БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Ректор Белорусского
государственного университета
_____А.Д.Король
15 июля 2024 г.
Регистрационный № 2506/б.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебная программа учреждения образования по учебной дисциплине для специальностей:

6-05-0533-12 Кибербезопасность

Профилизация: Компьютерная безопасность

2024 г.

Учебная программа составлена на основе ОСВО 6-05-0533-12-2023 и учебного плана №6-5.3-60/02 от 15.05.2023.

СОСТАВИТЕЛИ:

Колб О.О. - старший преподаватель кафедры технологий программирования факультета прикладной математики и информатики Белорусского государственного университета.

РЕЦЕНЗЕНТЫ:

В.М. Котов - заведующий кафедрой дискретной математики и алгоритмики Белорусского государственного университета, доктор физико-математических наук, профессор.

А.В. Федчук – инженер-программист ООО «Ювеком Системы».

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования БГУ
(протокол № 18 от 16.05.2024)

Научно-методическим советом БГУ
(протокол № 9 от 28.06.2024)

Заведующий кафедрой
технологий программирования _____ А.Н. Курбацкий

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Теоретические основы информационной безопасности» знакомит студентов с основами защиты информации, методами и средствами обеспечения информационной безопасности, а также с правовыми и организационными аспектами в данной области. Особое внимание уделяется основным концепциям информационной безопасности, таким как конфиденциальность, целостность и доступность данных. В рамках изучения дисциплины студенты знакомятся с методами анализа рисков, моделями угроз и уязвимостей, а также с некоторыми современными криптографическими технологиями. При изучении учебной дисциплины также рассматриваются основные этапы процесса обеспечения информационной безопасности, включая анализ и оценку рисков, разработку политик безопасности, мониторинг и аудит информационных систем. Дисциплина «Теоретические основы информационной безопасности» ориентирована на обучение студентов базовым знаниям, умениям и навыкам в области защиты информации. Изучаемые темы основываются на актуальной нормативной регулятивной базе и национальном законодательстве, а также на современных представлениях о процессах жизненного цикла информационных систем и парадигмах информационной безопасности.

Цели и задачи учебной дисциплины

Цель учебной дисциплины «Теоретические основы информационной безопасности» – формирование у студентов устойчивых теоретических знаний и некоторых практических навыков в области защиты информации, целостного представления о принципах и методах обеспечения информационной безопасности, а также умения применять полученные знания для решения прикладных задач в различных сферах деятельности. Дисциплина ориентирована на подготовку специалистов, способных создавать и исследовать защищенные информационные и компьютерно-коммуникационные системы.

Задачи учебной дисциплины:

1. Дать студентам базовые знания в области информационной безопасности.
2. Сформировать понимание основных концепций информационной безопасности, таких как конфиденциальность, целостность и доступность данных.
3. Изучить актуальную нормативную регулятивную базу и национальное законодательство в области информационной безопасности.
4. Изучить современные представления о процессах жизненного цикла информационных систем.
5. Исследовать основные этапы процесса обеспечения информационной безопасности, включая анализ и оценку рисков, разработку политик безопасности, мониторинг и аудит информационных систем.
6. Сформировать системное понимание проблем безопасности и путей их решения.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина относится к модулю «Безопасность информационных технологий» государственного компонента.

Дисциплина «Теоретические основы информационной безопасности» непосредственно связана с учебными дисциплинами: «Программно-аппаратные и технические средства защиты информации», «Компьютерная безопасность распределенных систем».

Требования к компетенциям

Освоение учебной дисциплины «Теоретические основы информационной безопасности» должно обеспечить формирование следующих компетенций:

Универсальные компетенции:

УК. Владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации.

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

УК. Работать в команде, толерантно воспринимать социальные, этнические, конфессиональные, культурные и иные различия.

УК. Быть способным к саморазвитию и совершенствованию в профессиональной деятельности.

УК. Проявлять инициативу и адаптироваться к изменениям в профессиональной деятельности

Базовые профессиональные компетенции:

БПК. Использовать основные понятия и нормативные правовые акты информационной безопасности для описания и классификации теоретических, правовых, организационных и инженерно-технических методов обеспечения конфиденциальности, целостности и доступности информации.

Сформированные при изучении дисциплины компетенции являются базовыми при освоении всех последующих дисциплин специализации, при выполнении курсовых и дипломных работ.

В результате изучения дисциплины студент должен:

знать:

– основные концепции информационной безопасности, такие как конфиденциальность, целостность и доступность данных;

– актуальную нормативную регулятивную базу и национальное законодательство в области информационной безопасности;

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

– основные этапы процесса обеспечения информационной безопасности;

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

уметь:

– обеспечивать конфиденциальность, целостность и доступность данных;

– анализировать и оценивать риски информационной безопасности;

– проводить исследования проблем информационной безопасности с использованием современных методов;

– применять полученные знания для решения прикладных задач в различных сферах деятельности;

– применять современные методы и средства для создания защищенных систем и их оценки;

иметь навык:

– анализа задач в области информационной безопасности с применением основных подходов;

– работы с информационными источниками и нормативными документами по вопросам информационной безопасности;

– применения базовых методов обеспечения информационной безопасности, включая средства криптографической защиты, защиту программного обеспечения и данных;

– обеспечения безопасности информации, обрабатываемой в компьютерных системах и информационно-телекоммуникационных сетях.

Структура учебной дисциплины

Дисциплина изучается в 3 семестре. В соответствии с учебным планом всего на изучение учебной дисциплины «Теоретические основы информационной безопасности» отведено для очной формы получения высшего образования 100 часов, в том числе 48 аудиторных часов (лекции – 30 часов, практические занятия – 18 часов). **Из них:**

Лекции – 30 часов, практические занятия – 16 часов, управляемая самостоятельная работа - 2 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Введение. Основы информационной грамоты. Информационное обеспечение деятельности.

Предмет, цели и задачи курса. Содержание дисциплины. Информационная безопасность и защита информации. Основные понятия. Термины и определения. Информация. Система показателей и качество информации.

Информационное обеспечение деятельности. Роль информационного обеспечения в бизнесе и управлении. Общая характеристика процессов сбора, передачи, обработки и накопления информации. Управление знаниями.

Тема 2. История развития технологий. Парадигма обеспечения информационной безопасности. Современные стандарты.

Исторические события, факты и персоналии. Возникновение и история развития проблемы защиты информации. Исторические примеры нарушений безопасности и их влияние на современные подходы. Парадигма информационной безопасности. Обзор и сравнительный анализ стандартов информационной безопасности.

Тема 3. Правовые и этические аспекты обеспечения информационной безопасности и защиты персональных данных.

Защита персональных данных. Законодательство и нормативные акты. Этические нормы и кодексы в области ИБ. Ответственность и юридические аспекты.

Тема 4. Основные характеристики безопасности и способы их обеспечения. Модели защиты информации.

Доступность, целостность и подлинность, конфиденциальность информации и информационных ресурсов. Методы и способы их защиты: правовые, организационно-административные, программно-технические. Модели Белла-ЛаПадулы, Биба и Кларка-Уилсона.

Тема 5. Угрозы и уязвимости информационной безопасности.

Угрозы безопасности информационно-коммуникационных технологий. Классификация умышленных угроз. Общая классификация угроз. Система дестабилизирующих факторов, влияющих на уязвимость информации. Методология формирования полного множества угроз. Основные методы реализации угроз. Причины, виды и каналы утечки информации. Уязвимость информации и информационных систем. Система показателей уязвимости. Классификация уязвимости. Методы и модели оценки уязвимостей. Стандарт CVSS.

Тема 6. Методы защиты информации и компьютерных систем.

Организационные и технические меры защиты. Принципы и методы защиты: принцип наименьших привилегий, принцип обязательной доступности.

Программные и программно-аппаратные средства защиты. Криптографические методы защиты и их реализация. Криптографические алгоритмы защиты информации. Базовые криптографические протоколы и функции хеширования.

Тема 7. 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 8. Методология оценки защищенности.

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

Тема 9. 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 информации. Общее содержание основных вопросов организации и обеспечения работ по защите информации.

Тема 10. Политика информационной безопасности.

Понятие политики безопасности. Основные типы и содержание политик безопасности.

Тема 11. Менеджмент информационной безопасности.

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

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения высшего образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1	Введение. Основы информационной грамоты. Информационное обеспечение деятельности	2						Дискуссия, экспресс-опрос
2	История развития технологий. Парадигма обеспечения информационной безопасности. Современные стандарты.	2	2					Экспресс-опрос, отчеты по практическим заданиям
3	Правовые и этические аспекты обеспечения информационной безопасности и защиты персональных данных.	2	2					Экспресс-опрос, доклад
4	Основные характеристики безопасности и способы их обеспечения. Модели защиты информации.	4	2					Доклад, электронный тест
5	Угрозы и уязвимости информационной безопасности.	2	2					Дискуссия, отчеты по практическим заданиям
6	Методы защиты информации и компьютерных систем.	4	2				2	Экспресс-опрос, доклад, дискуссия, контрольная работа
7	Технологии защиты информации, информационных	2	2					Экспресс-опрос, отчеты по практическим

	ресурсов, информационных систем.							заданиям
8	Методология оценки защищенности.	2						Дискуссия
9	Принципы построения систем защиты информации.	4	2					Коллоквиум
10	Политика информационной безопасности.	4	2					Экспресс-опрос, доклад, электронный тест
11	Менеджмент информационной безопасности.	2						Дискуссия
	Итого	**30**	**16**				**2**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Белоус, А. И. Основы кибербезопасности: стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 481 с.
2. Нестеров, С. А. Основы информационной безопасности: учебник / С. А. Нестеров. – Изд. 2-е, стер. – Санкт-Петербург ; Москва ; Краснодар : Лань, 2023. – 320 с. – URL: https://e.lanbook.com/book/370967.
3. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие для студ. высших учебных заведений, обуч. по направлению подготовки 10.03.01 "Информационная безопасность (квалификация (степень) "Бакалавр") / Ю. Н. Сычев. – Москва : ИНФРА-М, 2023. – 200 с. – URL: https://znanium.ru/catalog/product/1912987.
4. Щеглов, А. Ю. Защита информации: основы теории: учебник для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям. – Москва : Юрайт, 2020. – 309 с.

Дополнительная литература

1. Ашманов, И. Цифровая гигиена / И. Ашманов, Н. Касперская. – Санкт-Петербург ; Москва ; Минск : Питер, 2022. – 399 с.
2. Белоус, А. И. Кибероружие и кибербезопасность: о сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. – Москва ; Вологда : Инфра-Инженерия, 2020. – 690 с.
3. Вихорев, С. В., Сычев, А. М. Диалоги о безопасности информации, или введение в основы построения систем обеспечения безопасности информации: монография. – М.: Медиа Группа «Авангард», 2015. – 640 с.
4. Макконнелл, С. Совершенный код: мастер-класс. 2-е изд. – М.: Издательство «Русская редакция», 2017. – 896 с.
5. Насонова, Н. В., Пухир, Г. А., Петров, С. Н. Основы защиты информации: учеб.-метод. пособие для спец. I ступени высш. образования, закрепленных за УМО. – Минск : БГУИР, 2019. – 82 с.
6. Полещук, Д. Г. Уголовно-правовая охрана информационной безопасности: актуальные проблемы теории и практики. – Минск : Колорград, 2022. – 239 с.
7. Сёмкин, С. Н., Беляков, Э. В., Гребнев, С. В., Козачок, В. И. Основы организационного обеспечения информационной безопасности объектов информатизации. – М.: Гелиос АРВ, 2005. – 192 с.
8. Сикорски, М. Вскрытие покажет! Практический анализ вредоносного ПО / М. Сикорски, Э. Хониг ; [пер. с англ. С. Черников ; предисл. Р. Бейтлич]. – Санкт-Петербург ; Москва ; Минск : Питер, 2023. – 768 с. – URL: https://ibooks.ru/reading.php?short=1&productid=358154.

9. Ховард, М., Лебланк, Д., Вьега, Дж. 24 смертных греха компьютерной безопасности: как написать безопасный код. – М.: Издательство «Питер», 2010. – 400 с.

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

11. Энсон, С. Реагирование на компьютерные инциденты: прикладной курс = Applied Incident Response / С. Энсон ; [пер. с англ. Д. А. Беликова]. – Москва: ДМК Пресс, 2021. – 435 с.

12. Основы управления информационными рисками [Электронный ресурс]. – 2015. – Режим доступа: http://анализ-риска.рф. – Дата доступа 08.10.2024.

13. Национальный интернет-портал Республики Беларусь [Электронный ресурс] / Национальный центр правовой информации Республики Беларусь. – Минск, 2024. – Режим доступа: http://www.pravo.by. – Дата доступа 08.10.2024.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

1. Устная форма: экспресс-опрос, дискуссия.
2. Письменная форма: контрольные работы, коллоквиум.
3. Устно-письменная форма: доклад, отчеты по практическим заданиям.
4. Техническая форма: электронные тесты.

Критерием оценивания является выполнение заданий для управляемой самостоятельной работы и практических работ. Задания и практические работы по результатам выполнения и защиты оцениваются с учетом следующих основных параметров: своевременное выполнение работы; полнота и правильность ответов на вопросы, заданные в ходе защиты работы.

В случае выполнения данных условий студент имеет возможность сдавать зачет.

В качестве рекомендуемых технических средств диагностики используется обучение, организованное на платформе MS Moodle (https://edufpmi.bsu.by).

Формой промежуточной аттестации по дисциплине учебным планом предусмотрен **зачет.**

Для формирования итоговой отметки по учебной дисциплине используется модульно-рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущей и промежуточной аттестации студентов по учебной дисциплине.

Формирование итоговой отметки в ходе проведения контрольных мероприятий текущей аттестации (примерные весовые коэффициенты, определяющие вклад текущей аттестации в отметку при прохождении промежуточной аттестации):

- отчёты по практическим заданиям – 15 %;
- коллоквиум – 25 %;
- контрольные работы – 30 %;
- электронные тесты– 30%.

Итоговая отметка по дисциплине рассчитывается на основе итоговой отметки текущей аттестации (рейтинговой системы оценки знаний) 40 % и отметки на зачете 60 %.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Тема 6. Методы защиты информации и компьютерных систем (2 часа)

Организационные и технические меры защиты. Принципы и методы защиты: принцип наименьших привилегий, принцип обязательной доступности.

Программные и программно-аппаратные средства защиты. Криптографические методы защиты и их реализация. Криптографические алгоритмы защиты информации. Базовые криптографические протоколы и функции хеширования

Задание: Исследовать несколько реальных случаев кибератак (например, атаки на Target, Sony Pictures, Equifax). Описать типы использованных уязвимостей и предложить возможные методы защиты на основе изученных принципов информационной безопасности.

Форма контроля: доклад, дискуссия.

Примерная тематика практических занятий

Занятие № 1. Обзор и сравнительный анализ стандартов информационной безопасности.

Занятие № 2. Защита персональных данных.

Занятие № 3. Модели защиты информации.

Занятие № 4. Методы и модели оценки уязвимостей. Стандарт CVSS.

Занятие № 5. Базовые криптографические протоколы и функции хеширования.

Занятие № 6. Модели разграничения доступа информации.

Занятие № 7. Принципы построения систем защиты информации.

Занятие № 8. Политика информационный безопасности.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используются следующие методы:

– ***метод учебной дискуссии,*** который предполагает участие студентов в целенаправленном обмене мнениями, идеями для предъявления и/или Использование метода обеспечивает появление нового уровня понимания изучаемой темы, применение знаний (теорий, концепций) при решении проблем, определение способов их решения;

– ***метод группового обучения,*** который представляет собой форму организации учебно-познавательной деятельности обучающихся, предполагающую функционирование разных типов малых групп, работающих как над общими, так и специфическими учебными заданиями.

В качестве технических средств для организации работы в рамках учебной дисциплины рекомендуется использовать Образовательный портал БГУ (https://edufpmi.bsu.by) – инструмент с эффективной функциональностью контроля, тренинга и самостоятельной работы.

Методические рекомендации по организации самостоятельной работы

Для организации самостоятельной работы студентов по учебной дисциплине следует использовать современные информационные ресурсы: разместить на образовательном портале комплекс учебных и учебно-методических материалов (учебно-программные материалы, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно- программной документации, в том числе вопросы для подготовки к зачету, тесты, вопросы для самоконтроля и др., список рекомендуемой литературы, информационных ресурсов и др.).

Примерный перечень вопросов к зачету

1. Информация. Свойства информации.
2. Общая характеристика процессов сбора, передачи, обработки и накопления информации.
3. Качество информации и его обеспечение.
4. Система показателей, характеризующих информацию.
5. Системно-концептуальный подход.
6. Основные постулаты парадигмы безопасности. Постулаты.
7. Дать характеристику понятию «комплексная защита информации» и кратко раскрыть его содержание.
8. Архитектура защиты информации.
9. Основные принципы обеспечения информационной безопасности организации.
10. Модели управления доступом. Общая характеристика моделей.
11. Аутентификация.
12. Методы аутентификации.
13. Меры защиты информации.
14. Полномочное управление доступом (MAC).
15. Избирательное управление доступом (DAC).
16. Ролевое управление доступом (RBAC).
17. Модель зрелости организации в области информационной безопасности.
18. Угрозы информационной безопасности. Виды их классификации.
19. Методы реализации угроз информационной безопасности ИС.
20. Уязвимости ИС. Причины их возникновения.
21. Классификация уязвимостей ИС
22. Оценка соответствия.
23. Объекты, цели, принципы и формы подтверждения соответствия
24. Методы исследования проблем защиты информации
25. Подтверждение соответствия. Сертификация.
26. Оценка соответствия. Аккредитация.

27. Современные представления об аудите информационной безопасности.
28. Принципы аудита.
29. Виды аудита информационной безопасности.
30. Этапы аудита информационной безопасности.
31. Результаты аудита информационной безопасности.
32. Риск ИБ. Менеджмент риска.
33. Управление рисками ИБ.
34. Оценка рисков. Преимущества и методики.
35. Функциональные компоненты безопасности по ОК.
36. Гарантийные компоненты безопасности по ОК.
37. Уровни гарантий оценки по ОК.
38. Жизненный цикл ИС.
39. Дестабилизирующие факторы, влияющие на уязвимость информации.
40. Управление инцидентами информационной безопасности.
41. Методы и способы защиты информации
42. Политика информационной безопасности
43. Основные типы и содержание политик безопасности.
44. Системы менеджмента безопасности информации.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

Название учебной 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 (с указанием даты и номера протокола)
Программно-аппаратные и технические средства защиты информации	Кафедра технологий программирования	Предложения отсутствуют	Рекомендовать к утверждению учебную программу (протокол № 18 от 16.05.2024)

Заведующий кафедрой
д.т.н., профессор _____ А.Н. Курбацкий

16.05.2024

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УО

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры

_____(протокол № ____ от _____ 202_ г.)

(название кафедры)

Заведующий кафедрой

_____ _____

(ученая степень, ученое звание) (И.О.Фамилия)

УТВЕРЖДАЮ

Декан факультета

_____ _____

(ученая степень, ученое звание) (И.О.Фамилия)