Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования
«Полоцкий государственный университет
имени Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«_15_» ____12____ 2025 г.
Регистрационный №УД-_523-25_/уч.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебная программа учреждения образования
по учебной дисциплине для специальности
6-05-0533-12 «Кибербезопасность»

2025 г.

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 6-05-0533-12-2023 и учебного плана специальности 6-05-0533-12 «Кибербезопасность». Регистрационный №14-23/уч. ФКНЭ от 04.04.2023 г. для 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»

РЕЦЕНЗЕНТЫ:
К.Я. Раханов, к.т.н., доцент, технический директор ООО «ТриИнком»
В.А. Бондаренко, заместитель директора ОДО «Абсолют Интернет Системс»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 11 от «21» 11 2025 г.).

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 3 от «15» 12 2025 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Растет количество инцидентов, наиболее атакуемыми отраслями стали информационные технологии, промышленность и ритейл. Выросла доля компьютерных атак. Для организаций самые распространенные последствия кибератак – утечки конфиденциальной информации и нарушение основной деятельности. Наблюдается большое количество утечек персональных данных пользователей, массовые атаки через эксплуатацию уязвимостей. Успешные кибератаки затрагивают предприятия и малого, и крупного бизнеса. Поэтому подготовка специалистов в области информационной кибербезопасности в настоящее время – актуальная и востребованная задача.

Учебная дисциплина «Безопасность информационных систем» ориентирована на обучение студентов базовым знаниям, умениям и навыкам в области информационной безопасности и защиты информации и ориентирована на подготовку специалиста, умеющего создавать защищенные информационные системы, а также осуществлять оценку защищенности компьютерно-коммуникационных систем. Изучаемые темы представляются на основе современной нормативной регулятивной базы и национального законодательства.

Целью изучения дисциплины «Безопасность информационных систем» 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 кибербезопасности».

Задачи изучения дисциплины «Безопасность информационных систем». 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.

При изучении дисциплины «Безопасность информационных систем» у студентов специальности 6-05-0533-12 «Кибербезопасность» должен сформироваться набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «Специалист по кибербезопасности» обеспечивающих выпускникам по указанной специальности успешность применения полученных знаний и умений в дальнейшей профессиональной деятельности:

универсальные компетенции:

– владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации;

– решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий;

– работать в команде, толерантно воспринимать социальные, этнические, конфессиональные, культурные и иные различия;

– быть способным к саморазвитию и совершенствованию в профессиональной деятельности;

– проявлять инициативу и адаптироваться к изменениям в профессиональной деятельности;

базовые профессиональные компетенции:

– использовать основные понятия и нормативные правовые акты в сфере кибербезопасности для описания, классификации и применения теоретических, нормативно-правовых, инженерно-технических, организационных методов обеспечения безопасности информации и информационно-коммуникационных инфраструктур.

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

В результате изучения дисциплины «Безопасность информационных систем» 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.

Связи с другими учебными дисциплинами.

Основой для изучения учебной дисциплины «Безопасность информационных систем» по специальности 6-05-0533-12 «Кибербезопасность» является предмет «Информатика», изучаемый при получении общего базового и общего среднего образования, а также студентам необходимы знания, полученные при изучении базовых дисциплин государственного компонента модуля «Информатика и компьютерные системы»: «Архитектура компьютеров», «Операционные системы», «Компьютерные сети»; дисциплин модуля «Безопасность информационных технологий»: «Основы кибербезопасности», «Криптографические методы защиты информации» и дисциплины компонента учреждения высшего образования модуля «Криптография»: «Арифметические и алгебраические основы криптографии»; дисциплин модуля «Кибербезопасность»: «Защита информации в операционных системах и компьютерных сетях» и «Защита от вредоносного программного обеспечения».

Знания, полученные при изучении дисциплины «Безопасность информационных систем», непосредственно связаны с учебными дисциплинами компонента учреждения высшего образования модуля «Кибербезопасность»: «Программно-аппаратные и технические средства защиты информации», «Методы и стандарты оценки защищенности компьютерных систем», «Технологии и безопасность интернета вещей»; дисциплин модуля «Криптография» «Криптографические протоколы», «Криптографический инжиниринг», а также другими дисциплинами, предусмотренными учебным планом по специальности.

Изучение учебной дисциплины «Безопасность информационных систем» позволяет дать студентам базу, необходимую для успешного усвоения материала перечисленных выше

учебных дисциплин, а также получить знания, необходимые им в дальнейшем для успешной работы.

Форма получения высшего образования – дневная.

В соответствии с учебным планом по специальности 6-05-0533-12 «Кибербезопасность» на изучение учебной дисциплины отводится:

Курс (курсы)	3,4
Семестр	6,7
Всего часов по учебной дисциплине, часов	306
Всего аудиторных часов по учебной дисциплине, часов	140
В том числе:	
Семестр 6	
Всего часов по дисциплине	108
Всего аудиторных часов по дисциплине	68
Лекции, часов	34
Лабораторные занятия, часов	34
Самостоятельная работа по дисциплине, часов	40
Форма промежуточной аттестации по дисциплине	зачет
Трудоёмкость дисциплины, з.е.	3
Семестр 7	
Всего часов по дисциплине	198
Всего аудиторных часов по дисциплине	72
Лекции, часов	36
Лабораторные занятия, часов	36
Самостоятельная работа по дисциплине, часов	126
Форма промежуточной аттестации по дисциплине	экзамен
Трудоёмкость дисциплины, з.е.	6

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Семестр 6

ВВЕДЕНИЕ В ДИСЦИПЛИНУ

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

Раздел 1. БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Тема 1.1. Информационная безопасность и ее составляющие.

Понятие информационной безопасности. Информационное общество. Безопасность в информационном обществе. Место информационной безопасности в системе национальной безопасности. Основные формы проявления информации. Характеристики информации. Общая схема процесса обеспечения безопасности. Информационная безопасность и защита информации. Система показателей, характеризующих информацию. Качество информации и его обеспечение. Цели и задачи, решение которых должна обеспечить информационная безопасность.

Тема 1.2. Государственные органы и учреждения, занимающиеся вопросами защиты информации в Республики Беларусь.

Положения государственной политики информационной безопасности РБ. Государственная система защиты РБ. 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 и пр.

Тема 1.3. 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 1.4. 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. Обзор и сравнительный анализ стандартов информационной безопасности.

Тема 1.5. Основные характеристики безопасности и способы их обеспечения.

Доступность, целостность и подлинность, конфиденциальность информации и информационных ресурсов. Методы и способы их защиты: правовые, организационно-административные, программно-технические.

Раздел 2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. УРОВНИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 2.1. Угрозы информационной безопасности.

Ключевые термины: понятие ущерб, угроза, уязвимость. Внутренние и внешние угрозы. Угрозы безопасности информационно-коммуникационных технологий. Классификация умышленных угроз. Общая классификация угроз. Угрозы доступности.

Угрозы целостности. Угрозы конфиденциальности. Анализ угроз информационной безопасности информационно-коммуникационных технологий.

Тема 2.2. Методы реализации угроз.

Система дестабилизирующих факторов, влияющих на уязвимость информации. Методология формирования полного множества угроз. Основные методы реализации угроз. Причины, виды и каналы утечки информации. Каналы несанкционированного доступа к информации.

Тема 2.3. Уязвимости информации и информационных систем.

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

Тема 2.4. Методики и программные продукты для оценки рисков.

Матрица классификации рисков информационной безопасности. Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности ISO/ГОСТ 27005 (СТБ ISO/IEC 27005-2024). Проведение оценки рисков в соответствии с методикой Microsoft. Методологии моделирования угроз STRIDE, DREAD, PASTA.

Раздел 3 ПРАВОВЫЕ И ЭТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Тема 3.1. Организационные и правовые аспекты защиты данных.

Основные понятия и определения. Правовая защита от компьютерных преступлений. Виды компьютерных преступлений, мошенничество в интернете. Защита данных в коммерческих и государственных организациях. Авторские права. Административное и уголовное право в защите данных.

Тема 3.2. Правовое регулирование защиты персональных данных в Республике Беларусь

Информация как объект правовых отношений. Роль правового регулирования в обеспечении информационной безопасности. Категории персональных данных. Защита персональных данных. Законодательство и нормативные акты.

Тема 3.3. Этические нормы и кодексы в области информационной безопасности. Ответственность и юридические аспекты.

Общая характеристика нормативно-правовых актов в сфере обеспечения защиты персональных данных. Проблемные вопросы реализации правового обеспечения защиты персональных данных. Согласие субъекта персональных данных на обработку его персональных данных. Права субъекта персональных данных. Обязанности оператора. Ответственность за нарушение законодательства о персональных данных.

Тема 3.4. Организация обработки персональных данных.

Меры по обеспечению безопасности персональных данных при их обработке. Организация работ по обработке персональных данных. Организационно-распорядительная документация по защите персональных данных. Особенности обработки биометрических персональных данных. Осуществление технической и криптографической защиты персональных данных. Уведомление Центра о нарушениях систем защиты персональных данных.

Раздел 4. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 4.1. Уровни информационной безопасности.

Законодательный уровень информационной безопасности. Обзор белорусского и российского законодательств. Международные стандарты и спецификации. 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. Стандарты ISO/IEC 17799/27002 и 27001. Стандартизация и сертификация (СТБ ISO 27000. СТБ 34.101.XX).

Тема 4.4. Аудит информационной безопасности.

Аудит информационной безопасности. Методы анализа данных при аудите информационной безопасности. Управление рисками. Анализ информационных рисков предприятия. Методы оценивания информационных рисков. Управление информационными рисками.

Семестр 7

ВВЕДЕНИЕ ВО ВТОРУЮ ЧАСТЬ ДИСЦИПЛИНЫ

История развития систем защиты информации в зарубежных странах. Развитие средств и методов защиты информации. Этапы развития системы защиты информации в настоящее время. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности.

Раздел 1. ГОСУДАРСТВЕННАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 1.1. Информационное противоборство в системе международных отношений современного общества.

Современная концепция информационной войны в США. Правовое регулирование информационной безопасности в США. Государственные органы обеспечения национальной безопасности США. Состояние проблемы информационной безопасности в странах Евросоюза. Системы защиты информации в Соединённом королевстве Великобритании и Северной Ирландии. Системы защиты информации в Федеративной республике Германия. Системы защиты информации во Французской республике. Системы защиты информации в Швеции. «Великая стена» информационной безопасности Китае.

Тема 1.2. Международное сотрудничество в области обеспечения информационной безопасности.

Развитие международного сотрудничества в области информационной безопасности. Международные организации в области информационной безопасности. Правовое регулирование сети Интернет.

Тема 1.3. Стандарты информационной безопасности.

Предпосылки создания стандартов информационной безопасности. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерий». Стандарт COBIT. Стандарты по безопасности информационных технологий в России.

Раздел 2. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Тема 2.1. Программные и аппаратные средства защиты данных в информационных системах

Методы и средства защиты данных, основанные на использовании криптографии. Стеганография. Основные стандарты, применяемые в программных средствах шифрования данных (AES, belt, ГОСТ 28147). Применение программного средства TrueCrypt. Аппаратные средства защиты данных на примере использования переносимых устройств хранения данных (flash-накопителей). Программные и аппаратные средства защиты данных от копирования. Примеры.

Тема 2.2. Информационная безопасность вычислительных средств с использованием современных операционных систем, систем управления базами данных и языков программирования

Основные понятия. Администрирование операционных систем в контексте обеспечения безопасности. Фундаментальные концепции безопасности операционных систем: защищенные области, матрицы доступа, механизмы безопасности. Основы безопасности в Microsoft Windows (accounts, group policies, NTFS permission, audit). Примеры

администрирования. Различные аспекты безопасности баз данных, их администрирования: permission, roles, views and stored procedures.

Тема 2.3. Информационная безопасность и защита данных с использованием мобильных устройств их хранения

Понятие Firewall и их использование. Фильтрация пакетов. Применение «переносимых устройств» (на примере Flash-устройств Transcend) для защиты от посягательств на доступ к конфиденциальным данным. Возможности «шифрования данных на аппаратном уровне». «Беспроводная и мобильная» безопасность в сетях: GSM-security, Bluetooth-security.

Тема 2.4. Методы разграничение доступа

Методы разграничения доступа. Мандатное управление доступом. Дискретное управление доступом. Матрица полномочий. Уровень секретности и категория субъекта. Методы управления доступом, предусмотренные в руководящих документах. Рекомендации по обеспечению защиты общедоступной информации в информационных системах.

Тема 2.5. Модели защиты информации.

Модели защиты информации. Модель Харрисона-Рузо-Ульмана. Модель Белла-ЛаПадулы. Модель Биба и Кларка-Уилсона. 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. Методология оценки защищенности.

Тема 3.3. 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 3.4. Методики построения систем защиты информации.

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

РАЗДЕЛ 4 ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема 4.1 Классификация технических каналов утечки информации

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

Тема 4.2 Обзор технических средств негласного съёма акустической информации

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

Тема 4.3. Технические средства защиты речевой информации

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

Тема 4.4 Звуковые сигналы

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

Тема 4.5 Применение шумов для маскирования речевых сигналов

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

Тема 4.6 Методика и порядок проведения мероприятий по выявлению и исследованию каналов утечки информации

Аттестация объектов информатизации. Методика и порядок проведения мероприятий по выявлению и исследованию каналов утечки информации. Специальные проверки. Специальные обследования. Специальные исследования.

Учебно-методическая карта учебной дисциплины «Безопасность информационных систем»
Дневная форма получения высшего образования

6 семестр

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
	Введение в дисциплину Цели и задачи изучения дисциплины. Содержание и структура дисциплины. Основные термины и определения, использующиеся в материале.						
	Раздел 1 Безопасность информационных систем	**10**	**10**				
1	**Лекция № 1** *Тема 1.1 Основы информационной грамоты. Информационная безопасность и ее составляющие.* Понятие информационной безопасности. Информационное общество. Безопасность в информационном обществе. Место информационной безопасности в системе национальной безопасности. Основные формы проявления информации. Характеристики информации. Общая схема процесса обеспечения безопасности. Информационная безопасность и защита информации. Система показателей, характеризующих информацию. Качество информации и его обеспечение. Цели и задачи, решение которых должна обеспечить информационная безопасность.	2				Осн. лит.: [1], [2]. Доп. лит.: [2], [13]. Норм.: [1], [2], [11].	Блиц-опрос

1	2	3	4	5	6	7	8
2	**Лабораторная работа №1** Методы работы с PowerShell.		2			Методические указания	*Защита отчета по лабораторной работе № 1
3	**Лекция № 2** *Тема 1.2 Государственные органы и учреждения, занимающиеся вопросами защиты информации в Республики Беларусь.* Положения государственной политики информационной безопасности РБ. Государственная система защиты РБ. 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 и пр.	2				Осн. лит.: [1], [2]. Доп. лит.: [2], [13]. Норм.: [1], [2], [6], [7].	Блиц-опрос
4	**Лабораторная работа №2** Построение регулярных выражений.		2			Методические указания	*Защита отчета по лабораторной работе № 2
5	**Лекция № 3** *Тема 1.3 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]. Доп. лит.: [2], [13].	Блиц-опрос
6	**Лабораторная работа №3** Изучение базовых команд Windows.		2			Методические указания	*Защита отчета по лабораторной работе № 3

1	2	3	4	5	6	7	8
7	**Лекция № 4** *Тема 1.4. 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. Обзор и сравнительный анализ стандартов информационной безопасности.	2				Осн. лит.: [1], [2]. Доп. лит.: [2], [13].	*Контрольное тестирование №1
8	**Лабораторная работа №4** Изучение базовых команд Linux.		2			Методические указания	*Защита отчета по лабораторной работе № 4
9	**Лекция № 5** *Тема 1.5. Основные характеристики безопасности и способы их обеспечения.* Доступность, целостность и подлинность, конфиденциальность информации и информационных ресурсов. Методы и способы их защиты: правовые, организационно-административные, программно-технические.	2				Осн. лит.: [1], [2]. Доп. лит.: [13].	Блиц-опрос
10	**Лабораторная работа №5** Разграничение прав пользователей в защищенных версиях операционной системы Windows.		2			Методические указания	*Защита отчета по лабораторной работе № 5
	Раздел 2 Угрозы информационной безопасности. Уровни информационной безопасности	**8**		**8**			
11	**Лекция № 6** *Тема 2.1. Угрозы информационной безопасности.* Ключевые термины: понятие ущерб, угроза, уязвимость. Внутренние и внешние угрозы. Угрозы безопасности информационно-коммуникационных технологий.						

1	2	3	4	5	6	7	8
	Классификация умышленных угроз. Общая классификация угроз. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности. Анализ угроз информационной безопасности информационно-коммуникационных технологий.	2				Осн. лит.: [1], [2]. Доп. лит.: [4], [5].	Блиц-опрос
12	**Лабораторная работа №6** Изучение механизмов управления доступа к ресурсам, прав доступа в операционной системе Linux.		2			Методические указания	*Защита отчета по лабораторной работе № 6
13	**Лекция № 7** *Тема 2.2. Методы реализации угроз.* Система дестабилизирующих факторов, влияющих на уязвимость информации. Методология формирования полного множества угроз. Основные методы реализации угроз. Причины, виды и каналы утечки информации. Каналы несанкционированного доступа к информации.	2				Осн. лит.: [1], [2]. Доп. лит.: [2], [4], [5].	***Контрольная работа №1***
14	**Лабораторная работа №7** Реализация политики безопасности в защищенных версиях операционной системы Windows.		2			Методические указания	*Защита отчета по лабораторной работе № 7
15	**Лекция №8** *Тема 2.3. Уязвимости информации и информационных систем.* Уязвимость информации и информационных систем. Система показателей уязвимости. Методы и модели оценки уязвимостей. Стандарт CVSS.	2				Осн. лит.: [1], [2]. Доп. лит.: [4], [5], [13].	Блиц-опрос
16	**Лабораторная работа №8** Реализация политики безопасности в операционной системе Linux.		2			Методические указания	*Защита отчета по лабораторной работе № 8
17	**Лекция №9** *Тема 2.4. Методики и программные продукты для оценки рисков.* Матрица классификации рисков информационной безопасности. Методика CRAMM. Методика FRAP. Методика OCTAVE. Методика RiskWatch. Методы и средства обеспечения безопасности.						

1	2	3	4	5	6	7	8
	Менеджмент риска информационной безопасности ISO/ГОСТ 27005 (СТБ ISO/IEC 27005-2024). Проведение оценки рисков в соответствии с методикой Microsoft. Методологии моделирования угроз STRIDE, DREAD, PASTA.	2				Осн. лит.: [1], [2]. Доп. лит.: [1], [12]. Норм.: [12-24].	Блиц-опрос
18	**Лабораторная работа №9** Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности, при использовании глобальных вычислительных сетей.		2			Методические указания	*Защита отчета по лабораторной работе № 9
	Раздел 3 Правовые и этические аспекты обеспечения информационной безопасности и защиты персональных данных	**8**	**8**				
19	**Лекция №10** *Тема 3:1 Организационные и правовые аспекты защиты данных.* Основные понятия и определения. Правовая защита от компьютерных преступлений. Виды компьютерных преступлений, мошенничество в интернете. Защита данных в коммерческих и государственных организациях. Авторские права. Административное и уголовное право в защите данных.	2				Осн. лит.: [1], [2], [4]. Доп. лит.: [6], [8], [9]. Норм.: [3], [4], [5], [6], [7], [8], [9], [10].	Блиц-опрос
20	**Лабораторная работа №10** Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.		2			Методические указания	*Защита отчета по лабораторной работе № 10
21	**Лекция №11** *Тема 3.2 Правовое регулирование защиты персональных данных в Республике Беларусь* Информация как объект правовых отношений. Роль правового регулирования в обеспечении информационной безопасности. Категории персональных данных. Защита персональных данных. Законодательство и нормативные акты.	2				Осн. лит.: [1], [2], [4]. Доп. лит.: [6], [8], [9]. Норм.: [3], [4], [5], [6], [7], [8], [9], [10].	Блиц-опрос
22	**Лабораторная работа №11** Сброс пароля пользователя в операционной системе Windows.		2			Методические указания	*Защита отчета по лабораторной работе № 11

1	2	3	4	5	6	7	8
23	**Лекция № 12** *Тема 3.3 Этические нормы и кодексы в области информационной безопасности. Ответственность и юридические аспекты.* Общая характеристика нормативно-правовых актов в сфере обеспечения защиты персональных данных. Проблемные вопросы реализации правового обеспечения защиты персональных данных. Согласие субъекта персональных данных на обработку его персональных данных. Права субъекта персональных данных. Обязанности оператора. Ответственность за нарушение законодательства о персональных данных.	2				Осн. лит.: [1], [2], [4]. Доп. лит.: [6], [8], [9]. Норм.: [3], [4], [5], [6], [7], [8], [9], [10].	Блиц-опрос
24	**Лабораторная работа №12** Сброс пароля пользователя на ядре Linux.		2			Методические указания	*Защита отчета по лабораторной работе № 12
25	**Лекция № 13** *Тема 3.4 Организация обработки персональных данных.* Меры по обеспечению безопасности персональных данных при их обработке. Организация работ по обработке персональных данных. Организационно-распорядительная документация по защите персональных данных. Особенности обработки биометрических персональных данных. Осуществление технической и криптографической защиты персональных данных. Уведомление Центра о нарушениях систем защиты персональных данных.	2				Осн. лит.: [1], [2], [4]. Доп. лит.: [6], [8], [9]. Норм.: [3], [4], [5], [6], [7], [8], [9], [10].	*Контрольное тестирование №2
26	**Лабораторная работа №13** Обеспечение целостности и доступности данных с использованием избыточного массива независимых жестких дисков Raid и менеджера логических томов LVM.		2			Методические указания	*Защита отчета по лабораторной работе № 13
	Раздел 4 Политика информационной безопасности	**8**		**8**			
27	**Лекция № 14** *Тема 4.1. Уровни информационной безопасности.* Законодательный уровень информационной безопасности. Обзор белорусского и российского законодательств.						

1	2	3	4	5	6	7	8
	Международные стандарты и спецификации. 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]. Доп. лит.: [4], [5].	Блиц-опрос
28	**Лабораторная работа №14** Работа с программным межсетевым экраном VIPNet Office Firewall.		2			Методические указания	*Защита отчета по лабораторной работе № 14
29	**Лекция № 15** *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]. Доп. лит.: [4], [5].	*Контрольное тестирование №3
30	**Лабораторная работа №15** Практические навыки работы сканирования сети с помощью Honeypot, Nmap.		2			Методические указания	*Защита отчета по лабораторной работе № 15
31	**Лекция № 16** *Тема 4.3. Менеджмент информационной безопасности.* Системы менеджмента безопасности информации. Правила и требования. Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001. Стандартизация и сертификация (СТБ ISO 27000, СТБ 34.101.XX).	2				Осн. лит.: [1], [2]. Доп. лит.: [1], [4], [5].	***Контрольная работа №2***
32	**Лабораторная работа №16** Работа с частными виртуальными сетями.		2			Методические указания	*Защита отчета по лабораторной работе № 16
33	**Лекция № 17** *Тема 4.4. Аудит информационной безопасности.* Аудит информационной безопасности.						

1	2	3	4	5	6	7	8
	Методы анализа данных при аудите информационной безопасности. Управление рисками. Анализ информационных рисков предприятия. Методы оценивания информационных рисков. Управление информационными рисками.	2				Осн. лит.: [1], [2]. Доп. лит.: [1], [4], [5].	Блиц-опрос
34	**Лабораторная работа №17** DDoS (Distributed Denial of Service) – основные особенности их организации и защиты от них.		2			Методические указания	*Защита отчета по лабораторной работе № 17
	Всего (68 часов)	**34**	**34**				

*** МЕРОПРИЯТИЯ ТЕКУЩЕГО КОНТРОЛЯ**

Учебно-методическая карта учебной дисциплины «Безопасность информационных систем»
Дневная форма получения высшего образования

7 семестр

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Литература	Формы контроля знаний
		лекции	Лабораторные занятия	Практические занятия	Управляемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
	Введение во вторую часть дисциплины История развития систем защиты информации в зарубежных странах. Развитие средств и методов защиты информации. Этапы развития системы защиты информации в настоящее время. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности.					Осн. лит.: [3], [5]. Доп. лит.: [3], [15].	
	Раздел 1 Государственная политика информационной безопасности	**6**	**6**				
1	**Лекция № 1** *Тема 1.1. Информационное противоборство в системе международных отношений современного общества.* Современная концепция информационной войны в США. Правовое регулирование информационной безопасности в США. Государственные органы обеспечения национальной безопасности США. Состояние проблемы информационной безопасности в странах Евросоюза. Системы защиты информации в Соединённом королевстве Великобритании и Северной Ирландии.	2				Осн. лит.: [3], [5]. Доп. лит.: [3], [15].	Блиц-опрос

1	2	3	4	5	6	7	8
	Системы защиты информации в Федеративной республике Германия. Системы защиты информации во Французской республике. Системы защиты информации в Швеции. «Великая стена» информационной безопасности Китае.						
2	**Лабораторная работа №1** Методики работы антивирусных программ.		2			Методические указания	*Защита отчета по лабораторной работе № 1
3	**Лекция № 2** *Тема 1.2. Международное сотрудничество в области обеспечения информационной безопасности.* Развитие международного сотрудничества в области информационной безопасности. Международные организации в области информационной безопасности. Правовое регулирование сети Интернет.	2				Осн. лит.: [3], [5]. Доп. лит.: [3], [15].	Блиц-опрос
4	**Лабораторная работа №2** Работа с антивирусом «Kaspersky Antivirus».		2			Методические указания	*Защита отчета по лабораторной работе № 2
5	**Лекция № 3** *Тема 1.3. Стандарты информационной безопасности.* Предпосылки создания стандартов информационной безопасности. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран. Германский стандарт BSI. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерий». Стандарт COBIT. Стандарты по безопасности информационных технологий в России.	2				Осн. лит.: [3], [5]. Доп. лит.: [3], [15].	*Контрольное тестирование №1
6	**Лабораторная работа №3** Работа с антивирусом «Безопасность Windows».		2			Методические указания	*Защита отчета по лабораторной работе № 3

1	2	3	4	5	6	7	8
	Раздел 2 Методы и средства защиты информации	**10**	**10**				
7	**Лекция № 4** *Тема 2.1. Программные и аппаратные средства защиты данных в информационных системах* Методы и средства защиты данных, основанные на использовании криптографии. Стеганография. Основные стандарты, применяемые в программных средствах шифрования данных (AES, belt, ГОСТ 28147). Применение программного средства TrueCrypt. Аппаратные средства защиты данных на примере использования переносимых устройств хранения данных (flash-накопителей). Программные и аппаратные средства защиты данных от копирования. Примеры.	2				Осн. лит.: [2]. Доп. лит.: [3], [15].	Блиц-опрос
8	**Лабораторная работа №4** Работа с антивирусами в Linux.		2			Методические указания	*Защита отчета по лабораторной работе № 4
9	**Лекция № 5** *Тема 2.2. Информационная безопасность вычислительных средств с использованием современных операционных систем, систем управления базами данных и языков программирования.* Основные понятия. Администрирование операционных систем в контексте обеспечения безопасности. Фундаментальные концепции безопасности операционных систем: защищенные области, матрицы доступа, механизмы безопасности. Основы безопасности в Microsoft Windows (accounts, group policies, NTFS permission, audit). Примеры администрирования. Различные аспекты безопасности баз данных, их администрирования: permission, roles, views and stored procedures.	2				Осн. лит.: [2]. Доп. лит.: [3], [15].	***Контрольная работа №1**
10	**Лабораторная работа №5** Работа с брандмауэром в Windows.		2			Методические указания	*Защита отчета по лабораторной работе № 5

1	2	3	4	5	6	7	8
11	**Лекция №6** *Тема 2.3. Информационная безопасность и защита данных с использованием мобильных устройств их хранения.* Понятие Firewall и их использование. Фильтрация пакетов. Применение «переносимых устройств» (на примере Flash-устройств Transcend) для защиты от посягательств на доступ к конфиденциальным данным. Возможности «шифрования данных на аппаратном уровне». «Беспроводная и мобильная» безопасность в сетях: GSM-security, Bluetooth-security.	2				Осн. лит.: [2]. Доп. лит.: [3], [15].	Блиц-опрос
12	**Лабораторная работа №6** Работа с песочницами и файловыми антивирусами Sandbox.		2			Методические указания	*Защита отчета по лабораторной работе № 6
13	**Лекция №7** *Тема 2.4. Методы разграничение доступа.* Методы разграничения доступа. Мандатное управление доступом. Дискретное управление доступом. Матрица полномочий. Уровень секретности и категория субъекта. Методы управления доступом, предусмотренные в руководящих документах. Рекомендации по обеспечению защиты общедоступной информации в информационных системах.	2				Осн. лит.: [2]. Доп. лит.: [3], [15].	Блиц-опрос
14	**Лабораторная работа №7** Получение практических навыков программного восстановления данных при помощи программ TestDisk, PhotoRec, Extundelete, Foremost.		2			Методические указания	*Защита отчета по лабораторной работе № 7
15	**Лекция №8** *Тема 2.5. Модели защиты информации.* Модели защиты информации. Модель Харрисона-Рузо-Ульмана. Модель Белла-ЛаПадулы. Модель Биба и Кларка-Уилсона. Ролевая модель безопасности. Структура профиля защиты. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISI/IEC 15408.	2				Осн. лит.: [2]. Доп. лит.: [3], [15].	Блиц-опрос

1	2	3	4	5	6	7	8
16	**Лабораторная работа №8** Работа с программой электронно-цифровой подписи pgp.		2			Методические указания	*Защита отчета по лабораторной работе № 8
	Раздел 3 Построение систем защиты информации	**8**	**8**				
17	**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.: [2]. Доп. лит.: [3], [15].	Блиц-опрос
18	**Лабораторная работа №9** Создание и установка контролера домена с использованием технологии Active Directory.		2			Методические указания	*Защита отчета по лабораторной работе № 9
19	**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. Методология оценки защищенности.	2				Осн. лит.: [2]. Доп. лит.: [3], [15].	Блиц-опрос
20	**Лабораторная работа №10** Защита почтового сервера от спама при помощи Anti-Spam SMTP Proxy (ASSP).		2			Методические указания	*Защита отчета по лабораторной работе № 10
21	**Лекция № 11** *Тема 3.3. 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.: [2]. Доп. лит.: [10], [11].	*Контрольное тестирование №2

1	2	3	4	5	6	7	8
22	**Лабораторная работа №11** Защита с помощью систем обнаружения и предотвращения вторжений при помощи NIPS/NIDS: Snort.		2			Методические указания	*Защита отчета по лабораторной работе № 11
23	**Лекция № 12** *Тема 3.4. Методики построения систем защиты информации.* Модель Lifecycle Security. Модель многоуровневой защиты. Методика управления рисками, предлагаемая Microsoft.	2				Осн. лит.: [2]. Доп. лит.: [3], [15].	Блиц-опрос
24	**Лабораторная работа №12** Шифрование/дешифрование данных при помощи программ PGP, GPG, Шифрование данных «на лету» при помощи TrueCrypt. Спецификация шифрования диска LUCKS/dm-crypt.		2			Методические указания	*Защита отчета по лабораторной работе № 12
	Раздел 4 Инженерно-техническая защита объектов от несанкционированного доступа	**8**	**8**				
25	**Лекция № 13** *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.	2				Осн. лит.: [6]. Доп. лит.: [3], [7], [10], [14].	Блиц-опрос
26	**Лабораторная работа №13** Методы и модели оценки уязвимостей. Стандарт CVSS.		2			Методические указания	*Защита отчета по лабораторной работе № 13
27	**Лекция № 14** *Тема 4.2 Обзор технических средств негласного съёма акустической информации* Необходимость технической защиты информации. Классификация технических средств съёма акустической информации. Закладочные устройства. Технические средства дистанционного съёма информации. Технические средства съёма информации с линий связи.	2				Осн. лит.: [6]. Доп. лит.: [7], [10], [3], [14].	Блиц-опрос

1	2	3	4	5	6	7	8
28	**Лабораторная работа №14** Практически 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 лабораторной работе № 14
29	**Лекция № 15** *Тема 4.3. Технические средства защиты речевой информации.* Типы технических средств защиты информации. Подавители записывающих устройств. Обнаружители закамуфлированных камер. Устройства для активной защиты речевой информации от утечки по акустическому и вибрационному каналам.	2				Осн. лит.: [6]. Доп. лит.: [3], [7], [10], [14].	Блиц-опрос
30	**Лабораторная работа №15** Инженерно-техническая защита информации. Оценка первичных признаков элементов речевого сигнала.		2			Методические указания	*Защита отчета по лабораторной работе № 15
31	**Лекция № 16** *Тема 4.4 Звуковые сигналы.* Звуковые сигналы. Пример создания гармонического и полигармонического сигнала. Основные характеристики гармонического сигнала. Энергетический спектр речевого сигнала.	2				Осн. лит.: [6]. Доп. лит.: [3], [7], [10], [14].	*Контрольное тестирование №3
32	**Лабораторная работа №16** Инженерно-техническая защита информации. Создание маскирующего шума для имитации виброакустического зашумления.		2			Методические указания	*Защита отчета по лабораторной работе № 16
33	**Лекция № 17** *Тема 4.5 Применение шумов для маскирования речевых сигналов.* Маскирование речевых сообщений. Понятие шума. Основные характеристики шума. Примеры построения гистограммы распределения плотности вероятности шума. Синтез смеси гармонического сигнала и шума с заданным отношением сигнал/шум.	2				Осн. лит.: [6]. Доп. лит.: [3], [7], [10], [14].	***Контрольная работа №2**
34	**Лабораторная работа №17** Инженерно-техническая защита информации. Применение маскирующего шума для имитации виброакустического зашумления.		2			Методические указания	*Защита отчета по лабораторной работе № 17

1	2	3	4	5	6	7	8
35	**Лекция № 18** *Тема 4.6 Методика и порядок проведения мероприятий по выявлению и исследованию каналов утечки информации* Аттестация объектов информатизации. Методика и порядок проведения мероприятий по выявлению и исследованию каналов утечки информации. Специальные проверки. Специальные обследования. Специальные исследования.	2				Осн. лит.: [6]. Доп. лит.: [7], [3],[14],	*Контрольное тестирование №4
36	**Лабораторная работа №18** Инженерно-техническая защита информации. Мероприятия по выявлению каналов утечки информации (специальные проверки, специальные обследования, специальные исследования).		2			Методические указания	*Защита отчета по лабораторной работе № 18
	Всего (72 часа)	**36**	**36**				

*** МЕРОПРИЯТИЯ ТЕКУЩЕГО КОНТРОЛЯ**

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Зенков, А. В. Основы информационной безопасности : учебное пособие : [16+] / А. В. Зенков. – Москва ; Вологда : Инфра-Инженерия, 2022. – 104 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=725671 (дата обращения: 18.02.2026). – Библиогр.: с. 95. – ISBN 978-5-9729-0864-6. – Текст : электронный.

2. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд., стер. – Санкт-Петербург : Лань, 2024. – 324 с. – ISBN 978-5-507-49077-6. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/370967 (дата обращения: 18.02.2025). – Режим доступа: для авториз. пользователей.

3. 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».

4. Меры по обеспечению защиты персональных данных: учебное пособие / А.И. Гавриленко, Д. Н. Гайкевич, В. И. Диско [и др.]; под общ. ред. А.А. Гаева, М. А. Городецкой. – Минск: РИВШ, 2025. – 78 с.

5. 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: 01.02.2026). – Библиогр.: с. 192-193. – ISBN 978-5-9765-1274-0. – Текст : электронный.

6. Киренберг, А. Г., Коротин, В. О. Защита информации от утечки по техническим каналам : учебное пособие / А. Г. Киренберг, В. О. Коротин; Министерство науки и высшего образования Российской Федерации, Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово, 2023. – 221 с. – ISBN 978-5-00137-407-7. – Текст : непосредственный.

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.

2. 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.

3. Данилова, О. Т. Технические средства разведки и защита информации : учебное пособие : в 4 частях : [16+] / О. Т. Данилова ; Омский государственный технический университет. – Омск : Омский государственный технический университет (ОмГТУ), 2019. –

Вид Гуркова Е. В.

Часть 1. Технические каналы утечки речевой акустической конфиденциальной информации. – 64 с. : ил., табл., схем., граф. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=682094 (дата обращения: 04.03.2026). – Библиогр. в кн. – ISBN 978-5-8149-2839-9 (Ч. 1). – ISBN 978-5-8149-2838-2. – Текст : электронный.

4. 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.

5. 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.

6. Мансуров, Г. З. Право цифровой безопасности : учебник : [16+] / Г. З. Мансуров. – Москва : Директ-Медиа, 2022. – 148 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=687364 (дата обращения: 18.02.2026). – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – DOI 10.23681/687364. – Текст : электронный.

7. 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.

8. 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.

9. Правовая система Республики Беларусь: состояние, проблемы и перспективы развития : со. науч. ст. ГрГУ им. Янки Купалы ; редкол.: С. Е. Чебуранова (гл. ред.) [и др.]. - Гродно : ГрГУ. 2022. – 463 с.

10. 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.

11. 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.

12. Целых, А. Н. Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения : учебное пособие : [16+] / А. Н. Целых, Э. М. Котов ; Южный федеральный университет, Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону : Южный федеральный университет, 2023. – 118 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=713464 (дата обращения: 18.02.2026). – Библиогр. в кн. – ISBN 978-5-9275-4515-5. – Текст : электронный.

13. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2026. – 252 с. – (Профессиональное образование). – ISBN 978-5-534-20154-3.

14. Программно-аппаратные средства обеспечения информационной безопасности : лабораторный практикум : [16+] / Р. А. Филиппов, Л. Б. Филиппова, Ю. А. Леонов [и др.]. – Москва ; Берлин : Директ-Медиа, 2020. – 128 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700563 (дата обращения: 18.12.2025). – Библиогр. в кн. – ISBN 978-5-4499-1762-1. – DOI 10.23681/700563. – Текст : электронный.

15. Стасышин, В. М. Базы данных. Лекции по курсу: учебное пособие: В 4 ч. / В. М. Стасышин, Т. Л. Стасышина. – Новосибирск: Изд-во НГТУ. 2021. – 2025.

Нормативные источники:

1. 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: 19.03.2025.

2. 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: 19.03.2025.

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

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

5. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (с изм. и доп. Закона Республики Беларусь от 1 июня 2022 г. № 175-З).

6. Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное приказом ОАЦ от 20 февраля 2020 г. № 66.

7. Приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 12 «О классификации информационных ресурсов (систем)».

8. Приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 г. № 13 «Об уведомлении о нарушениях систем защиты персональных данных».

9. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 1 июня 2022 г. № 94 «О государственном информационном ресурсе «Реестр операторов персональных данных».

10. Указ Президента Республики Беларусь от 28 октября 2021 г. № 422 (с изм. и доп. Указа Президента Республики Беларусь от 5 февраля 2024 г. № 46) «О мерах по совершенствованию защиты персональных данных».

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

12. 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.

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

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

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

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

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

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

19. 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.

20. 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.

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

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

23. СТБ 2659-2024. «Умный город». Структура «умных городов» (введен в действие с 1 февраля 2025 г.)

24. СТБ ISO/IEC 27005-2024. Информационная безопасность, кибербезопасность и защита конфиденциальности.

Электронные ресурсы:

1. Национальный правовой портал Республики Беларусь. [Электрон, ресурс]. – http://www.pravo.by. – Дата доступа: 19.03.2025.

2. Научно-исследовательский институт технической защиты информации. [Электрон, ресурс]. – Режим доступа: http://www.niitzi.by. – Дата доступа: 19.03.2025.

3. Национальный центр интеллектуальной собственности. [Электрон, ресурс]. – Режим доступа: http://www.belgospatent.org.by. – Дата доступа: 19.03.2025.

4. Оперативно-аналитический центр при Президенте Республики Беларусь [Электрон, ресурс]. – Режим доступа: http://oac.gov.by. – Дата доступа: 19.03.2025.

5. Министерство связи и информатизации Республики Беларусь. [Электрон, ресурс]. – Режим доступа: http://www.mpt.gov.by. – Дата доступа: 19.03.2025.

6. Государственный комитет по стандартизации. [Электрон, ресурс]. – Режим доступа: http://www.gosstandart.goy.by. – Дата доступа: 19.03.2025.

7. 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: 19.03.2025.

8. Отчеты о деятельности. – Национальный центр защиты персональных данных Республики Беларусь (cpd.by) – Режим доступа: https://cpd.by/o-centre/otchety-o-dejatelnosti/– Дата доступа: 17.11.2025.

ПЕРЕЧЕНЬ ЛАБОРАТОРНЫХ ЗАНЯТИЙ

6 семестр

Лабораторная работа №1 Методы работы с PowerShell.

Лабораторная работа №2 Построение регулярных выражений.

Лабораторная работа №3 Изучение базовых команд Windows.

Лабораторная работа №4 Изучение базовых команд Linux.

Лабораторная работа №5 Разграничение прав пользователей в защищенных версиях операционной системы Windows.

Лабораторная работа №6 Изучение механизмов управления доступа к ресурсам, прав доступа в операционной системе Linux.

Лабораторная работа №7 Реализация политики безопасности в защищенных версиях операционной системы Windows.

Лабораторная работа №8 Реализация политики безопасности в операционной системе Linux.

Лабораторная работа №9 Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности, при использовании глобальных вычислительных сетей.

Лабораторная работа №10 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.

Лабораторная работа №11 Сброс пароля пользователя в операционной системе Windows.

Лабораторная работа №12 Сброс пароля пользователя на ядре Linux.

Лабораторная работа №13 Обеспечение целостности и доступности данных с использованием избыточного массива независимых жестких дисков Raid и менеджера логических томов LVM.

Лабораторная работа №14 Работа с программным межсетевым экраном VIPNet Office Firewall.

Лабораторная работа №15 Практические навыки работы сканирования сети с помощью Honeypot, Nmap.

Лабораторная работа №16 Работа с частными виртуальными сетями.

Лабораторная работа №17 DDoS (Distributed Denial of Service) – основные особенности их организации и защиты от них.

Семестр 7

Лабораторная работа №1 Методики работы антивирусных программ.

Лабораторная работа №2 Работа с антивирусом «Kaspersky Antivirus».

Лабораторная работа №3 Работа с антивирусом «Безопасность Windows».

Лабораторная работа №4 Работа с антивирусами в Linux.

Лабораторная работа №5 Работа с брандмауэром в Windows.

Лабораторная работа №6 Работа с песочницами и файловыми антивирусами Sandbox.

Лабораторная работа №7 Получение практических навыков программного восстановления данных при помощи программ TestDisk, PhotoRec, Extundelete, Foremost.

Лабораторная работа №8 Работа с программой электронно-цифровой подписи pgp.

Лабораторная работа №9 Создание и установка контролера домена с использованием технологии Active Directory.

Лабораторная работа №10 Защита почтового сервера от спама при помощи Anti-Spam SMTP Proxy (ASSP).

Лабораторная работа №11 Защита с помощью систем обнаружения и предотвращения вторжений при помощи NIPS/NIDS: Snort.

Лабораторная работа №12 Шифрование/дешифрование данных при помощи программ PGP, GPG, Шифрование данных «на лету» при помощи TrueCrypt. Спецификация шифрования диска LUCKS/dm-crypt.

Лабораторная работа №13 Методы и модели оценки уязвимостей. Стандарт CVSS.

Лабораторная работа №14 Практически работа с SIEM (Security information and event management): SIM – Security Information Management – управление информационной безопасностью SEM – Security Event Management – управление событиями безопасности.

Лабораторная работа №15 Инженерно-техническая защита информации. Оценка первичных признаков элементов речевого сигнала.

Лабораторная работа №16 Инженерно-техническая защита информации. Создание маскирующего шума для имитации виброакустического зашумления.

Лабораторная работа №17 Инженерно-техническая защита информации. Применение маскирующего шума для имитации виброакустического зашумления.

Лабораторная работа №18 Инженерно-техническая защита информации. Мероприятия по выявлению каналов утечки информации (специальные проверки, специальные обследования, специальные исследования).

ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

1. Виртуальные частные сети.
2. Деструктивные возможности современных вредоносных программ.
3. Защита персональных данных.
4. Инструменты проверки целостности содержимого дисков.
5. Исторические события факты в области информационной безопасности.
6. Компьютерная стеганография в нашей жизни.
7. Понятие SQL-инъекции и меры борьбы.
8. Порядок действий в случае несанкционированного взлома вашего аккаунта.
9. Приемы безопасного использования личной и корпоративной электронной почты.
10. Приемы навыки безопасного использования мобильных устройств.
11. Примеры использования электронной цифровой подписи в Республике Беларусь.
12. Примеры стандартизированных кодов банков, супермаркетов и других крупных подсистем экономики.
13. Системы обнаружения уязвимостей сетей и анализаторы сетевых атак.
14. Современные криптосистемы.
15. Средства антивирусной защиты.
16. Средства идентификации и аутентификации пользователей (комплекс 3А).
17. Средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям.
18. Существующие в мире механические системы защиты.
19. Цифровая грамотность: что необходимо знать при использовании паролей.
20. Законодательное и нормативно-правовое регулирование в сфере информационной безопасности в Республике Беларусь.
21. Противодействие киберпреступности и противодействие мошенничеству в Республике Беларусь.
22. Искусственный интеллект, как инструмент кибербезопасности.
23. Безопасность цифровых платформ.
24. Триада ИБ: конфиденциальность, целостность и доступность как фундамент защиты данных.
25. Виды современных кибератак и методы их классификации.
26. Социальная инженерия как один из самых эффективных методов взлома.
27. Человеческий фактор как угроза информационной безопасности.
28. Сравнительный анализ межсетевых экранов (Firewalls) и систем обнаружения вторжений (IDS/IPS).
29. Особенности защиты данных в облачных инфраструктурах и концепция Cloud Security.
30. Уязвимости интернета вещей и способы защиты «умных» устройств.
31. Как искусственный интеллект помогает в защите информационных ресурсов и как его используют хакеры.
32. Постквантовая криптография и будущее защиты данных.
33. Внедрение практик безопасности в процесс создания программного обеспечения.
34. Применение блокчейна для обеспечения целостности и защиты информации.
35. Принципы работы современных антивирусов и борьба с угрозами нулевого дня.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

6 семестр

1. Цели и задачи изучения дисциплины. Основные понятия и определения.
2. Отличительные черты информационного общества. В чем заключается проблема информационной безопасности?
3. Основные понятия информационной безопасности. Что понимается под «компьютерной безопасностью»?
4. Информационные технологии и необходимость информационной безопасности.
5. Система защиты информации и ее структуры. Система показателей, характеризующих информацию. Качество информации и его обеспечение.
6. Положения государственной политики информационной безопасности Республики Беларусь. Государственная система защиты Республики Беларусь.
7. Государственное регулирование информационной безопасности в Республике Беларусь.
8. Государственные органы и учреждения, занимающиеся вопросами информационной безопасности в Республики Беларусь.
9. Идентификация, аутентификация, управление доступом.
10. Защита от несанкционированного доступа.
11. Методологические основы защиты информации.
12. Парадигма информационной безопасности.
13. Обзор и сравнительный анализ стандартов информационной безопасности.
14. Экономическая информация как товар и объект безопасности.
15. Ключевые термины: понятие ущерб, угроза, уязвимость.
16. Внутренние и внешние угрозы. Угрозы безопасности информационно-коммуникационных технологий.
17. Система дестабилизирующих факторов, влияющих на уязвимость информации.
18. Основные методы реализации угроз.
19. Каналы несанкционированного доступа к информации.
20. Уязвимость информации и информационных систем.
21. Способы воздействия информационных угроз на объекты.
22. Внешние и внутренние субъекты информационных угроз.
23. Информационные угрозы, их виды и причины возникновения.
24. Информационные угрозы для государства.
25. Информационные угрозы для компании.
26. Информационные угрозы для личности (физического лица).
27. Общая характеристика нормативно-правовых актов в сфере обеспечения защиты персональных данных.
28. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
29. Персональные данные и их защита.
30. Меры по обеспечению безопасности персональных данных при их обработке.
31. Ответственность за нарушение законодательства о персональных данных.
32. Особенности обработки биометрических персональных данных.
33. Действия и события, нарушающие информационную безопасность.
34. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
35. Компьютерные преступления и их классификация.
36. Исторические аспекты компьютерных преступлений и современность.
37. Субъекты и причины совершения компьютерных преступлений.
38. Законы в сфере информатизации и информационной безопасности в Республике Беларусь.
39. Уголовно-правовой контроль над компьютерной преступностью в Республике Беларусь.
40. Вредоносные программы, их виды. История компьютерных вирусов и современность.

41. Политика безопасности и ее принципы.
42. Законодательный уровень информационной безопасности. Обзор белорусского и российского законодательств.
43. Понятие политики безопасности.
44. Основные типы и содержание политик безопасности.
45. Принципы государственной политики обеспечения информационной безопасности.
46. Система защиты государственной тайны.
47. Методы и средства защиты информации.
48. Организационное обеспечение информационной безопасности.
49. Организация конфиденциального делопроизводства.
50. Организационно-экономическое обеспечение информационной безопасности.
51. Инженерно-техническое обеспечение компьютерной безопасности.
52. Организационно-правовой статус службы безопасности.
53. Этапы и освоение защиты информации экономических объектов.
54. Криптографические методы защиты информации.
55. Менеджмент и аудит информационной безопасности на уровне предприятия.
56. Аудит информационной безопасности автоматизированных банковских систем.
57. Аудит информационной безопасности электронной коммерции.
58. Информационная безопасность предпринимательской деятельности.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЭКЗАМЕНА

7 семестр

1. История развития систем защиты информации в зарубежных странах.
2. Развитие средств и методов защиты информации.
3. Этапы развития системы защиты информации в настоящее время.
4. Структура систем защиты информации, применяемых в общемировой практике обеспечения информационной безопасности.
5. Современная концепция информационной войны в США.
6. Правовое регулирование информационной безопасности в США.
7. Государственные органы обеспечения национальной безопасности США.
8. Состояние проблемы информационной безопасности в странах Евросоюза.
9. Системы защиты информации в Соединённом королевстве Великобритании и Северной Ирландии.
10. Системы защиты информации в Федеративной республике Германия.
11. Системы защиты информации во Французской республике.
12. Системы защиты информации в Швеции. «Великая стена» информационной безопасности Китае.
13. Деятельность международных организаций в сфере информационной безопасности.
14. Развитие международного сотрудничества в области информационной безопасности.
15. Международные организации в области информационной безопасности.
16. Правовое регулирование сети Интернет. Защита информации в Интернете. Электронная почта и ее защита.
17. Задачи информационной безопасности в программе «цифровая экономика».
18. Доктрина информационной безопасности в Республике Беларусь.
19. Предпосылки создания стандартов информационной безопасности.
20. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии европейских стран.
21. Международные стандарты информационной безопасности.
22. Методы и средства защиты данных, основанные на использовании криптографии.
23. Основные стандарты, применяемые в программных средствах шифрования данных (AES, belt, ГОСТ 28147).
24. Аппаратные средства защиты данных на примере использования переносимых устройств хранения данных (flash-накопителей).
25. Программные и аппаратные средства защиты данных от копирования. Примеры.
26. Информационная безопасность вычислительных средств с использованием современных операционных систем,
27. Информационная безопасность вычислительных средств с использованием систем управления базами данных и языков программирования.
28. Понятие Firewall и их использование.
29. Информационная безопасность и защита данных с использованием мобильных устройств их хранения.
30. Администрирование операционных систем в контексте обеспечения безопасности.
31. Методы разграничение доступа.
32. Модели защиты информации. Модель Харрисона-Рузо-Ульмана.
33. Модели защиты информации. Модель Белла-ЛаПадулы.
34. Модели защиты информации. Модель Биба и Кларка-Уилсона.
35. Ролевая модель безопасности.
36. Структура профиля защиты. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISI/IEC 15408.
37. Управление жизненным циклом информационных систем.
38. Технологии обеспечения доступности, целостности и подлинности, конфиденциальности информации, информационных ресурсов и информационных систем.

39. Понятие информации. Кто относится к потребителям и обладателям информации?
40. Составляющие информационной безопасности.
41. Определение доступности информации, целостности информации, конфиденциальности информации.
42. Методы исследования проблем защиты информации.
43. Общеметодологические принципы построения систем защиты информации.
44. Модели разграничения доступа к информации.
45. Методики построения систем защиты информации.
46. Построение системы защиты информации. Модель Lifecycle Security.
47. Модель многоуровневой защиты.
48. Методика управления рисками, предлагаемая Microsoft.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Обучение дисциплине «Безопасность информационных систем» 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;

– наличием и полной доступностью электронных вариантов курса лекций и учебно-методических указаний по основным разделам дисциплины на https://moodle.psu.by – образовательном портале Полоцкого государственного университета имени Евфросинии Полоцкой.

Дополнительное учебно-методическое обеспечение самостоятельной работы студентов очной формы обучения

1. Материалы, размещены на бесплатном сервисе для учебных заведений, некоммерческих организаций и пользователей личных аккаунтов Google – Google Класс: шифр курса **FELCBLPN**.
2. Материалы, размещённые на образовательном портале Полоцкого государственного университета имени Евфросинии Полоцкой **https://moodle.psu.by**.
3. Методические указания к выполнению лабораторных работ по дисциплине «Безопасность информационных систем» для студентов специальности 6-05-0533-12 «Кибербезопасность».

Содержание самостоятельной работы студентов (дневная форма получения высшего образования)

6 семестр

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины	*Тема 2.2. Методы реализации угроз.* Система дестабилизирующих факторов, влияющих на уязвимость информации. Методология формирования полного множества угроз. Осн. лит.: [1], [2]. Доп. лит.: [2], [4], [5].	2
	Тема 3.2 Правовое регулирование защиты персональных данных в Республике Беларусь Роль правового регулирования в обеспечении информационной безопасности. Категории персональных данных. Защита персональных данных. Законодательство и нормативные акты. Осн. лит.: [1], [2], [4]. Доп. лит.: [6], [8], [9]. Норм.: [3], [4], [5], [6], [7], [8], [9], [10].	2
	Тема 4.2. Политика информационной безопасности. Принципы государственной политики обеспечения информационной безопасности. Система защиты государственной тайны. Осн. лит.: [1], [2]. Доп. лит.: [4], [5].	2
Подготовка к защите отчетов по лабораторным работам	*Лабораторная работа №1* Методы работы с PowerShell.	2
	Лабораторная работа №2 Построение регулярных выражений.	2
	Лабораторная работа №3 Изучение базовых команд Windows.	2
	Лабораторная работа №4 Изучение базовых команд Linux.	2
	Лабораторная работа №5 Разграничение прав пользователей в защищенных версиях операционной системы Windows.	2
	Лабораторная работа №6 Изучение механизмов управления доступа к ресурсам, прав доступа в операционной системе Linux.	2
	Лабораторная работа №7 Реализация политики безопасности в защищенных версиях операционной системы Windows.	2
	Лабораторная работа №8 Реализация политики безопасности в операционной системе Linux.	2

1	2	3
Подготовка к защите отчетов по лабораторным работам	*Лабораторная работа №9* Изучение штатных средств операционной системы Windows, предназначенных для обеспечения информационной безопасности, при использовании глобальных вычислительных сетей.	2
	Лабораторная работа №10 Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows.	2
	Лабораторная работа №11 Сброс пароля пользователя в операционной системе Windows.	2
	Лабораторная работа №12 Сброс пароля пользователя на ядре Linux.	2
	Лабораторная работа №13 Обеспечение целостности и доступности данных с использованием избыточного массива независимых жестких дисков Raid и менеджера логических томов LVM.	2
	Лабораторная работа №14 Работа с программным межсетевым экраном VIPNet Office Firewall.	2
	Лабораторная работа №15 Практические навыки работы сканирования сети с помощью Honeypot, Nmap.	2
	Лабораторная работа №16 Работа с частными виртуальными сетями.	2
	Лабораторная работа №17 DDoS (Distributed Denial of Service) – основные особенности их организации и защиты от них.	2
	ИТОГО:	**40**

Содержание самостоятельной работы студентов (дневная форма получения высшего образования)

7 семестр

Вид самостоятельной работы	Тематическое содержание и используемые источники	Количество часов
1	2	3
Самостоятельное изучение отдельных вопросов по темам дисциплины	*Тема 2.1. Программные и аппаратные средства защиты данных в информационных системах* Методы и средства защиты данных, основанные на использовании криптографии. Стеганография. Основные стандарты, применяемые в программных средствах шифрования данных (AES, belt, ГОСТ 28147). Осн. лит.: [2]. Доп. лит.: [3], [15].	6
	Тема 2.2. Информационная безопасность вычислительных средств с использованием современных операционных систем, систем управления базами данных и языков программирования. Администрирование операционных систем в контексте обеспечения безопасности. Основы безопасности в Microsoft Windows (accounts, group policies, NTFS permission, audit). Различные аспекты безопасности баз данных, их администрирования: permission, roles, views and stored procedures. Осн. лит.: [2]. Доп. лит.: [3], [15].	6
	Тема 2.3. Информационная безопасность и защита данных с использованием мобильных устройств их хранения. Применение «переносимых устройств» (на примере Flash-устройств Transcend) для защиты от посягательств на доступ к конфиденциальным данным. «Беспроводная и мобильная» безопасность в сетях: GSM-security, Bluetooth-security. Осн. лит.: [2]. Доп. лит.: [3], [15].	6
	Тема 3.2. Методы исследования проблем защиты информации. Общая характеристика методов исследования и проблем защиты информации. Методология оценки защищенности. Осн. лит.: [2]. Доп. лит.: [3], [15].	6
	Тема 4.4 Звуковые сигналы. Звуковые сигналы. Пример создания гармонического и полигармонического сигнала. Основные характеристики гармонического сигнала. Энергетический спектр речевого сигнала. Осн. лит.: [6]. Доп. лит.: [3], [7], [10], [14].	6
	Тема 4.5 Применение шумов для маскирования речевых сигналов. Маскирование речевых сообщений. Основные характеристики шума. Синтез смеси гармонического сигнала и шума с заданным отношением сигнал/шум. Осн. лит.: [6]. Доп. лит.: [3], [7], [10], [14].	6

1	2	3
Подготовка к защите отчетов по лабораторным работам	*Лабораторная работа №1* Методики работы антивирусных программ.	2
	Лабораторная работа №2 Работа с антивирусом «Kaspersky Antivirus».	2
	Лабораторная работа №3 Работа с антивирусом «Безопасность Windows».	2
	Лабораторная работа №4 Работа с антивирусами в Linux.	2
	Лабораторная работа №5 Работа с брандмауэром в Windows.	2
	Лабораторная работа №6 Работа с песочницами и файловыми антивирусами Sandbox.	2
	Лабораторная работа №7 Получение практических навыков программного восстановления данных при помощи программ TestDisk, PhotoRec, Extundelete, Foremost.	2
	Лабораторная работа №8 Работа с программой электронно-цифровой подписи pgp.	2
	Лабораторная работа №9 Создание и установка контролера домена с использованием технологии Active Directory.	2
	Лабораторная работа №10 Защита почтового сервера от спама при помощи Anti-Spam SMTP Proxy (ASSP).	2
	Лабораторная работа №11 Защита с помощью систем обнаружения и предотвращения вторжений при помощи NIPS/NIDS: Snort.	2
	Лабораторная работа №12 Шифрование/дешифрование данных при помощи программ PGP, GPG, Шифрование данных «на лету» при помощи TrueCrypt. Спецификация шифрования диска LUCKS/dm-crypt.	2
	Лабораторная работа №13 Методы и модели оценки уязвимостей. Стандарт CVSS.	2
	Лабораторная работа №14 Практически работа с SIEM (Security information and event management): SIM – Security Information Management – управление информационной безопасностью SEM – Security Event Management – управление событиями безопасности.	2
	Лабораторная работа №15 Инженерно-техническая защита информации. Оценка первичных признаков элементов речевого сигнала.	2
	Лабораторная работа №16 Инженерно-техническая защита информации. Создание маскирующего шума для имитации виброакустического зашумления.	2

1	2	3
	Лабораторная работа №17 Инженерно-техническая защита информации. Применение маскирующего шума для имитации виброакустического зашумления.	2
	Лабораторная работа №18 Инженерно-техническая защита информации. Мероприятия по выявлению каналов утечки информации (специальные проверки, специальные обследования, специальные исследования).	2
Подготовка реферативного выступления		22
Систематизация полученных знаний при подготовке к экзамену		32
	ИТОГО:	**126**

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

6 семестр

Учебном планом специальности в качестве формы промежуточной аттестации по учебной дисциплине «Безопасность информационных систем» в **6 семестре** предусмотрен **зачет**. Оценка учебных достижений студента производится по десятибалльной шкале.

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, контрольные работы, письменные отчёты по лабораторным работам);

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

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

Лабораторный практикум предполагает выполнение и защиту лабораторных работ. Последнее занятие по лабораторному практикуму в семестре предусматривает выполнение и защиту зачетной работы и контрольное тестирование. По каждой лабораторной работе выдается индивидуальное задание. Отчет по лабораторной 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:

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_n) + (\text{КР}_1 + \text{КР}_2) + (\text{ЛР}_1 + \ldots + \text{ЛР}_m)}{(m + n + 2)},$$

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

n – количество тестов;

КР – контрольная работа;

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

m – количество лабораторных работ.

В таблице 1 представлены составляющие, формирующие отметку текущего контроля Т по дисциплине.

Таблица 1 – 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)**
Контрольная работа №1	*Тема 2.1. Угрозы информационной безопасности.* *Тема 2.2. Методы реализации угроз.* *Тема 2.3. Уязвимости информации и информационных систем.*	Предлагается три вопроса	Максимальная отметка 10 (десять) баллов

Продолжение таблицы 1

Контрольная работа №2	*Тема 4.2. Политика информационной безопасности* *Тема 4.3. Менеджмент информационной безопасности.*	Предлагается 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

Результат текущего контроля рассчитывается как округленное 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 зачета.

Заключение о *зачете* формируется по формуле:

$$З = k \cdot Т,$$

где k– весовой коэффициент текущего контроля;

Т – результат текущего контроля за семестр.

Весовой коэффициент k принимается равным 1.

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

Перевод отметки по зачету осуществляется по следующим правилам: отметка «зачтено» выставляется студентам, получившим от 4 до 10 баллов, отметка «не зачтено» выставляется студентам, получившим от 1 до 3 баллов.

7 семестр

Учебном планом специальности в качестве формы промежуточной аттестации по учебной дисциплине «Безопасность информационных систем» **в 7 семестре** предусмотрен **экзамен**. Оценка учебных достижений студента производится по десятибалльной шкале.

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, реферативные выступления);

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

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

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

Лабораторные работы предполагают выполнение и защиту. Последнее занятие каждой из активностей в семестре предусматривает выполнение и защиту зачётной итоговой работы. При выполнении лабораторных работ выдаётся индивидуальное задание. Отчёты по лабораторным работам представляются 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:

$$\text{Т} = \frac{(\text{КТ}_1 + \ldots + \text{КТ}_n) + (\text{ЛР}_1 + \ldots + \text{ЛР}_m) + (\text{КР}_1 + \text{КР}_2)}{(2 + n + m)},$$

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

n – количество тестов;

m – количество лабораторных работ.

$\text{ЛР}_1 + \ldots + \text{ЛР}_{1m}$ – отметки, выставленные по результатам защит лабораторных работ.

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

В таблице 1 представлены составляющие, формирующие отметку текущего контроля Т по дисциплине.

Таблица 1 – Составляющие отметки текущего контроля Т по дисциплине

Текущие контрольные мероприятия	**Содержание контрольного мероприятия – название раздела (темы)**	**Задания контрольного мероприятия**	**Отметка контрольных мероприятий** (КР), (КТ), (ЛР)
Контрольная работа №1	*Тема 1.3. Стандарты информационной безопасности.* *Тема 2.2. Информационная безопасность вычислительных средств с использованием современных операционных систем, систем управления базами данных и языков программирования.*	Предлагается ответить на вопросы	Максимальная отметка 10 (десять) баллов
Контрольная работа №2	*Тема 4.1 Классификация технических каналов утечки информации* *Тема 4.3. Технические средства защиты речевой информации.* *Тема 4.4 Звуковые сигналы.*	Предлагается ответить на вопросы.	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

Итоговая экзаменационная отметка (ИЭ) учитывает отметку по результатам текущего контроля (Т) и экзаменационную отметку (Э). Весовой коэффициент к принимается равным 0,5. Информация о весовом коэффициенте доводится до студентов на первом занятии в семестре. Составляющие для формирования итоговой отметки по дисциплине и их весовые коэффициенты представлены в таблице 2.

Таблица 2 – Составляющие итоговой отметки по дисциплине

Составляющие (ИЭ)	*k*	Т	*1-k*	Э
	0,5	Представлены в таблице 1	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 «Безопасность 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 «Безопасность информационных систем» 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 лабораторных 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 лабораторных 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, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу
«Программно-аппаратные и технические средства защиты информации»	Кафедра математики и компьютерной безопасности	нет	
«Методы и стандарты оценки защищенности компьютерных систем»		нет	
«Технологии и безопасность интернета вещей»		нет	
«Криптографические протоколы»		нет	
«Криптографический инжиниринг»		нет	

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

РЕЦЕНЗИЯ
на учебную программу учреждения высшего образования
по учебной дисциплине «Безопасность информационных систем»
для специальности 6-05-0533-12 «Кибербезопасность»,
подготовленную к.т.н., доцентом Бураченок И.Б.

Разработанная учебная программа составлена на основе учебного плана специальности 6-05-0533-12 «Кибербезопасность» дневной формы получения высшего образования. Программа оформлена в соответствии с предъявляемым к высшей школе требованиями. В пояснительной записке отражены основные цели и задачи, указаны требования к уровню освоения и содержание учебной дисциплины, а также набор компетенций, соответствующих присваиваемой по завершению высшего образования квалификации «специалист по кибербезопасности», обеспечивающих выпускникам по указанной специальности успешность применения полученных знаний и умений в результате изучения дисциплины «Безопасность информационных систем» в дальнейшей профессиональной деятельности. Также в программе представлен тематический план, теоретические сведения, основные знания и умения по темам, перечень практических работ, сведения о самостоятельной работе студентов, литературные источники. Программа предполагает использование материалов и контрольных тестов, размещённых на образовательном портале Полоцкого государственного университета имени Евфросинии Полоцкой https://moodle.psu.by, которые доступны студентам через Интернет в любое удобное для них время.

В учебной программе реализованы дидактические принципы обучения: целостность, структурность, учтены метапредметные связи, особенности обучения по специальности 6-05-0533-12 «Кибербезопасность». Разработанная программа реализует подход, основанный на максимально возможном использовании внутренней и учебной мотивации студента. Программой предусмотрено закрепление знаний, полученных на лекционных занятиях с использованием проблемного обучения. Также предлагается внедрение активных методов обучения в рамках лабораторных работ.

Учебная программа рассчитана на два семестра – 306 часов (из которых 140 часов аудиторной работы, в том числе 70 часов лекционных занятий и 70

часов лабораторных работ, на самостоятельную работу предусмотрено 166 часов). Дисциплина разбита на 8 модулей, логически связанных по содержанию.

Критерии оценки знаний студентов изложены в общем плане и адаптированы к модульно-рейтинговой системе обучения.

Таким образом, рецензируемая программа заслуживает высокой оценки, она хорошо продумана и ориентирована на подготовку студентов к использованию полученных навыков в своей профессиональной деятельности. Вопросы, подлежащие изучению, позволят студентам сформировать системный взгляд на системное понимание проблем обеспечения безопасности в разрабатываемых, эксплуатируемых или сопровождаемых информационных системах, способность решать профессиональную задачу организации защиты информации и безопасного использования программных средств в вычислительных системах.

Программа учреждения высшего образования по учебной дисциплине «Безопасность информационных систем» соответствует уровню подготовки студентов в вузах и может быть рекомендована для использования в учебном процессе.

Зам. директора ОДО «Абсолют Интернет Системс» В.А. Бондаренко

РЕЦЕНЗИЯ
на учебную программу учреждения высшего образования
по учебной дисциплине «Безопасность информационных систем»
для специальности 6-05-0533-12 «Кибербезопасность»,
подготовленную к.т.н., доцентом Бураченок И.Б.

Представленная на рецензию учебная программа по учебной дисциплине «Безопасность информационных систем» для специальности 6-05-0533-12 «Кибербезопасность» соответствует учебному плану специальности – регистрационный №14-23/уч. ФКНЭ от 04.04.2023 г. для дневной формы получения высшего образования. Программа полностью соответствует предъявляемым к высшей школе требованиями. В пояснительной записке четко отражены основные цели и задачи, требования к уровню освоения, а также представлено содержание учебной дисциплины. Представленный набор компетенций, соответствует присваиваемой по завершению высшего образования квалификации «специалист по кибербезопасности». В программе представлена методическая карта, включающая теоретические сведения и перечень практических работ с указанием количества часов, отведенных на отдельные темы и разделы дисциплины. В программе также представлен план организации самостоятельной работы студентов и представлены литературные источники для самоподготовки. Программа предполагает использование образовательного портала Полоцкого государственного университета имени Евфросинии Полоцкой https://moodle.psu.by для размещения материалов по дисциплине и проведения контрольного тестирования.

Учебная программа рассчитана на два семестра, всего 306 часов (из которых 140 часов аудиторной работы, в том числе 70 часов лекционных занятий и 70 часов лабораторных работ, на самостоятельную работу предусмотрено 166 часов).

В учебной программе реализованы дидактические принципы обучения: целостность, структурность, учтены метапредметные связи, особенности обучения по специальности. Структура программы логична. Сначала

разбираются теоретические вопросы тем дисциплины, а затем полученные знания закрепляются на практических занятиях с использованием проблемного обучения. Также предлагается внедрение активных методов обучения в рамках практических работ для решения ситуационных задач.

Рецензируемая программа ориентирована на подготовку студентов к использованию полученных навыков в области безопасности информационных систем. Программа нацелена на подготовку специалистов в области информационной безопасности и защиты информационных систем, создания ими безопасных инфраструктур и аудиту компьютерно-коммуникационных сетей. Учебный материал ориентирован на формирование практических навыков, а ключевым элементом обучения является подход, основанный на максимальном использовании внутренней мотивации студента.

Программа учреждения высшего образования по учебной дисциплине «Безопасность информационных систем» соответствует уровню подготовки студентов в вузах и может быть рекомендована для использования в учебном процессе.

Технический директор
ООО «ТриИнком», к.т.н., доцент _____ К.Я. Раханов