БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Ректор Белорусского
государственного университета
_____ А.Д.Король
10 июня 2024 г.
Регистрационный №УД-13138/уч.

ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Учебная программа учреждения образования
по учебной дисциплине для специальностей:

1-98 01 01 Компьютерная безопасность (по направлениям)

Направление специальности:
1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)

2024 г.

Учебная программа составлена на основе ОСВО 1-98 01 01-2021, учебного плана №Р98-1-206/уч. от 22.03.2022.

СОСТАВИТЕЛИ:

Курбацкий А.Н., заведующий кафедрой технологий программирования факультета прикладной математики и информатики Белорусского государственного университета, доктор технических наук, профессор.

РЕЦЕНЗЕНТ:

Листопад Н.И., доктор технических наук, профессор, заведующий кафедрой информационных радиотехнологий БГУИР.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования БГУ
(протокол № 18 от 16.05.2024);

Научно-методическим советом БГУ
(протокол № 8 от 31.05.2024).

Заведующий кафедрой _____ А.Н.Курбацкий

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель преподавания дисциплины «Введение в информационную безопасность» является введение в обширную проблематику информационной безопасности, охватывает программно-технические, теоретические, организационно-методические, правовые аспекты обеспечения информационной безопасности. Является платформой для дальнейшего углубленного изучения базовых дисциплин специальности «Компьютерная безопасность».

Задачи учебной дисциплины:

– дать студентам базу, необходимую для успешного усвоения материала дисциплин специализации;

– дать студентам базу, необходимую для успешного освоения современных тенденций в сфере информационной безопасности;

– получить знания, необходимые им в дальнейшем для успешной работы в качестве специалистов по защите информации и руководителей проектами в области IT.

Место учебной дисциплины

Учебная программа по дисциплине специализации «Введение в информационную безопасность» разработана в соответствии с учебным планом и образовательными стандартами первой ступени высшего образования по специальности 1-98 01 01 Компьютерная безопасность.

Учебная дисциплина относится к дисциплинам специализации компонента учреждения высшего образования.

Основой для изучения являются следующие курсы: «Промышленное программирование» модуля «Программирование» государственного компонента, «Операционные системы» модуля «Информатика и компьютерные системы» государственного компонента, «Теоретические основы информационной безопасности» государственного компонента.

Материал, излагаемый в курсе, используется при изучении ряда дисциплин специальности: «Методы оптимизации» модуля «Математические методы принятия решений» компонента учреждения высшего образования, «Криптографические методы» модуля «Криптография» компонента учреждения высшего образования.

Требования к компетенциям

Освоение учебной дисциплины «Введение в информационную безопасность» 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. Проявлять инициативу и адаптироваться к изменениям в профессиональной деятельности.

Базовые профессиональные компетенции

БПК. Строить, анализировать и тестировать алгоритмы и программы решения типовых задач обработки информации с использованием структурного, объектно-ориентированного и иных парадигм программирования.

Специализированные компетенции

СК. Решать профессиональные задачи с использование правовых знаний в сфере информационной и компьютерной безопасности

СК. Применять навыки проектирования и реализации систем безопасности, осуществлять выбор подходящего криптографического метода защиты типа данных и его реализации.

В результате изучения учебной дисциплины студент должен

знать:

– общепринятые принципы ИБ;
– классические и современные тенденции в развитии ИБ;
– анализ угроз, причины утечки информации;
– криптографические методы защиты ИБ
– организационно-методическое и правовое обеспечение ИБ;
– комплексное обеспечение ИБ автоматизированных систем, сложных интегрированных систем.

уметь:

– осуществлять разработку и поддержку ПО;
– определять причины и виды утечки и искажения информации, устранять возникающие в процессе разработки ПО проблемы;
– быть в курсе новых разработок по ИБ, быстро адаптироваться к постоянно изменяющимся угрозам.

владеть:

– базовыми знаниями по защите информации;
– определять подходы к выбору средств защиты информации;
– навыками работы с системами защиты конфиденциальной информации.

Структура учебной дисциплины.

Дисциплина изучается в пятом семестре. Всего на изучение учебной дисциплины «Введение в информационную безопасность» отведено:

– для очной формы получения высшего образования – 108 учебных часа, в том числе 68 часов аудиторных занятий, из которых лекционных - 34 часа, лабораторные занятия – 30 часов, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетных единиц.

Форма промежуточной аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Информационная безопасность (ИБ) в системе национальной безопасности

Понятие национальной безопасности, виды безопасности.

Тема 2. Общеметодологические принципы теории ИБ

Основные понятия ИБ, краткая характеристика теории ИБ, общеметодологические принципы.

Тема 3. Анализ объектов ИБ

Объекты ИБ, критерии их классификации, анализ.

Тема 4. ИБ государства, корпорации, личности

Общность и различия ИБ государства, корпорации, личности.

Тема 5. Анализ угроз ИБ

Понятие угроз, критерии их классификации. Роль ИИ в анализе угроз ИБ.

Тема 6. Методы и средства обеспечения ИБ

Методы, средства, их классификация. Возрастание роли ИИ.

Тема 7. Методы нарушения конфиденциальности, целостности, доступности информации

Конфиденциальность, целостность, доступность информации, нарушение этих свойств.

Тема 8. Причины, виды, каналы утечки и искажения информации

Утечка информации, каналы утечки информации, искажение информации, каналы искажения.

Тема 9. Теоретические основы компьютерной безопасности

Формальные модели. Модели безопасности. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Тема 10. Организационно-методическое обеспечение информационной безопасности

Анализ и оценка угроз информационной безопасности объекта.

Тема 11. Правовое обеспечение информационной безопасности

Законодательство в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.

Понятие и виды защищаемой информации по законодательству. Государственная тайна как особый вид защищаемой информации.

Тема 12. Криптографические методы защиты информации

История криптографии. Характер криптографической деятельности. Простейшие шифры и их свойства. Виды информации, подлежащие закрытию, их модели и свойства.

Тема 13. Программно-аппаратные средства обеспечения информационной безопасности

Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем. Методы и средства ограничения доступа к компонентам вычислительных систем.

Тема 14. Комплексное обеспечение информационной безопасности сложных интегрированных систем

Постановка проблемы комплексного обеспечения информационной безопасности сложных интегрированных систем. Роль ИИ в комплексном обеспечении ИБ сложных интегрированных систем.

Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы, технология, управление. Методология формирования задач защиты.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная форма получения высшего образования с применением дистанционных образовательных технологий (ДОТ)

№п/п	Название темы	Количество часов					Количество часов УСР	Форма контроля знаний
		Аудиторные						
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	Информационная безопасность (ИБ) в системе национальной безопасности	2			2			Устный опрос
2.	Общеметодологические принципы теории ИБ	2			2			Устный опрос
3.	Анализ объектов ИБ	2			2			Отчёт по лабораторной работе
4.	ИБ государства, корпорации, личности	2			2			Устный опрос
5.	Анализ угроз ИБ	2			2			Отчёт по лабораторной работе
6.	Методы и средства обеспечения ИБ	2			2			Отчёт по лабораторной работе
7.	Методы нарушения конфиденциальности, целостности, доступности информации	4			4			Контрольная работа
8.	Причины, виды, каналы утечки и искажения информации	2			2			Отчёт по лабораторной работе
9.	Теоретические основы компьютерной безопасности	2			2			Отчёт по лабораторной работе
10.	Организационно-	2			2			Отчёт по

	методическое обеспечение информационной безопасности							лабораторной работе
11.	Правовое обеспечение информационной безопасности	4			2		2	Контрольная работа
12.	Криптографические методы защиты информации	2			2			Отчёт по лабораторной работе
13.	Программно-аппаратные средства обеспечения информационной безопасности	2			2			Коллоквиум
14.	Комплексное обеспечение информационной безопасности сложных интегрированных систем	4			2		2	Проект
ИТОГО		34			30		4	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Душкин Р.В. Искусственный интеллект – М.: ДМК Пресс, 2019. – 280 с.
2. Ашманов И.С., Касперская Н.И. Цифровая гигиена – Спб.: Питер, 2022. – 400 с.
3. Баланов А.Н. Комплексная информационная безопасность. Учебное пособие для СПО / А.Н Баланов. – Спб.: Лань, 2024. – 284 с.
4. Баланов А.Н. Защита информационных систем. Кибербезопасность. Учебное пособие для СПО / А.Н Баланов. – Спб.: Лань, 2024. – 84 с.
5. Галатенко В.А. Основы информационной безопасности, 2-ое издание. – М.: ИНТУИТ, 2004. – 264 с.
6. Родичев Ю. Нормативная база и стандарты в области информационной безопасности. – Спб.: Питер, 2017. – 256 с.
7. Шерстюк В.П. Научные и методологические проблемы информационной безопасности. – М.: МЦНМО, 2005. – 208 с.
8. Казарин О.В. Методология защиты программного обеспечения. – М.: МЦНМО, 2009. – 464 с.
9. Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.
10. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М., ДМК Пресс, 2012. – 592 с.
11. Проскурин В., Защита программ и данных. – М.: Академия, 2012. – 208 с.

Дополнительная литература

1. Krause M., Tipton H.F. Handbook of information Security Management. – CRC Press LLC. – www.cccure.com
2. The Red Book: A Roadmap for Systems Security Research. Seventh framework programme.- The SysSec Consortium. – www.syssec-project.eu
3. Boran S. IT Security CookBook. – www.boran.com/security
4. Указ Президента Республики Беларусь № 575 от 9 ноября 2010 г. «Об утверждении Концепции национальной безопасности Республики Беларусь. – www.pravo.by

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Объектом диагностики компетенций студентов являются знания, умения, практический опыт, полученные ими в результате изучения учебной дисциплины. Выявление учебных достижений студентов осуществляется с помощью мероприятий текущего контроля и промежуточной аттестации.

Текущий контроль работы студента проходит в следующих формах:

- технические: лабораторные работы, выполняемые на компьютере. Они оцениваются исходя из читаемости и оптимизации программного кода;
- устно-письменные: устная и/или письменная (в виде отчёта) защита лабораторных работ, оцениваемая на основе полноты и последовательности ответа (отчёта), полноты раскрытия содержания выполненного задания, понимания работы алгоритмов и методов, использованных при выполнении задания, контрольная работа, проект;
- устные: устные опросы, проводимые в целях первичного мониторинга усвоения материала студентами и оцениваемые исходя из полноты и последовательности ответа, понимания основных понятий, методов и алгоритмов, изложенных на лекционных или лабораторных занятиях, коллоквиум.

Формой промежуточной аттестации по дисциплине «Введение в информационную безопасность» предусмотрен зачет.

В случае успешной защиты отчётов по всем лабораторным работам, положительных результатов контрольной работы, коллоквиума и устного опроса, успешной защиты проекта студент допускается к сдаче зачета.

Примерная тематика лабораторных занятий

Лабораторная работа № 1. Информационная безопасность (ИБ) в системе национальной безопасности.

Лабораторная работа № 2. Общеметодологические принципы теории ИБ.

Лабораторная работа № 3. Анализ объектов ИБ.

Лабораторная работа № 4. ИБ государства, корпорации, личности.

Лабораторная работа № 5. Анализ угроз ИБ.

Лабораторная работа № 6. Методы и средства обеспечения ИБ.

Лабораторная работа № 7. Методы нарушения конфиденциальности, целостности, доступности информации.

Лабораторная работа № 8. Причины, виды, каналы утечки и искажения информации.

Лабораторная работа № 9. Теоретические основы компьютерной безопасности.

Лабораторная работа № 10. Организационно-методическое обеспечение информационной безопасности.

Лабораторная работа № 11. Правовое обеспечение информационной безопасности.

Лабораторная работа № 12. Криптографические методы защиты информации.

Лабораторная работа № 13. Программно-аппаратные средства обеспечения информационной безопасности.

Лабораторная работа № 14. Комплексное обеспечение информационной безопасности сложных интегрированных систем.

Примерный перечень заданий для управляемой самостоятельной работы

Тема 11. Правовое обеспечение информационной безопасности.

Понятие и виды защищаемой информации по законодательству. Государственная тайна как особый вид защищаемой информации. (2ч.)

(Форма контроля – контрольная работа).

Тема 14. Комплексное обеспечение информационной безопасности сложных интегрированных систем.

Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы, технология, управление. Методология формирования задач защиты. (2ч.)

(Форма контроля – проект).

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используются следующие инновационные подходы:

практико-ориентированный подход, который предполагает:

- освоение содержания образования через решения практических задач;
- приобретение навыков эффективного выполнения разных видов профессиональной деятельности;
- ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;
- использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

метод проектного обучения, который предполагает:

- способ организации учебной деятельности студентов, развивающий актуальные для учебной и профессиональной деятельности навыки планирования, самоорганизации, сотрудничества и предполагающий создание собственного продукта;
- приобретение навыков для решения исследовательских, творческих, социальных, предпринимательских и коммуникационных задач.

Методические рекомендации по организации самостоятельной работы обучающихся

Самостоятельная работа с целью изучения материала учебной дисциплины предполагает работу с рекомендованной учебной литературой и Интернет-ресурсами. Теоретические сведения закрепляются выполнением лабораторных заданий, при выполнении которых следует руководствоваться методическими разработками, размещенными в электронной библиотеке университета и на образовательном портале. Также могут быть предложены дополнительные задания (тесты, задания для самостоятельного выполнения) для самооценки и более глубокого усвоения полученного материала.

Примерный перечень вопросов к зачету

1. Информационная безопасность (ИБ) в системе национальной безопасности. Понятие национальной безопасности, виды безопасности.
2. Общеметодологические принципы теории ИБ. Основные понятия ИБ, краткая характеристика теории ИБ, общеметодологические принципы.
3. Анализ объектов ИБ. Объекты ИБ, критерии их классификации, анализ.
4. ИБ государства, корпорации, личности. Общность и различия ИБ государства, корпорации, личности.
5. Анализ угроз ИБ. Понятие угроз, критерии их классификации.
6. Методы и средства обеспечения ИБ. Методы, средства, их классификация.
7. Методы нарушения конфиденциальности, целостности, доступности информации. Конфиденциальность, целостность, доступность информации, нарушение этих свойств.
8. Причины, виды, каналы утечки и искажения информации. Утечка информации, каналы утечки информации, искажение информации, каналы искажения.
9. Теоретические основы компьютерной безопасности. Формальные модели. Модели безопасности. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
10. Организационно-методическое обеспечение информационной безопасности. Анализ и оценка угроз информационной безопасности объекта.
11. Правовое обеспечение информационной безопасности. Законодательство в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
12. Понятие и виды защищаемой информации по законодательству. Государственная тайна как особый вид защищаемой информации.
13. Криптографические методы защиты информации. История криптографии. Характер криптографической деятельности.

14. Простейшие шифры и их свойства. Виды информации, подлежащие закрытию, их модели и свойства.

15. Программно-аппаратные средства обеспечения информационной безопасности. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.

16. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем.

17. Методы и средства ограничения доступа к компонентам вычислительных систем.

18. Комплексное обеспечение информационной безопасности сложных интегрированных систем. Постановка проблемы комплексного обеспечения информационной безопасности сложных интегрированных систем.

19. Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ), функциональные и обеспечивающие подсистемы, технология, управление. Методология формирования задач защиты.

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)
Защита данных и программ в информационных системах	Кафедра технологий программирования	Изменений не требуется	Протокол № 18 от 16.05.2024

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

16. 05 2024г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 20_ г.)

Заведующий кафедрой
_____ _____ _____

УТВЕРЖДАЮ
Декан факультета
_____ _____ _____