дать студентам базу, необходимую для успешного усвоения материала перечисленных выше учебных дисциплин, а также получить знания, необходимые им в дальнейшем для успешной работы.

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

Форма получения высшего образования первой ступени	дневная
Курс (курсы)	3
Семестр	5
Всего часов по дисциплине	216
Всего аудиторных часов по дисциплине	72
В том числе:	
Лекции, часов	36
Практические занятия, часов	36
Самостоятельная работа, часов	144
Форма промежуточной аттестации	зачет, экзамен
Трудоёмкость дисциплины, з.е.	6

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

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

Раздел 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 1.1 Основы информационной грамоты.

Понятие информационной безопасности. Информационное общество. Безопасность в информационном обществе. Информационная безопасность и ее составляющие. Место информационной безопасности в системе национальной безопасности. Основные формы проявления информации. Характеристики информации. Общая схема процесса обеспечения безопасности. Информационная безопасность и защита информации. Термины и определения. Система показателей, характеризующих информацию. Качество информации и его обеспечение.

Тема 1.2 Информационное обеспечение деятельности.

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.

Тема 1.3. История развития технологий и современная парадигма обеспечения информационной безопасности.

Исторические события факты и персоналии. Возникновение и история развития проблемы защиты информации. Структура теории компьютерной безопасности. Методологические основы защиты информации. Суть системно-концептуального подхода. Парадигма информационной безопасности.

Раздел 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 2.1. 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. Причины, виды и каналы утечки информации.

Тема 2.2. Информационная война как угроза национальной безопасности.

Понятие информационной войны и ее особенности. Информационное оружие. Информационные правоотношения.

Тема 2.3. Уязвимости информации и информационных систем.

Уязвимость информации и информационных систем. Система показателей уязвимости. Методы и модели оценки уязвимостей.

Тема 2.4. Основные характеристики безопасности и способы их обеспечения. Модели защиты информации.

Доступность, целостность и подлинность, конфиденциальность информации и информационных ресурсов. Методы и способы их защиты: правовые, организационно-административные, программно-технические. Модели защиты информации. Модель Харрисона-Рузо-Ульмана. Модель Белла-ЛаПадулы. Ролевая модель безопасности. Структура профиля защиты. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISI/IEC 15408.

Раздел 3. ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 3.1. Технологии защиты информации, информационных ресурсов, информационных систем.

Управление жизненным циклом информационных систем. Технологии обеспечения доступности, целостности и подлинности, конфиденциальности информации, информационных ресурсов и информационных систем.

Тема 3.2. Методы исследования проблем защиты информации.

Общая характеристика методов исследования и проблем защиты информации. Основные положения теории нечетких множеств. Основные положения нестрогой математики. Неформальные методы оценивания. Неформальные методы поиска оптимальных решений.

Тема 3.3. Методология оценки защищенности.

Оценка защищенности средств информатизации и ИТ-систем. Общие критерии оценки защищенности. Функциональные и гарантийные требования.

Тема 3.4. Принципы построения систем защиты информации.

Системы защиты информации. Общеметодологические принципы построения систем защиты информации. Основы архитектурного построения. Модели систем и процессов защиты информации. Модели разграничения доступа к информации. Общее содержание основных вопросов организации и обеспечения работ по защите информации. Структура и функции органов защиты информации.

Тема 3.5. Методики построения систем защиты информации.

Модель Lifecycle Security. Модель многоуровневой защиты. Методика управления рисками, предлагаемая Microsoft.

Тема 3.6. Методики и программные продукты для оценки рисков.

Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Проведение оценки рисков в соответствии с методикой Microsoft.

Раздел 4. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 4.1. 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 4.2. Политика информационной безопасности.

Понятие политики безопасности. Основные типы и содержание политик безопасности. Принципы государственной политики обеспечения информационной безопасности. Система защиты государственной тайны.

Тема 4.3. Менеджмент информационной безопасности.

Системы менеджмента безопасности информации. Правила и требования. Управление информационной безопасностью. Управление рисками. Аудит информационной безопасности.

Стандарты ISO/IEC 17799/27002 и 27001.

Учебно-методическая карта учебной дисциплины «Теоретические основы информационной безопасности»
Дневная форма получения высшего образования

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
1	**Лекция № 1** *Введение в дисциплину* Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [17], [19].	
	Раздел 1 Теоретические основы информационной безопасности	**6**		**8**			
2	**Лекция № 2** *Тема 1.1 Основы информационной грамоты.* Понятие информационной безопасности. Информационное общество. Безопасность в информационном обществе. Информационная безопасность и ее составляющие. Место информационной безопасности в системе национальной безопасности. Основные формы проявления информации. Характеристики информации. Общая схема процесса обеспечения безопасности. Информационная безопасность и защита информации. Термины и определения. Система показателей, характеризующих информацию. Качество информации и его обеспечение.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [3], [4], [6], [7], [8], [9], [14].	Блиц-опрос

1	2	3	4	5	6	7	8
3	**Практическая работа №1** Изучение Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) (утверждён Постановлением Совета Министров Республики Беларусь 15.05.2013 № 375).			2		Методические указания	Защита отчета по практической работе № 1
4	**Лекция № 3** *Тема 1.2 Информационное обеспечение деятельности.* 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.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [17], [19].	Блиц-опрос
5	**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.			2		Методические указания	Защита отчета по практической работе № 2
6	**Лекция № 4** *Тема 1.3. История развития технологий и современная парадигма обеспечения информационной безопасности.* Исторические события факты и персоналии. Возникновение и история развития проблемы защиты информации. Структура теории компьютерной безопасности. Методологические основы защиты информации. Суть системно-концептуального подхода. Парадигма информационной безопасности.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [17], [19].	*Контрольное тестирование №1
7	**Практическая работа №3** 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 № 3

1	2	3	4	5	6	7	8
	Раздел 2 Угрозы информационной безопасности. Уровни информационной безопасности	**8**		**8**			
8	**Лекция № 5** *Тема 2.1. 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. Причины, виды и каналы утечки информации.	2				Осн. лит.: [1], [2], [3], [5], [7]. Доп. лит.: [1], [6], [15], [17], [19].	Блиц-опрос
9	**Практическая работа №4** 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 № 4
10	**Лекция № 6** *Тема 2.2. Информационная война как угроза национальной безопасности.* Понятие информационной войны и ее особенности. Информационное оружие. Информационные правоотношения.	2				Осн. лит.: [1], [2], [3], [4], [5], [7]. Доп. лит.: [1], [6], [15], [17], [19].	***Контрольная работа №1**
11	**Практическая работа №5** Правовое обеспечение информационной безопасности. Выявление и фиксация следов противоправной деятельности на ПЭВМ.			2		Методические указания	Защита отчета по практической работе № 5
12	**Лекция №7** *Тема 2.3. Уязвимости информации и информационных систем.* Уязвимость информации и информационных систем. Система показателей уязвимости. Методы и модели оценки уязвимостей.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [17], [19].	Блиц-опрос

1	2	3	4	5	6	7	8
13	**Практическая работа №6** Изучение международных стандартов, определяющих требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.			2		Методические указания	Защита отчета по практической работе № 6
14	**Лекция №8** *Тема 2.4. Основные характеристики безопасности и способы их обеспечения. Модели защиты информации.* Доступность, целостность и подлинность, конфиденциальность информации и информационных ресурсов. Методы и способы их защиты: правовые, организационно-административные, программно-технические. Модели защиты информации. Модель Харрисона-Рузо-Ульмана. Модель Белла-ЛаПадулы. Ролевая модель безопасности. Структура профиля защиты. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISI/IEC 15408.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [17], [19].	Блиц-опрос
15	**Практическая работа №7** Использование программной систем PGP и TrueCrypt для обеспечения конфиденциальности и целостности информационных ресурсов.			2		Методические указания	Защита отчета по практической работе № 7
	Раздел 3 Построение систем защиты информации	**12**		**12**			
16	**Лекция №9** *Тема 3.1. Технологии защиты информации, информационных ресурсов, информационных систем.* Управление жизненным циклом информационных систем. Технологии обеспечения доступности, целостности и подлинности, конфиденциальности информации, информационных ресурсов и информационных систем.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [11], [19].	Блиц-опрос
17	**Практическая работа №8** Получение практических навыков программного восстановления данных при помощи программы TestDisk.			2		Методические указания	Защита отчета по практической работе № 8

1	2	3	4	5	6	7	8
18	**Лекция №10** *Тема 3.2. Методы исследования проблем защиты информации.* Общая характеристика методов исследования и проблем защиты информации. Основные положения теории нечетких множеств. Основные положения нестрогой математики. Неформальные методы оценивания. Неформальные методы поиска оптимальных решений.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [11], [17], [19].	Блиц-опрос
19	**Практическая работа №9** Создание и удаление учетной записи пользователя, групп пользователей. Управления и групповой политикой.			2		Методические указания	Защита отчета по практической работе № 9
20	**Лекция № 11** *Тема 3.3. Методология оценки защищенности.* Оценка защищенности средств информатизации и ИТ-систем. Общие критерии оценки защищенности. Функциональные и гарантийные требования.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [17], [19].	Блиц-опрос
21	**Практическая работа №10** Реализация политики безопасности в защищенных версиях операционной системы Windows.			2		Методические указания	Защита отчета по практической работе № 10
22	**Лекция № 12** *Тема 3.4. Принципы построения систем защиты информации.* Системы защиты информации. Общеметодологические принципы построения систем защиты информации. Основы архитектурного построения. Модели систем и процессов защиты информации. Модели разграничения доступа к информации. Общее содержание основных вопросов организации и обеспечения работ по защите информации. Структура и функции органов защиты информации.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [16], [17], [19].	*Контрольное тестирование №2
23	**Практическая работа №11** Разграничение прав пользователей в защищенных версиях операционной системы Windows. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.			2		Методические указания	Защита отчета по практической работе № 11

1	2	3	4	5	6	7	8
24	**Лекция № 13** *Тема 3.5. Методики построения систем защиты информации.* Модель Lifecycle Security. Модель многоуровневой защиты. Методика управления рисками, предлагаемая Microsoft.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [2], [6], [15], [17], [19].	Блиц-опрос
25	**Практическая работа №12** Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности, при использовании глобальных вычислительных сетей.			2		Методические указания	Защита отчета по практической работе № 12
26	**Лекция № 14** *Тема 3.6. Методики и программные продукты для оценки рисков.* Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Проведение оценки рисков в соответствии с методикой Microsoft.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [5], [15], [17], [18], [19].	*Контрольное тестирование №3
27	**Практическая работа №13** Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.			2		Методические указания	Защита отчета по практической работе № 13
	Раздел 4 Политика информационной безопасности	**8**		**8**			
28	**Лекция № 15** *Тема 4.1. 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.	2				Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [15], [16], [20-31], [32], [34-40].	Блиц-опрос
29	**Практическая работа №14** Практические навыки работы сканирования сети с помощью Honeypot, Nmap.			2		Методические указания	Защита отчета по практической работе № 14

1	2	3	4	5	6	7	8
30	**Лекция № 16** *Тема 4.1. Уровни информационной безопасности.* 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]. Доп. лит.: [15], [16], [20-31], [32], [34-40].	Блиц-опрос
31	**Практическая работа №15** Изучение антивирусных программ.			2		Методические указания	Защита отчета по практической работе № 15
32	**Лекция № 17** *Тема 4.2. Политика информационной безопасности.* Понятие политики безопасности. Основные типы и содержание политик безопасности. Принципы государственной политики обеспечения информационной безопасности. Система защиты государственной тайны.	2				Осн. лит.: [1], [2], [3], [4], [6]. Доп. лит.: [13], [15], [32], [34], [35], [36].	***Контрольная работа №2***
33	**Практическая работа №16** Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.			2		Методические указания	Защита отчета по практической работе № 16
34	**Лекция № 18** *Тема 4.3. Менеджмент информационной безопасности.* 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.: [1], [2], [3], [4], [6]. Доп. лит.: [12], [13], [16], [17], [24-31].	*Контрольное тестирование №4

1	2	3	4	5	6	7	8
35	**Практическая работа №17** Работа с SIEM (Security information and event management): SIM – Security Information Management – управление информационной безопасностью SEM – Security Event Management – управление событиями безопасности.			2		Методические указания	Защита отчета по практической работе № 17
36	**Практическая работа №18** Защита с помощью систем обнаружения и предотвращения вторжений при помощи NIPS/NIDS: Snort.			2		Методические указания	Защита отчета по практической работе № 18
	Всего (36 часов)	**36**		**36**			

*** МЕРОПРИЯТИЯ ТЕКУЩЕГО КОНТРОЛЯ**

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729 (дата обращения: 20.07.2021). – Библиогр. в кн. – ISBN 978-5-7782-3640-0. – Текст : электронный.

2. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=362895 (дата обращения: 20.07.2021). – Библиогр. в кн. – ISBN 978-5-4475-3947-4. – DOI 10.23681/362895. – Текст : электронный.

3. Нестеров, С. А. Основы информационной безопасности : учебное пособие : [16+] / С. А. Нестеров ; Санкт-Петербургский государственный политехнический университет. – Санкт-Петербург : Издательство Политехнического университета, 2014. – 322 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 20.07.2021). – ISBN 978-5-7422-4331-1. – Текст : электронный.

4. 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.

5. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник : [16+] / Б. И. Филиппов, О. Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 240 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499170 (дата обращения: 20.07.2021). – Библиогр.: с. 221-226. – ISBN 978-5-4475-9823-5. – DOI 10.23681/499170. – Текст : электронный.

6. 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».

7. 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.

Дополнительная:

1. Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В. И. Аверченков ; В.И. Аверченков. – 3-е изд., стер. – Москва: Издательство «Флинта», 2016. – 269 с. – Режим доступа: по подписке: URL: http://biblioclub.ru/index.php?page=book&id=93245.

Гурьева Е. В

2. 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.

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

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

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

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

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

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

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

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

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

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

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

14. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. – 5-е изд., стер. – Санкт-Петербург : Лань, 2019. – 324 с. – ISBN 978-5-8114-4067-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/114688 (дата обращения: 19.08.2022). – Режим доступа: для авториз. пользователей.

15. 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.

16. 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.

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

18. 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.

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

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

21. 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.

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

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

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

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

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

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

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

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

30. 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.

31. 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.

32. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

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

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

35. 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.

36. 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.

37. Закон Республики Беларусь «О защите персональных данных» №99-З от 07.05.2021.

38. Закон Республики Беларусь «О коммерческой тайне» № 16-З от 05.01.2013.

39. Закон Республики Беларусь «Об информатизации» №3850-XII от 6.09.1995.

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

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

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 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: 19.03.2019.

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.

ПЕРЕЧЕНЬ 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 Изучение Закона Республики Беларусь 19 июля 2010 г. №170-З «О Государственных Секретах». Государственное регулирование и управление в области информации, информатизации и защиты информации.

Практическая работа №3 Изучение Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».

Практическая работа №4 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 №5 Правовое обеспечение информационной безопасности. Выявление и фиксация следов противоправной деятельности на ПЭВМ.

Практическая работа №6 Изучение международных стандартов, определяющих требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

Практическая работа №7 Использование программной систем PGP и TrueCrypt для обеспечения конфиденциальности и целостности информационных ресурсов.

Практическая работа №8 Получение практических навыков программного восстановления данных при помощи программы TestDisk.

Практическая работа №9 Создание и удаление учетной записи пользователя, групп пользователей. Управления и групповой политикой.

Практическая работа №10 Реализация политики безопасности в защищенных версиях операционной системы Windows.

Практическая работа №11 Разграничение прав пользователей в защищенных версиях операционной системы Windows. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.

Практическая работа №12 Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности, при использовании глобальных вычислительных сетей.

Практическая работа №13 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.

Практическая работа №14 Практические навыки работы сканирования сети с помощью Honeypot, Nmap.

Практическая работа №15 Изучение антивирусных программ.

Практическая работа №16 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.

Практическая работа №17 Работа с SIEM (Security information and event management): SIM – Security Information Management – управление информационной безопасностью SEM – Security Event Management – управление событиями безопасности.

Практическая работа №18 Защита с помощью систем обнаружения и предотвращения вторжений при помощи NIPS/NIDS: Snort.

ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

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. Что необходимо знать при использовании паролей.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

1. Цели и задачи изучения дисциплины. Основные понятия и определения.
2. Основные понятия информационной безопасности.
3. Информационные технологии и необходимость ИБ.
4. Система защиты информации и ее структуры.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).
12. Действия и события, нарушающие информационную безопасность.
13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
14. Способы воздействия информационных угроз на объекты.
15. Внешние и внутренние субъекты информационных угроз.
16. Компьютерные преступления и их классификация.
17. Исторические аспекты компьютерных преступлений и современность.
18. Субъекты и причины совершения компьютерных преступлений.
19. Вредоносные программы, их виды.
20. История компьютерных вирусов и современность.
21. Деятельность международных организаций в сфере информационной безопасности.
22. Государственное регулирование информационной безопасности в Республике Беларусь.
23. Задачи ИБ в программе «цифровая экономика».
24. Доктрина информационной безопасности в Республике Беларусь.
25. Законы в сфере информатизации и информационной безопасности в Республике Беларусь.
26. Уголовно-правовой контроль над компьютерной преступностью в Республике Беларусь.
27. Политика безопасности и ее принципы.
28. Фрагментарный и системный подход к защите информации.
29. Методы и средства защиты информации.
30. Организационное обеспечение ИБ.
31. Организация конфиденциального делопроизводства.
32. Организационно-экономическое обеспечение ИБ.
33. Инженерно-техническое обеспечение компьютерной безопасности.
34. Организационно-правовой статус службы безопасности.
35. Защита информации в Интернете.
36. Электронная почта и ее защита.
37. Защита от компьютерных вирусов.
38. «Больные» мобильники и их «лечение».
39. Популярные антивирусные программы и их классификация.
40. Этапы и освоение защиты информации экономических объектов.
41. Криптографические методы защиты информации.
42. Оценка эффективности инвестиций в информационную безопасность.
43. Фирмы, оценивающие работу персонала в компании.
44. Менеджмент и аудит ИБ на уровне предприятия.
45. Аудит ИБ автоматизированных банковских систем.
46. Аудит ИБ электронной коммерции.
47. Информационная безопасность предпринимательской деятельности.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЭКЗАМЕНА

1. Назовите отличительные черты информационного общества.
2. В чем заключается проблема информационной безопасности?
3. Дайте определение понятию «информационная безопасность».
4. Что понимается под «компьютерной безопасностью»?
5. Аспекты информационной безопасности.
6. Цели и задачи, решение которых должна обеспечивает информационная безопасность.
7. Важность и сложность проблемы информационной безопасности.
8. Дайте понятие информации.
9. Кто относится к потребителям и обладателям информации.
10. Перечислите составляющие информационной безопасности.
11. Приведите определение доступности информации.
12. Приведите определение целостности информации.
13. Приведите определение конфиденциальности информации.
14. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
15. Перечислите классы угроз информационной безопасности.
16. Назовите причины и источники случайных воздействий на информационные системы.
17. Дайте характеристику преднамеренным угрозам.
18. Перечислите каналы несанкционированного доступа.
19. Перечислите задачи информационной безопасности общества.
20. Перечислите уровни формирования режима информационной безопасности.
21. Дайте краткую характеристику законодательно-правового уровня.
22. Какие подуровни включает программно-технический уровень?
23. Что включает административный уровень?
24. В чем особенность морально-этического подуровня?
25. Перечислите основополагающие документы по информационной безопасности.
26. Понятие государственной тайны.
27. Что понимается под средствами защиты государственной тайны?
28. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РБ.
29. Какие категории государственных информационных ресурсов определены в Законе «Об информации, информатизации и защите информации»?
30. Какая ответственность в Уголовном кодексе РБ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
31. Цели и задачи административного уровня обеспечения информационной безопасности.
32. Содержание административного уровня.
33. Дайте определение политики безопасности.
34. Направления разработки политики безопасности.
35. Перечислите составные элементы автоматизированных систем.
36. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.
37. Сколько классов защищенности СВТ от НСД к информации устанавливает РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?
38. Дайте характеристику уровням защиты СВТ от НСД к информации по РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?
39. Классы защищенности АС от НСД по РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации».
40. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
41. Показатели защищенности межсетевых экранов.
42. Классы защищенности межсетевых экранов.
43. Перечислите виды «вирусоподобных» программ.

44. Поясните механизм функционирования «троянской программы» (логической бомбы).
45. В чем заключаются деструктивные свойства логических бомб?
46. Как используются утилиты скрытого администрирования и их деструктивные возможности?
47. Охарактеризуйте «intended»-вирусы и причины их появления.
48. Для чего используются конструкторы вирусов?
49. Как обнаружить загрузочный вирус?
50. Как обнаружить резидентный вирус?
51. Характерные черты макровируса.
52. Как проверить систему на наличие макровируса?
53. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?
54. Перечислите основные этапы алгоритма обнаружения вируса.
55. Как рассматривается сеть в концепции протокола IP?
56. Что такое IP-адрес?
57. Преобразуйте IP-адрес «11110011 10100101 00001110 11000001» в десятичную форму.
58. Сколько классов сетей определяет IP протокол?
59. Из каких частей состоит IP-адрес?
60. К какому классу относится следующий адрес: 199.226.33.168?
61. Какой из этих адресов не может существовать: 109.256.33.18 или 111.223.44.1?
62. Поясните понятие домена.
63. В чем заключается иерархический принцип системы доменных имен?
64. Для чего предназначен DNS-сервер?
65. Приведите примеры доменов верхнего уровня по географическому признаку.
66. Дайте определение типовой удаленной атаки.
67. Механизм реализации удаленной атаки «анализ сетевого трафика».
68. Что является целью злоумышленников при «анализе сетевого трафика»?
69. Назовите причины успеха удаленной атаки «ложный объект».
70. Охарактеризуйте удаленную атаку «подмена доверенного объекта» по классам угроз.
71. Поясните возможные механизмы реализации удаленной атаки «отказ в обслуживании».
72. Какие составляющие «информационной безопасности» могут быть нарушены при реализации каждой из типовых удаленных атак?
73. Перечислите основные причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях.
74. Почему виртуальное соединение не обеспечивает требуемого уровня защиты вычислительных сетей?
75. Какая из причин приводит к успеху удаленной угрозы «анализ сетевого трафика»?
76. Что является следствием недостаточной аутентификации субъектов и объектов вычислительных сетей?
77. К чему приводит недостаточность информации об объектах вычислительной сети? Приведите пример.
78. Может ли быть нарушена целостность информации при отсутствии в распределенных вычислительных сетях возможности контроля за маршрутом сообщений? Почему?
79. В чем заключаются преимущества сети с выделенными каналами?
80. Какие алгоритмы удаленного поиска Вам известны?
81. Какой из алгоритмов поиска более безопасный?
82. Как повысить защищенность вычислительных сетей при установлении виртуального соединения?
83. Как можно защитить сеть от реализации атаки «отказ в обслуживании»?
84. Как можно контролировать маршрут сообщения в сети?
85. Что понимается под идентификацией пользователя?
86. Что понимается под аутентификацией пользователей?
87. Применим ли механизм идентификации к процессам? Почему?
88. Перечислите возможные идентификаторы при реализации механизма идентификации.
89. Перечислите возможные идентификаторы при реализации механизма аутентификации.

90. Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
91. В чем особенности динамической аутентификации?
92. Опишите механизм аутентификации пользователя.
93. Что такое «электронный ключ»?
94. Перечислите виды аутентификации по уровню информационной безопасности.
95. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?
96. Что входит в состав криптосистемы?
97. Какие составляющие информационной безопасности могут обеспечить криптосистемы?
98. Назовите классификационные признаки методов шифрования данных.
99. Поясните механизм шифрования «на лету».
100. Как реализуется симметричный метод шифрования?
101. Как реализуется асимметричный метод шифрования?
102. Что понимается под ключом криптосистемы?
103. Какие методы шифрования используются в вычислительных сетях?
104. Что такое электронная цифровая подпись?
105. Какой метод шифрования используется в электронной цифровой подписи?
106. Чем определяется надежность криптосистемы?
107. Перечислите известные методы разграничения доступа.
108. В чем заключается разграничение доступа по спискам?
109. Как используется матрица разграничения доступа?
110. Опишите механизм разграничения доступа по уровням секретности и категориям.
111. Какие методы управления доступа предусмотрены в руководящих документах Гостехкомиссии?
112. Поясните механизм дискретного управления доступом?
113. Сравните дискретное и мандатное управление доступом.
114. На чем основан механизм регистрации?
115. Какие события, связанные с безопасностью, подлежат регистрации?
116. Чем отличаются механизмы регистрации и аудита?
117. Дайте определение аудита событий информационной системы.
118. Что относится к средствам регистрации и аудита?
119. Что такое регистрационный журнал? Его форма.
120. Что понимается под подозрительной активностью?
121. Какие этапы предусматривают механизмы регистрации и аудита?
122. Охарактеризуйте известные методы аудита безопасности информационных систем.
123. В чем заключается механизм межсетевого экранирования?
124. Дайте определение межсетевого экрана.
125. Принцип функционирования межсетевых экранов с фильтрацией пакетов.
126. На уровне каких протоколов работает шлюз сеансового уровня?
127. В чем особенность межсетевых экранов экспертного уровня?
128. Какие сервисы безопасности включает технология виртуальных частных сетей?
129. Назовите функции VPN-агента.
130. Каким образом технология VPN обеспечивает конфиденциальность данных?
131. Каким образом технология VPN обеспечивает целостность данных?
132. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?
133. Что такое «туннель» и технология его создания?
134. Чем определяется политика безопасности виртуальной частной сети?

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Теоретические основы информационной безопасности» 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 письменным контрольным работам;

–систематизация полученных знаний при подготовке к зачету;

–систематизация полученных знаний при подготовке к экзамену.

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;

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

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

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещённые в бизнес-мессенджере для групповой работы и общения Microsoft Teams: шифр курса **R2DRILQ**.

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 2.1. Угрозы информационной безопасности.* Система дестабилизирующих факторов, влияющих на уязвимость информации. Методология формирования полного множества угроз. Осн. лит.: [1], [2], [3], [4], [7]. Доп. лит.: [1], [6], [15], [17], [19].	4
	Тема 2.2. Информационная война как угроза национальной безопасности. Понятие информационной войны и ее особенности. Информационное оружие. Информационные правоотношения. Осн. лит.: [1], [2], [3], [4], [7]. Доп. лит.: [1], [6], [15], [17], [19].	4
	Тема 2.3. Уязвимости информации и информационных систем. Уязвимость информации и информационных систем. Система показателей уязвимости. Методы и модели оценки уязвимостей. Осн. лит.: [1], [2], [3], [4]. Доп. лит.: [1], [6], [15], [17], [19].	4
	Тема 2.4. Основные характеристики безопасности и способы их обеспечения. Модели защиты информации. Модели защиты информации. Модель Харрисона-Рузо-Ульмана. Модель Белла-ЛаПадулы. Ролевая модель безопасности. Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [15], [17], [19].	4
	Тема 3.2. Методы исследования проблем защиты информации. Основные положения теории нечетких множеств. Основные положения нестрогой математики. Осн. лит.: [1], [2], [3], [5]. Доп. лит.: [1], [6], [11], [17], [19].	4
	Тема 3.5. Методики построения систем защиты информации. Модель Lifecycle Security. Модель многоуровневой защиты. Методика управления рисками, предлагаемая Microsoft. Осн. лит.: [1], [2], [3], [4]. Доп. лит.: [2], [6], [15], [17], [19].	4
	Тема 3.6. Методики и программные продукты для оценки рисков. Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Проведение оценки рисков в соответствии с методикой Microsoft. Осн. лит.: [1], [2], [3], [4]. Доп. лит.: [5], [15], [17], [18], [19].	4
	Тема 4.2. Политика информационной безопасности. Понятие политики безопасности. Основные типы и содержание политик безопасности. Принципы государственной политики обеспечения информационной безопасности. Система защиты государственной тайны. Осн. лит.: [1], [2], [3], [4], [6]. Доп. лит.: [13], [15], [32], [34], [35], [36].	4

1	2	3
Подготовка к защите отчетов по практическим работам	*Практическая работа №1* Изучение Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY (утверждён Постановлением Совета Министров Республики Беларусь 15.05.2013 № 375)).	2
	Практическая работа №2 Изучение Закона Республики Беларусь 19 июля 2010 г. №170-З «О Государственных Секретах». Государственное регулирование и управление в области информации, информатизации и защиты информации.	2
	Практическая работа №3 Изучение Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации».	2
	Практическая работа №4 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
	Практическая работа №5 Правовое обеспечение информационной безопасности. Выявление и фиксация следов противоправной деятельности на ПЭВМ.	2
	Практическая работа №6 Изучение международных стандартов, определяющих требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.	2
	Практическая работа №7 Использование программной систем PGP и TrueCrypt для обеспечения конфиденциальности и целостности информационных ресурсов.	2
	Практическая работа №8 Получение практических навыков программного восстановления данных при помощи программы TestDisk.	2
	Практическая работа №9 Создание и удаление учетной записи пользователя, групп пользователей. Управления и групповой политикой.	2
	Практическая работа №10 Реализация политики безопасности в защищенных версиях операционной системы Windows.	2
	Практическая работа №11 Разграничение прав пользователей в защищенных версиях операционной системы Windows. Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows.	2
	Практическая работа №12 Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности, при использовании глобальных вычислительных сетей.	2

1	2	3
	Практическая работа №13 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.	2
	Практическая работа №14 Практические навыки работы сканирования сети с помощью Honeypot, Nmap.	2
	Практическая работа №15 Изучение антивирусных программ.	2
	Практическая работа №16 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.	2
	Практическая работа №17 Работа с SIEM (Security information and event management): SIM – Security Information Management – управление информационной безопасностью SEM – Security Event Management – управление событиями безопасности.	2
	Практическая работа №18 Защита с помощью систем обнаружения и предотвращения вторжений при помощи NIPS/NIDS: Snort.	2
Подготовка реферативного выступления		40
Систематизация полученных знаний при подготовке к экзамену		36
	ИТОГО:	**144**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

Учебном планом специальности в качестве формы промежуточной аттестации по учебной дисциплине «Теоретические основы информационной безопасности» предусмотрены зачет и экзамен. 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, письменный экзамен);

–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:

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_n) + (\text{ПР}_1 + \ldots + \text{ПР}_9) + (\text{КР}_1) + (\text{КР}_2)}{(12 + n)},$$

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

$\text{ПР}_1 + \ldots + \text{ПР}_9$ – отметки, выставленные по результатам защит практических работ;

n – количество тестов;

$\text{КР}_1, \text{КР}_2$ – отметки, выставленные по результатам контрольных работ.

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 №1	*Тема 2.1.* Угрозы информационной безопасности. *Тема 2.2.* Информационная война как угроза национальной безопасности.	Предлагается пять вопросов: два из их теоретических, остальные представлены в виде тестовых заданий	Каждый вопрос оценивается в два балла Максимальная отметка 10 (десять) баллов
Контрольная работа №2	*Тема 4.1.* Уровни информационной безопасности. *Тема 4.2.* Политика информационной безопасности.	Предлагается ответить на три вопроса	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 зачёта и экзамена.

1. Зачёт проводится согласно Положению.

Заключение о *зачёте* формируется по формуле:

$$З = k \cdot Т,$$

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

2. Экзамен проводится согласно Положению.

Итоговая экзаменационная отметка (ИЭ) учитывает отметку по результатам текущего контроля (Т) и экзаменационную отметку (Э). 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 1.

Таблица 1 – Составляющие итоговой отметки по дисциплине

Составляющие (ИЭ)	*k*	Т	*1-k*	Э
	0,5	Представлены в таблице 2	0,5	*

*Отметка, полученная студентом на экзамене за письменный ответ по экзаменационному билету.

Итоговая отметка по дисциплине определяется по формуле:

$$ИЭ = 0{,}5Т + 0{,}5Э.$$

Положительной является отметка не ниже 4 баллов.

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.

Используемые технологии обучения и диагностики компетенций в преподавании дисциплины «Теоретические основы информационной безопасности» 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 «Теоретические основы информационной безопасности» 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 информационной безопасности и формируют системное понимание проблем безопасности и путей их решения и практических занятиях, на которых развиваются и формируются необходимые практические умения и навыки в области информационной безопасности.

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 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**
«Программно-аппаратные и технические средства защиты информации»	Кафедра математики и компьютерной безопасности	Замечаний и предложений нет	
«Методы и стандарты оценки защищенности компьютерных систем»	Кафедра математики и компьютерной безопасности	Замечаний и предложений нет	
«Криптографические протоколы»	Кафедра математики и компьютерной безопасности	Замечаний и предложений нет	

Заведующий кафедрой математики и компьютерной безопасности, к.т.н., доцент И.Б. Бураченок

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**
«Защита информации в операционных системах и компьютерных сетях»	Вычислительных систем и сетей	Предложений нет	
«Компьютерная защита финансовой информации»		Предложений нет	

Заведующий кафедрой вычислительных систем и сетей, д.т.н., доцент Р. П. Богуш