

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Ректор Белорусского
государственного университета

А.Д.Король

23 сентября 2024 г.

Регистрационный № 2517/б.



ПРОГРАММНО-АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

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.

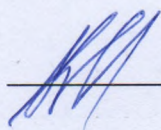
А.В. Федчук - инженер-программист ООО «Ювеком Системы».

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования БГУ
(протокол № 2 от 12.09.2024).

Научно-методическим советом БГУ
(протокол № 2 от 19.09.2024)

Заведующий кафедрой



А.Н. Курбацкий

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дисциплина «Программно-аппаратные и технические средства защиты информации» направлена на изучение ключевых компонентов и механизмов обеспечения информационной безопасности в современных информационных системах, включая как архитектурные, так и технические аспекты. В рамках курса рассматриваются аппаратные, программные и сетевые компоненты информационных систем, их архитектура (клиент-серверная, распределённая, облачная), угрозы и уязвимости, а также методы анализа и минимизации рисков. Изучаются реальные инциденты безопасности и подходы к оценке их последствий.

В ходе изучения дисциплины рассматриваются типовые угрозы и уязвимости, методы их анализа и предотвращения. Изучаются современные средства защиты: криптография, электронная подпись, протоколы безопасности, модели управления доступом, а также методы аутентификации и авторизации, включая многофакторную и биометрическую. Освещаются принципы проектирования систем защиты, внедрение защитных механизмов, тестирование безопасности и аудит. Отдельное внимание уделяется защите информации в операционных системах, базах данных, вычислительных сетях и персональных ЭВМ. Анализируются методы обнаружения вредоносных программ и организация защиты от них.

В рамках дисциплины также рассматриваются актуальные вызовы: безопасность в IoT, облаках, мобильных устройствах, а также применение ИИ, машинного обучения и блокчейна в обеспечении защиты. Изучаются основы управления рисками и инцидентами, а также построение систем управления безопасностью.

В результате студенты получают практические навыки оценки, проектирования и реализации комплексных решений по защите информации в современных ИС.

Цели и задачи учебной дисциплины

Цель учебной дисциплины «Программно-аппаратные и технические средства защиты информации» - формирование устойчивых знаний и практических навыков в области обеспечения информационной безопасности в современных системах. Студенты знакомятся с основными стандартами безопасности, такими как ISO 27k и NIST, рассматривают основные угрозы и уязвимости, изучают ключевые аспекты проектирования и управления безопасностью, учатся реализовывать меры политики безопасности и проводить аудит информационной системы. В завершение курса рассматриваются перспективы и будущее компьютерной безопасности, включая новые технологии и инновации, которые меняют подходы к обеспечению безопасности в распределённых системах.

Задачи учебной дисциплины:

1. Обеспечить базовые знания по вопросам информационной безопасности в информационных системах.

2. Сформировать понимание ключевых механизмов защиты: аутентификация, авторизация, шифрование, управление доступом и конфиденциальность.

3. Ознакомить с международными стандартами (например, ISO 27001) и подходами к управлению рисками и анализу угроз.

4. Изучить современные методы защиты информации: криптографические алгоритмы, протоколы безопасности, контроль целостности и аудит.

5. Рассмотреть актуальные вызовы и тренды в кибербезопасности: IoT, мобильные и облачные среды, виртуализация.

6. Изучить процесс проектирования систем защиты - от анализа уязвимостей до тестирования и внедрения решений.

7. Развить навыки оценки угроз и построения комплексных систем защиты информационных сред.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

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

Дисциплина «Программно-аппаратные и технические средства защиты информации» непосредственно связана с учебной дисциплиной «Теоретические основы информационной безопасности».

Требования к компетенциям

Освоение учебной дисциплины «Программно-аппаратные и технические средства защиты информации» 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:

- архитектуру информационных систем, принципы построения клиент-серверных, распределённых и облачных ИС;
- международные стандарты информационной безопасности, такие как ISO 27k, и протоколы защиты данных (SSL/TLS, IPsec);
- классификацию угроз и уязвимостей, методы анализа рисков, подходы к обеспечению защищённости;
- принципы защиты в операционных системах, сетях, базах данных, облачных и мобильных средах;
- модели, методы и алгоритмы обеспечения безопасности в информационных системах, включая аутентификацию, авторизацию, шифрование, цифровые подписи, контроль целостности и контроль доступа;
- основы проектирования и управления системами защиты, включая DevSecOps и современные инструменты анализа;
- особенности защиты данных в многоуровневых инфраструктурах;

уметь:

- выполнять анализ уязвимостей информационных систем, выявлять риски и оценивать уровень защищённости в зависимости от типа системы;
- оценивать риски и разрабатывать политики безопасности и планы реагирования на инциденты;
- применять методы криптографической защиты информации для информационных систем, включая шифрование, управление ключами и цифровые подписи;
- проектировать и внедрять механизмы для различных компонентов системы защиты информации;
- проектировать, настраивать и тестировать средства защиты для различных компонентов ИС;
- использовать IDS/IPS, антивирусы, сканеры уязвимостей и сетевые фильтры;
- определять и применять эффективные методы обеспечения конфиденциальности данных и контроля доступа;

иметь навык:

- проектирования и реализации систем безопасности информационных систем с использованием современных инструментов;
- работы с программно-аппаратными средствами защиты данных, операционных систем, сетевых ресурсов и облачных сервисов;
- применения криптографических методов защиты информации, включая PKI, цифровые подписи и управление ключами, в том числе в распределённых вычислительных средах;
- работы с системами анализа и оценки рисков, включая автоматизированные средства, для обеспечения безопасности информационных систем;
- использования инструментов анализа и тестирования безопасности, таких как Nessus, OpenVAS, Wireshark, Metasploit и других.

Структура учебной дисциплины

Дисциплина изучается в 4 семестре. В соответствии с учебным планом всего на изучение учебной дисциплины «Программно-аппаратные и технические средства защиты информации» отведено для очной формы получения высшего образования: 108 часов, в том числе 68 аудиторных часов (лекции – 34 часа, лабораторные занятия – 18 часов, практические занятия – 16 часов). **Из них:**

Лекции – 34 часа, лабораторные занятия – 16 часов, практические занятия – 16 часов, управляемая самостоятельная работа – 2 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – зачет и экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Архитектура информационных систем и основные задачи защиты.

Тема 1.1. Введение. Архитектура ИС.

Цели и задачи курса, содержание дисциплины. Компоненты информационных систем: аппаратные, программные и сетевые. Архитектурные подходы: клиент-серверные, распределённые и облачные системы. Примеры использования информационных систем в различных отраслях - финансах, здравоохранении, промышленности.

Тема 1.2. Основные задачи защиты информации.

Разграничение доступа к объектам системы. Идентификация, аутентификация и авторизация пользователей. Задачи идентификации, аутентификации и авторизации. Основные схемы аутентификации. Достоинства и недостатки различных схем аутентификации. Политики безопасности, управление пользователями. Критерии защищённости, аудит, проблемы реализации аудита.

Раздел 2. Угрозы, уязвимости и вредоносные воздействия.

Тема 2.1. Угрозы и уязвимости информационных систем.

Классификация угроз и уязвимостей. Методологии анализа уязвимостей. Факторы, влияющие на безопасность: недочёты проектирования, человеческий фактор, организационные аспекты. Анализ инцидентов безопасности и их последствия.

Тема 2.2. Вредоносное программное обеспечение и защита от него.

Понятие и классификация вредоносных программ. Особенности технологий стелс и полиморфизма. Методы заражения программ и деструктивные функции вредоносного ПО. Методы выявления и удаления вредоносных программ. Антивирусы, мониторы, сетевые фильтры. Принципы работы антивирусных сканеров, мониторов и сетевых фильтров.

Раздел 3. Криптография и защита данных.

Тема 3.1. Криптографические методы и протоколы.

Основы симметричного и асимметричного шифрования. Применение электронной цифровой подписи для обеспечения подлинности и целостности данных. Протоколы безопасности в распределённых системах. Оценка надёжности и эффективности криптографических методов. Требования к средствам криптографической защиты информации. Особенности разработки программно-аппаратных средств защиты.

Тема 3.2. Хранение и защита ключевой информации.

Методы и средства хранения и защиты ключей. Обеспечение целостности и защита от изменений. Контроль целостности данных с использованием программно-аппаратных средств.

Раздел 4. Защита на уровне программного и аппаратного обеспечения.

Тема 4.1. Защита информации в ПЭВМ и программном обеспечении.

Методы и средства привязки программного обеспечения к аппаратной среде. Анализ машинного кода: статический, динамический и экспериментальный подходы. Факторы, ограничивающие возможности отладчиков. Методы защиты от дизассемблирования и отладки. Методы встраивания защиты в программное обеспечение. Защита от изменения и контроль целостности кода.

Тема 4.2. Ограничение доступа и защита в операционных системах.

Субъекты и объекты доступа. Группирование пользователей и специальные субъекты. Механизмы избирательного разграничения доступа. Применение монитора ссылок. Способы хранения матрицы доступа. Понятие владельца объекта и полномочий пользователей. Контроль информационных потоков и проблемы его реализации. Применение изолированных программных сред. Особенности программных средств защиты в операционных системах Windows и UNIX.

Раздел 5. Безопасность сетей и баз данных.

Тема 5.1. Защита информации в вычислительных сетях.

Анализ уязвимостей сетевых протоколов. Специфические виды атак на вычислительные сети. Удалённые атаки в сети Internet. Организация безопасной распределённой обработки информации. Протоколы аутентификации при удалённом доступе. Принципы использования и реализации межсетевых экранов. Методы обеспечения целостности и конфиденциальности данных. Программно-аппаратные средства криптографической защиты.

Тема 5.2. Особенности защиты информации в системах управления базами данных.

Средства обеспечения безопасности в СУБД. Механизмы идентификации и аутентификации пользователей баз данных. Средства управления доступом и контроля целостности информации. Организация аудита действий пользователей. Причины и методы нарушения конфиденциальности. Специфические атаки на базы данных и методы их предотвращения. Роль администратора безопасности баз данных.

Раздел 6. Проектирование и управление защитой.

Тема 6.1. Проектирование систем защиты информации.

Этапы проектирования систем защиты. Анализ требований безопасности. Выбор методов защиты с учётом стандартов и рекомендаций. Многоуровневая

архитектура защиты. Интеграция средств защиты в существующие ИС. Обеспечение безопасности на этапе разработки с применением DevSecOps-подхода.

Тема 6.2. Оценка уязвимостей и тестирование систем безопасности.

Методы анализа уязвимостей и их оценка с помощью автоматизированных инструментов (Nessus, OpenVAS). Проведение статического и динамического анализа. Этапы пенетрационного тестирования. Применение проактивных мер по предотвращению инцидентов.

Тема 6.3. Менеджмент информационной безопасности.

Системы менеджмента информационной безопасности. Управление рисками и проведение аудита. Разработка планов реагирования на инциденты и устранения последствий. Организация процессов информационной безопасности на уровне управления.

Раздел 7. Современные тенденции в информационной безопасности.

Тема 7.1. Актуальные вызовы в области информационной безопасности.

Современные угрозы: киберпреступность, атаки на искусственный интеллект, уязвимости облачных решений. Проблемы безопасности в инфраструктурах интернета вещей и облачных сервисов.

Тема 7.2. Новейшие технологии и разработки в области ИБ.

Применение машинного обучения в системах защиты. Использование искусственного интеллекта для обеспечения информационной безопасности. Влияние блокчейн-технологий на развитие современных подходов к защите данных.

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 знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1.	Архитектура информационных систем и основные задачи защиты.	4	4					
1.1	Введение. Архитектура ИС.	2	2					Экспресс-опрос, дискуссия
1.2	Основные задачи защиты информации.	2	2					Экспресс-опрос, доклад
2.	Угрозы, уязвимости и вредоносные воздействия.	4	2		2			
2.1	Угрозы и уязвимости информационных систем.	2	2					Экспресс-опрос, доклад
2.2	Вредоносное программное обеспечение и защита от него.	2			2			Экспресс-опрос, отчеты по лабораторным заданиям.
3.	Криптография и защита данных.	4	2		4		2	
3.1	Криптографические методы и протоколы.	2	2		2		2	Электронный тест, отчеты по лабораторным заданиям, доклад
3.2	Хранение и защита ключевой информации.	2			2			Отчеты по лабораторным заданиям, экспресс-опрос

4.	Защита на уровне программного и аппаратного обеспечения.	4	2		4			
4.1	Защита информации в ПЭВМ и программном обеспечении.	2			2			Отчеты по лабораторным заданиям, дискуссия
4.2	Ограничение доступа и защита в операционных системах.	2			2			Электронный тест, отчеты по лабораторным заданиям
5.	Безопасность сетей и баз данных.	6	2		2			
5.1	Защита информации в вычислительных сетях.	4			2			Отчеты по лабораторным заданиям, дискуссия, экспресс-опрос
5.2	Особенности защиты информации в системах управления базами данных.	2	2					Дискуссия, доклад, контрольная работа
6	Проектирование и управление защитой.	8	4		2			
6.1	Проектирование систем защиты информации.	2	2					Электронный тест, экспресс-опрос
6.2	Оценка уязвимостей и тестирование систем безопасности.	4			2			Коллоквиум, дискуссия
6.3	Менеджмент информационной безопасности.	2	2					Экспресс-опрос, дискуссия
7	Современные тенденции в информационной безопасности.	4	2		2			
7.1	Актуальные вызовы в области информационной безопасности.	2	2					Экспресс-опрос, доклад
7.2	Новейшие технологии и разработки в области ИБ.	2			2			Отчеты по лабораторным заданиям, Дискуссия, экспресс-опрос
	Итого	34	16		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. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие для студентов высших учебных заведений, обучающихся по направлению "Информационная безопасность" / П. Б. Хорев. – 3-е изд., испр. и доп. – Москва : ИНФРА-М, 2022. – 326 с. – URL: <https://znanium.com/catalog/document?id=397282>.

Дополнительная литература

1. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / И. И. Белоус, В. А. Солодуха. – Москва ; Вологда : Инфра-Инженерия, 2020. – 690 с.
2. 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.
3. Гусаков, А. В., Куренев, А. В. Основы защиты информации в автоматизированных системах обработки информации : учебное пособие для курсантов учреждения образования "Военная академия Республики Беларусь" / Вооруженные Силы Республики Беларусь, Военная академия Республики Беларусь. – Минск : ВА РБ, 2019. – 218 с.
4. Дубко, М. А. и др. Уголовно-правовая охрана информационной безопасности и электронные доказательства = Cybercrime and digital evidence : учебное пособие для студентов учреждений высшего образования по специальности магистратуры "юриспруденция" / под ред. М. А. Дубко, О. В. Петровой ; БГУ. – Минск : БГУ, 2023. – 327 с.
5. Макконнелл, С. Совершенный код. Мастер-класс. Второе издание. – М.: Издательство «Русская редакция», 2017. – 896 с.
6. Насонова, Н. В. Основы защиты информации : учеб.-метод. пособие для спец. I ступени высш. образования, закрепленных за УМО / Н. В. Насонова, Г. А. Пухир, С. Н. Петров ; М-во образования Республики Беларусь, УО "Бел.

гос. ун-т информатики и радиоэлектроники", Факультет инфокоммуникаций, Каф. защиты информации. – Минск : БГУИР, 2019. – 82 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. Ховард, М., Лебланк, Д., Вьег, Дж. 24 смертных греха компьютерной безопасности. Как написать безопасный код. – Издательство «Питер», 2010. – 400 с.

9. 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.

10. 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: контрольная работа, коллоквиум.
3. Устно-письменная форма: отчеты по лабораторным заданиям, доклад.
4. Техническая форма: электронные тесты.

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

Критерием оценивания является выполнение заданий для управляемой самостоятельной работы, практических и лабораторных 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.

Отметка «зачтено» выставляется студенту, который твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.

Отметка «не зачтено» выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, допускающему в ответе или в решении задач грубые ошибки. (перенесла)

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

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.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний в рейтинговую оценку (формирование оценки за текущую успеваемость):

- отчёты по лабораторным работам – 35 %;
- контрольные работы – 30 %;
- электронные тесты – 35%.

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

Примерная тематика лабораторных занятий

Занятие № 1. Методы заражения программ и деструктивные функции вредоносного ПО.

Занятие № 2. Применение электронной цифровой подписи для обеспечения подлинности и целостности данных.

Занятие № 3. Методы и средства хранения и защиты ключей.

Занятие № 4. Методы и средства привязки программного обеспечения к аппаратной среде.

Занятие № 5. Ограничение доступа и защита в операционных системах.

Занятие № 6. Защита информации в вычислительных сетях.

Занятие № 7. Методы анализа уязвимостей и их оценка с помощью автоматизированных инструментов.

Занятие № 8. Использование искусственного интеллекта для обеспечения информационной безопасности.

Примерная тематика практических занятий

Занятие № 1. Примеры использования информационных систем в различных отраслях - финансах, здравоохранении, промышленности.

Занятие № 2. Основные схемы аутентификации. Достоинства и недостатки различных схем аутентификации.

Занятие № 3. Анализ инцидентов безопасности и их последствия.

Занятие № 4. Оценка надёжности и эффективности криптографических методов.

Занятие № 5. Средства обеспечения безопасности в СУБД.

Занятие № 6. Обеспечение безопасности на этапе разработки с применением DevSecOps-подхода.

Занятие № 7. Системы менеджмента информационной безопасности.

Занятие № 8. Проблемы безопасности в инфраструктурах интернета вещей и облачных сервисов.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Тема 3.1. Криптографические методы и протоколы (2 часа)

Основы симметричного и асимметричного шифрования. Применение электронной цифровой подписи для обеспечения подлинности и целостности данных. Протоколы безопасности в распределённых системах. Оценка надёжности и эффективности криптографических методов. Требования к средствам криптографической защиты информации. Особенности разработки программно-аппаратных средств защиты.

Задание: Изучить принципы работы электронной цифровой подписи (ЭЦП) и ее применение для обеспечения подлинности и целостности данных. Практически освоить процесс создания и проверки ЭЦП с использованием программного обеспечения.

Форма контроля: доклад, электронный тест.

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 использования 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.

- ***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; использование процедур, способов оценивания, фиксирующих профессиональные компетенции.

Методические рекомендации по организации самостоятельной работы обучающихся

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/экзамену

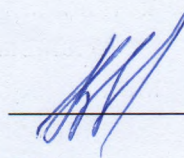
1. Компоненты информационных систем: аппаратные, программные и сетевые.
2. Архитектурные подходы: клиент-серверные, распределённые и облачные системы.
3. Основные задачи защиты информации.
4. Разграничение доступа к объектам системы.
5. Идентификация, аутентификация и авторизация пользователей.
6. Задачи идентификации, аутентификации и авторизации.
7. Основные схемы аутентификации.
8. Достоинства и недостатки различных схем аутентификации.
9. Политики безопасности, управление пользователями.
10. Критерии защищённости, аудит, проблемы реализации аудита.
11. Классификация угроз и уязвимостей.
12. Методологии анализа уязвимостей.
13. Факторы, влияющие на безопасность: недочёты проектирования, человеческий фактор, организационные аспекты.
14. Анализ инцидентов безопасности и их последствия.
15. Понятие и классификация вредоносных программ.
16. Особенности технологий стелс и полиморфизма.
17. Методы заражения программ и деструктивные функции вредоносного ПО.
18. Методы выявления и удаления вредоносных программ.
19. Антивирусы, мониторы, сетевые фильтры.
20. Принципы работы антивирусных сканеров, мониторов и сетевых фильтров.
21. Основы симметричного и асимметричного шифрования.
22. Применение электронной цифровой подписи для обеспечения подлинности и целостности данных.
23. Протоколы безопасности в распределённых системах.
24. Оценка надёжности и эффективности криптографических методов.

25. Требования к средствам криптографической защиты информации.
26. Особенности разработки программно-аппаратных средств защиты.
27. Методы и средства хранения и защиты ключей.
28. Обеспечение целостности и защита от изменений.
29. Контроль целостности данных с использованием программно-аппаратных средств.
30. Методы и средства привязки программного обеспечения к аппаратной среде.
31. Анализ машинного кода: статический, динамический и экспериментальный подходы.
32. Факторы, ограничивающие возможности отладчиков.
33. Методы защиты от дизассемблирования и отладки
34. Методы встраивания защиты в программное обеспечение.
35. Защита от изменения и контроль целостности кода.
36. Группирование пользователей и специальные субъекты.
37. Механизмы избирательного разграничения доступа.
38. Применение монитора ссылок.
39. Способы хранения матрицы доступа.
40. Понятие владельца объекта и полномочий пользователей.
41. Контроль информационных потоков и проблемы его реализации.
42. Применение изолированных программных сред
43. Особенности программных средств защиты в операционных системах Windows и UNIX.
44. Анализ уязвимостей сетевых протоколов.
45. Специфические виды атак на вычислительные сети.
46. Удалённые атаки в сети Internet.
47. Организация безопасной распределённой обработки информации.
48. Протоколы аутентификации при удалённом доступе.
49. Принципы использования и реализации межсетевых экранов.
50. Методы обеспечения целостности и конфиденциальности данных.
51. Программно-аппаратные средства криптографической защиты.
52. Средства обеспечения безопасности в СУБД.
53. Механизмы идентификации и аутентификации пользователей баз данных.
54. Средства управления доступом и контроля целостности информации.
55. Организация аудита действий пользователей.
56. Специфические атаки на базы данных и методы их предотвращения.
57. Роль администратора безопасности баз данных.

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)
Безопасность операционных систем	кафедра технологий программирования	Предложения отсутствуют	Рекомендовать к утверждению учебную программу (протокол №2 от 12.09.2024).

Заведующий кафедрой технологий
программирования,
доктор технических наук, профессор



А.Н. Курбацкий

12.09.2024

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)