КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

РАЗРАБОТКА И РЕАЛИЗАЦИЯ ПРОЕКТОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Разработка и реализация проектов в сфере информационной безопасности» по специальности 10.05.01 Компьютерная безопасность, специализация «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от 2 апреля 2025 г., протокол № 3

СОДЕРЖАНИЕ

1. Цель освоения дисциплины

Целью изучения дисциплины «Разработка и реализация проектов в сфере информационной безопасности» является формирование у студентов знаний, умений и навыков, необходимых для проектирования, разработки и внедрения проектов в области информационной безопасности, включая управление их жизненным циклом и обеспечение соответствия требованиям стандартов.

Основные задачи освоения дисциплины:

- формирование системного представления о процессах разработки и реализации проектов в сфере информационной безопасности;
- изучение методов управленияпроектами и их адаптации к задачам информационной безопасности;
- развитие практических навыков проектирования и внедрения систем защиты информации в автоматизированных системах.

В результате освоения дисциплины студент должен:

Знать:

- основные этапы жизненного цикла проектов в сфере информационной безопасности;
- методы и подходы к управлению проектами в области защиты информации;
- стандарты и нормативные документы, регулирующие разработку систем информационной безопасности.

Уметь:

- разрабатывать проектную документацию для систем информационной безопасности;
- планировать и реализовывать проекты с учетом требований к защите информации;
- оценивать эффективность реализованных проектов и их соответствие поставленным целям. Иметь навыки (приобрести опыт):
- управления проектами в области информационной безопасности;
- применения современных инструментов и технологий для реализации проектов;
- анализа рисков и разработки мер по их минимизации в процессе выполнения проектов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Разработка и реализация проектов в сфере информационной безопасности»» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ОПК-3.2	Администрирование серверов	**Разработка и реализация проектов в сфере информационной безопасности**	

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ОПК-3.2 Способен использовать современные технологии программирования для разработки защищенного программного обеспечения	ОПК-3.2.1 Демонстрирует умение анализа средств защиты информации и выполнения анализа защищенности сетевых сервисов с использованием средств мониторинга и автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Знает: основные средства защиты информации, принципы их работы и применения, а также методы анализа защищенности сетевых сервисов. Уметь: проводить анализ событий информационной безопасности с использованием средств мониторинга, выявлять попытки несанкционированного доступа и реагировать на них с помощью автоматизированных систем. Владеет: навыками настройки и управления средствами защиты информации для обеспечения устойчивости компьютерных систем и сетей.
	ОПК-3.2.2 Демонстрирует умение организовывать аудит безопасности и участвовать в проверках защищенности компьютерных сетей и информационных систем	Знает: методы и инструменты проведения аудита информационной безопасности, а также основные подходы к проверке защищенности компьютерных сетей и информационных систем. Умеет: организовывать и проводить аудит безопасности, выявлять уязвимости и оценивать их влияние на информационные системы. Владеет: навыками участия в проверках защищенности, документирования результатов аудита и разработки рекомендаций по улучшению уровня безопасности.

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности	ак.часов

		Всего	По семестрам
			10
1. Контактная работа обучающихся с преподавателем:		51	51
Аудиторные занятия, часов всего, в том числе:		50	50
• занятия лекционного типа		16	16
• занятия семинарского типа:		34	34
практические занятия		-	-
лабораторные занятия		34	34
в том числе занятия в форме практической подготовки		-	-
Контроль самостоятельной работы (КСР)		0,5	0,5
Промежуточная аттестация (ИКР)		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		57	57
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		19	19
- выполнение индивидуальных заданий (подготовка сообщений, презентаций)		19	19
- реферат		17	17
- подготовка к зачету		2	2
Промежуточная аттестация: зачет		-	-
ИТОГО:	часов	108	108
общая трудоемкость	зач. ед.	3	3

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Раздел 1. Теоретические основы БД и СУБД

Тема 1. Основы управления проектами в сфере информационной безопасности

Жизненный цикл проектов. Методы управления проектами (PMI,Agile). Особенности проектов в области информационной безопасности.

Тема 2. Разработка проектной документации для систем защиты информации

Структура проектной документации. Требования стандартов (ГОСТ, ISO). Анализ рисков и угроз в проектах.

Тема 3. Реализация и оценка проектов в сфере информационной безопасности

Этапы внедрения проектов. Методы оценки эффективности. Инструменты мониторинга и контроля реализации

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	
1	Тема 1. Основы управления проектами в сфере информационной безопасности	4	8/8	20	ОПК-3.2, ОПК-3.2.1, ОПК-3.2.2,
2	Тема 2 Разработка проектной документации для систем защиты информации	6	10/10	20	ОПК-3.2, ОПК-3.2.1, ОПК-3.2.2,
3	Тема 3. Реализация и оценка проектов в сфере информационной безопасности	6	16/16	17	ОПК-3.2, ОПК-3.2.1, ОПК-3.2.2,
	Всего	**16**	**34/34**	**57**	

6. Практические занятия

Практические занятия не предусмотрены.

7. Лабораторные работы

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
1.	Тема 1. Анализ требований к проекту защиты информации	Жизненный цикл проектов. Методы управления проектами (PMI, Agile). Особенности проектов в области информационной безопасности.	6
2.	Тема 2. Планирование проекта с использованием инструментов MS	Структура проектной документации. Требования стандартов (ГОСТ, ISO). Анализ рисков и угроз в проектах Project	6
3.	Тема 3. Разработка Технического задания на систему защиты информации	Этапы внедрения проектов. Методы оценки эффективности. Инструменты мониторинга и контроля реализации	6
4	Тема 4.Оценка рисков в Проекте Обеспечения информационной безопасности	Определение риска в контексте информационной безопасности. Классификация рисков: технические, организационные, человеческие.	6

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
5	Тема 5.Моделирование процессов реализации проекта	Определение и цели моделирования процессов. Важность моделирования для управления проектами.	6
6	Тема 6. Оценка эффективности реализованного проекта	Введение в оценку эффективности проектов	4
	Всего		**34**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Разработка и реализация проектов в сфере информационной безопасности» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях.

Вопросы для самостоятельной работы

1.Основные этапы жизненного цикла проекта в сфере информационной безопасности. (ОПК- 3.2.1, ОПК-3.2.2)

2.Сравнение методов управления проектами PMI и Agile: преимущества и недостатки в контексте защиты информации. (ОПК-3.2.1, ОПК-3.2.2)

3.Роль анализа рисков в управлении проектами информационной безопасности. (ОПК-3.2.1, ОПК-3.2.2)

4.Принципы планирования ресурсов и сроков в проектах защиты информации. (ОПК-3.2.1, ОПК-3.2.2)

5.Особенности управления проектами в области информационной безопасности по сравнению с другими сферами. (ОПК-3.2.1, ОПК-3.2.2)

6.Структура и содержание технического задания на разработку системы защиты информации.

(ОПК-3.2.1, ОПК-3.2.2)

7.Требования к проектной документации согласно стандартам ГОСТ и ISO/IEC 27001. (ОПК- 3.2.1, ОПК-3.2.2)

8.Методы оценки угроз и уязвимостей при разработке проектной документации. (ОПК-3.2.1, ОПК-3.2.2)

9.Разработка регламентов и инструкций как части проектной документации. (ОПК-3.2.1, ОПК- 3.2.2)

10Принципы документирования процессов управления рисками в проектах ИБ. (ОПК-3.2.1, ОПК-3.2.2)

11.Основные этапы внедрения проектов защиты информации в автоматизированных системах. (ОПК-3.2.1, ОПК-3.2.2)

12.Методы мониторинга и контроля реализации проектов ИБ. (ОПК-3.2.1, ОПК-3.2.2)

13.Критерии оценки эффективности реализованных систем защиты информации. (ОПК-3.2.1, ОПК-3.2.2)

14.Инструменты управления изменениями в процессе реализации проектов. (ОПК-3.2.1, ОПК- 3.2.2)

15.Анализ типичных ошибок при внедрении проектов и способы их предотвращения. (ОПК-3.2.1, ОПК-3.2.2)

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература

1. Торстейнсон, П. Криптография и безопасность в технологии .NET : руководство / П. Торстейнсон, Г. А. Ганеш ; перевод с англ. В. Д. Хорева под редакцией С. М. Молявко. - 5-е изд. (эл.). - Москва : Лаборатория знаний, 2024. - 482 с. - URL: https://e.lanbook.com/book/418025 (дата обращения: 17.01.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-93208-734-3. - Текст : электронный.

2. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр.- Москва : Юрайт, 2022. - 473 с. - URL: https://urait.ru/bcode/489242 (дата обращения: 26.01.2022).-Режим доступа: для авториз. пользователей. - ISBN 978-5-534-12474-3. - Текст : электронный.

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Юрайт, 2022. - 349 с. - URL:

: https://urait.ru/bcode/489919дата обращения: 30.05.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-02883-6. - Текст : электронный**.**

Дополнительная литература:

1.Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - Санкт-Петербург : Лань, 2022. - 400 с. - URL: https://e.lanbook.com/book/210746 (дата обращения: 18.03.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-1116-0. - Текст : электронный.

2.Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стереотипное. - Москва : Горячая линия-Телеком, 2017. - 230 с.- https://e.lanbook.com/book/111097. - Текст : электронный.

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/

5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search

6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного

типа, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для самостоятельной работы студентов.

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения лабораторных занятий. Лаборатория сетей и систем передачи информации, безопасности компьютерных сетей

Рабочее место преподавателя (стол, стул), рабочие места обучающихся.

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» - - 15, сетевое коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак, средства анализа защищенности компьютерных сетей.

Учебная аудитория для проведения лабораторных занятий. Аудитория информационных технологий

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения:

персональный компьютер с подключением к сети «Интернет» - 15, сетевое оборудование.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____