Ф 27-022

УТВЕРЖДАЮ
Ректор учреждения образования
«Гродненский государственный университет имени Янки Купалы»
_____ И.Ф. Катурко
04 октября 2024 г.

КОМПЛЕКСНАЯ ПРОГРАММА РАЗВИТИЯ СПЕЦИАЛЬНОСТИ

6-05-0533-12 Кибербезопасность

образовательной программы **бакалавриата**

на 2024-2028 гг.

в учреждении образования «Гродненский государственный университет имени Янки Купалы»

Гродно 2024

Комплексная программа развития специальности разработана:

А.М. Кадан, заведующий кафедрой системного программирования и компьютерной безопасности;
Е.Н. Ливак, доцент кафедры системного программирования и компьютерной безопасности;
А.А. Врублевский, заказчик кадров, ведущий инженер-программист ООО «Когнитек»;
М.С. Яковенко, выпускник, представитель Ассоциации выпускников, директор ООО «СкилСофт»;
Е.А. Шитик, студент 3 курса специальности 1-98-01 01 Компьютерная безопасность;

Эксперты:
П.Н. Борель, представитель базовой организации, заместитель директора ООО «ИнтэксСофт»

СОГЛАСОВАНО_____ П.Н. Борель

А.В. Бабкин, председатель Координационного совета по подготовке кадров факультета математики и информатики, директор ООО «Азати»

СОГЛАСОВАНО_____ А.В. Бабкин

Перечень используемых обозначений и сокращений

УР	– учебная работа
НР	– научная работа
ПР	– профориентационная работа
НИиИД	– научно-исследовательская и инновационная деятельность
НИР	– научно-исследовательская работа
НИРС	– научно-исследовательская работа студентов
ИВР	– идеологическая и воспитательная работа
УСРС	– управляемая самостоятельная работа студентов
ППС	– профессорско-преподавательский состав
ИИ	– искусственный интеллект
КБ	– кибербезопасность
ИТ	– информационные технологии
СПКБ	– кафедра системного программирования и компьютерной безопасности
СШ	– средние школы

Раздел 1. Паспорт образовательной программы

1.1. Описание образовательной программы

Код и наименование специальности	6-05-0533-12 Кибербезопасность
Квалификация, степень	Специалист по кибербезопасности, бакалавр
Образовательный стандарт	ОСВО-6-05-0533-12-2023
Форма обучения, срок и объем (з.е.)	Дневная, 4 года, 240 з.е.
Профилизация(и)	–
Факультет	Математики и информатики
Выпускающая кафедра	Системного программирования и компьютерной безопасности
Язык реализации	русский
Сетевая форма реализации	нет
Партнеры по реализации специальности	БГУ, ГГУ, АО «ГродноАзот», РУП «Гродноэнерго»
Виды профессиональной деятельности (согласно ОС)	26 Производство вычислительной, электронной и оптической аппаратуры; 582 Издание программного обеспечения; 61 Деятельность в области телекоммуникаций; 62 Компьютерное программирование, консультационные и другие сопутствующие услуги; 63 Деятельность в области информационного обслуживания; 70 Деятельность головных организаций; консультирование по вопросам управления; 721 Научные исследования и разработки в области естественных и технических наук; 80200 Деятельность в области систем обеспечения безопасности.
Перечень возможных должностей	Специалист по защите информации; Стажер младшего научного сотрудника или младший научный сотрудник; Инженер-программист; Ассистент; Системный администратор; Администратор баз данных; Специалист по тестированию программного обеспечения; Специалист по сопровождению программных продуктов; Специалист по внедрению программного обеспечения

1.2. Конкурентные преимущества образовательной программы

В настоящее время, наряду с Гродненским государственным университетом им.Янки Купалы, подготовку по специальности 6-05-0533-12 Кибербезопасность обеспечивают еще 4 вуза Республики Беларусь: Белорусский государственный университет (БГУ), Витебский государственный университет имени П. М. Машерова (ВГУ), Гомельский государственный университет им. Франциска Скорины (ГГУ), Полоцкий государственный университет имени Евфросинии Полоцкой (ПГУ). Ведущим вузом является БГУ, обеспечивающий подготовку образовательного стандарта по специальности и большинства типовых программ государственного компонента. Особенностью обучения студентов по специальности 6-05-0533-12 Кибербезопасность в БГУ является фундаментальная математическая подготовка в области прикладной математики и криптографии Особенностью обучения студентов по специальности Кибербезопасность в ВГУ, ГГУ, ПГУ является ориентация на приоритет изучения технических и радиофизических средств и методов защиты информации и программно-аппаратные средства обеспечения информационной безопасности.

В структуре факультета математики и информатики подготовка по специальности 6-05-0533-12 Кибербезопасность (с учетом предшествующей ей специальности 6-05-0533-12 Кибербезопасность ведется с 2010-11 уч.года и является одной из самых популярных у абитуриентов. Развитие специальности является одной из приоритетных составляющих политики факультета по подготовке специалистов для сферы ИТ и высокотехнологичных отраслей цифровой экономики.

В учебном процессе специальности мы активно сотрудничаем с признанными мировыми лидерами в области безопасности, такими как компания АО «ИнфоВотч» (Российская Федерация), АО «Позитив Текнолоджис» (Российская Федерация), ЗАО «АВЕСТ» (Республика Беларусь). В научной работе специальности активно изучаются интеллектуальные методы в защите информации, основанные на технологиях искусственного интеллекта и машинного обучения. Во время обучения на факультете студенты специальности имеют возможность получить несколько сертификатов международного образца.

Часть дисциплин специальности интегрирована с учебными планами других ИТ-специальностей факультета: «Программная инженерия», «Прикладная математика», «Управление информационными ресурсами». Это позволяет выстраивать междисциплинарные связи и дает возможность привлекать студентов различных специальностей к командной работе над междисциплинарными проектами, развивая тем самым востребованные универсальные и профессиональные компетенции.

Основные из конкурентных преимуществ обучения по данной специальности:

1. Критическая важность для бизнеса и общества

- Защита ключевых активов: В условиях постоянных кибератак и угроз информационной безопасности компании и государственные учреждения осознают, что кибербезопасность — это не просто техническая задача, а стратегический приоритет. Специалисты по кибербезопасности защищают данные, интеллектуальную собственность и конфиденциальную информацию, что делает их незаменимыми в любой организации.
- Значимость для национальной безопасности: Кибербезопасность имеет огромное значение на уровне государственной безопасности, что делает выпускников востребованными в государственных структурах, оборонной и стратегической отраслях.

2. Высокий спрос на рынке труда

- Увеличивающийся спрос на специалистов: В связи с ростом числа и сложности кибератак, организации по всему миру активно ищут квалифицированных специалистов по кибербезопасности. Это создает стабильные и высокооплачиваемые карьерные возможности для выпускников.
- Множество карьерных направлений: Специалисты по кибербезопасности могут работать в различных отраслях и ролях, включая управление безопасностью, аудит, ана-

лиз угроз, разработку безопасных систем, консультирование и исследовательскую деятельность.

3. Актуальность и динамичность специальности

- Быстрое развитие области: Кибербезопасность — одна из самых динамично развивающихся сфер, что предоставляет специалистам возможность быть на переднем крае технологических новшеств и постоянно развивать свои навыки.

- Реакция на новые угрозы: Появление новых типов кибератак и угроз требует от специалистов постоянного обучения и адаптации, что делает работу в этой сфере интересной и интеллектуально насыщенной.

4. Незаменимость в цифровую эпоху

- Обязательность для цифровой трансформации: Кибербезопасность является основой для успешной цифровой трансформации бизнеса и государственного управления, поскольку без надежной защиты данных любые инновации могут оказаться уязвимыми.

- Комплексный подход к безопасности: Специалисты в этой области обладают знаниями и навыками, позволяющими защищать системы на всех уровнях — от технической защиты до управления рисками и обеспечения соответствия нормативным требованиям.

5. Этическая и социальная значимость

- Защита прав и свобод: Специалисты по кибербезопасности играют ключевую роль в защите прав и свобод граждан, предотвращая несанкционированный доступ к их личным данным и конфиденциальной информации.

- Этические аспекты и ответственность: Выпускники должны соблюдать высокие стандарты этики, поскольку их работа напрямую связана с защитой частной жизни, данных и цифровых прав людей.

6. Глобальная востребованность и международная карьера

- Глобальный характер угроз: Киберугрозы не знают границ, поэтому специалисты по кибербезопасности востребованы по всему миру, что открывает возможности для международной карьеры и участия в глобальных проектах.

- Сотрудничество на международном уровне: Возможность работать в транснациональных корпорациях, международных организациях и сотрудничать с коллегами из разных стран, обмениваясь опытом и лучшими практиками.

7. Способность к адаптации и непрерывному обучению

- Адаптация к новым вызовам: Область кибербезопасности требует от специалистов постоянной адаптации к новым технологиям и угрозам, что развивает их гибкость и способность быстро осваивать новые навыки.

- Постоянное профессиональное развитие: Специалисты по кибербезопасности обязаны постоянно обновлять свои знания и навыки, что делает их востребованными и конкурентоспособными в долгосрочной перспективе.

8. Роль в управлении рисками

- Управление информационными рисками: Специалисты по кибербезопасности играют ключевую роль в управлении и минимизации рисков, связанных с информационными системами и данными, что является критически важным для любого бизнеса.

- Разработка стратегий защиты: Выпускники этой специальности способны разрабатывать и внедрять стратегии киберзащиты, которые позволяют организациям минимизировать последствия возможных атак и быстро восстанавливаться после инцидентов.

9. Командная работа и междисциплинарный подход

- Взаимодействие с различными специалистами: Кибербезопасность требует тесного взаимодействия с другими отделами и специалистами, такими как разработчики, IT-администраторы, менеджеры и юристы, что развивает навыки работы в команде и междисциплинарное мышление.

- Комплексные решения: Специалисты в этой области разрабатывают и внедряют комплексные решения, которые охватывают технические, организационные и правовые аспекты безопасности.

1.2. Компетентностная модель выпускника

После завершения учебы на данной специальности наши выпускники будут обладать, кроме универсальных и базовых профессиональных компетенций, представленных в образовательном стандарте, целым рядом специализированных знаний и компетенций, которые отражают особенности будущей профессиональной деятельности.

Комплексная интегрированная модель конечного результата образования по специальности 6-05-0533-12 Кибербезопасность обеспечивается учебным планом специальности и формирует целостное видение того, каким должен быть выпускник, окончивший обучение по данной специальности в ГрГУ им.Янки Купалы. Основные положения такой модели включают:

1. Цели и задачи образования:

- Формирование профессиональных компетенций, необходимых для защиты информационных систем и данных.
- Подготовка специалистов, способных предотвращать, выявлять и устранять угрозы информационной безопасности.
- Развитие умений в области управления рисками информационной безопасности и обеспечение непрерывности бизнес-процессов.

2. Знания:

- Теоретические основы кибербезопасности: Понимание основных принципов и методов защиты информации, криптографии, сетевой безопасности, управления доступом.
- Законодательные и нормативные акты: Знание законодательства в области защиты информации и персональных данных, стандартов и норм по информационной безопасности.
- Информационные технологии: Глубокое понимание современных информационных технологий, сетевых протоколов, операционных систем, баз данных и программного обеспечения.

3. Умения:

- Проектирование и внедрение систем защиты: Способность разрабатывать и внедрять системы защиты информации на различных уровнях, включая сети, операционные системы и базы данных.
- Анализ и оценка рисков: Умение проводить анализ рисков в области информационной безопасности и разрабатывать мероприятия по их минимизации.
- Построение и управление безопасностью сети: Умение настраивать и управлять сетевыми экранами, системами обнаружения и предотвращения вторжений (IDS/IPS), VPN и другими средствами защиты.
- Мониторинг и реагирование на инциденты: Способность осуществлять мониторинг безопасности, выявлять инциденты и реагировать на них в соответствии с установленными процедурами.

4. Навыки:

- Практическое применение средств защиты: Владение инструментами и программными средствами для обеспечения кибербезопасности, такими как антивирусы, межсетевые экраны, криптографическое ПО.
- Обнаружение и предотвращение кибератак: Навыки проведения тестирования на проникновение (penetration testing), анализа вредоносного ПО, противодействия кибератакам.
- Анализ и обработка данных: Умение использовать средства анализа больших данных и инструментов искусственного интеллекта для выявления угроз.

5. Компетенции:

- Профессиональные: Способность применять полученные знания и навыки для обеспечения информационной безопасности на предприятиях и в организациях различного профиля.

- Аналитические: Способность критически оценивать ситуации, связанные с информационными угрозами, и принимать обоснованные решения.

- Коммуникативные: Умение эффективно взаимодействовать с коллегами, пользователями и руководством, объясняя сложные технические аспекты доступным языком.

- Этические: Осознание этических аспектов кибербезопасности, соблюдение профессиональных стандартов и конфиденциальности.

6. Личностные качества:

- Внимательность и скрупулезность: Важные качества для выявления и устранения уязвимостей в информационных системах.

- Стрессоустойчивость: Способность сохранять спокойствие и принимать правильные решения в условиях кибератак и других кризисных ситуаций.

- Непрерывное самообучение: Готовность постоянно обновлять свои знания в стремительно развивающейся области кибербезопасности.

Эта модель позволяет создать целостное представление о выпускнике по специальности 6-05-0533-12 Кибербезопасность, готовом к выполнению профессиональных задач в условиях современного информационного общества.

Раздел 2. Каталог учебных дисциплин, модулей специальности

6-05-0533-12 Кибербезопасность

Модуль	Учебная дисциплина	Краткое содержание (аннотация)	Цель изучения модуля в структуре профессиональной подготовки, результаты обучения	Общее количество часов	Количество аудиторных часов	Трудоемкость (з.е.)	Форма аттестации
Государственный компонент							
Социально-гуманитарный модуль-1	История белорусской государственности	Формирование устойчивых представлений об историческом прошлом и направлениях дальнейшего развития белорусского государства с целью формирование обоснованной патриотической позиции.	*Цель модуля:* развить способность формирования гражданской идентичности, культуры мышления и гуманистического мировоззрения. *Результаты обучения позволят:* - обладать способностью анализировать процессы государственного строительства в разные исторические периоды; - выявлять факторы и механизмы исторических изменений, определять социально-политическое значение исторических событий (личностей, артефактов и символов) для современной белорусской государственности; - использовать выявленные закономерности в процессе формирования гражданской идентичности; - обладать современной культурой мышления, гуманистическим мировоззрением, аналитическим и инновационно-критическим стилем познавательной, социально-практической и коммуникативной деятельности; - использовать основы философских знаний в профессиональной деятельности, самостоя-	108	54	3	экзамен
	Философия	Освоение студентами наследия мировой и отечественной философской мысли, формирование у них творческого отношения к этому наследию, развитие навыков самостоятельного философского мышления, что позволяет адекватно оценить фундаментальные особенности развития современной культуры и цивилизационное многообразие современного мира.		108	54	3	экзамен
	Современная политэкономия	Формирование у студентов целостной картины мира, понимания сущности социальных, экономических и политических явлений и процессов, происходящих в белорусском обществе и мире		108	54	3	экзамен

		под воздействием внутренних политико-экономических факторов и трансформации глобальной социально-экономической среды и современного миропорядка.	тельно усваивать философские знания и выстраивать на их основании мировоззренческую позицию; - обладать способностью анализировать экономическую систему общества в ее динамике, законы ее функционирования и развития для понимания факторов возникновения и направлений развития современных социально-экономических систем; - использовать инструменты экономического анализа для оценки политического процесса принятия экономических решений и результативности экономической политики.				
Иностранный язык	Иностранный язык (английский)	Подготовка студентов к активному и полноценному сотрудничеству в современном поликультурном мире средствами иностранного языка, что предполагает формирование коммуникативной компетенции.	*Цель модуля:* развить компетенции устной и письменной коммуникации для решения задач межличностного, профессионального и межкультурного взаимодействия на иностранном языке. *Результаты обучения позволят:* - осуществлять коммуникации на иностранном языке, для решения задач межличностного, профессионального и межкультурного взаимодействия; - использовать основные понятия и термины специальной лексики иностранного языка в профессиональной деятельности.	340	204	9	зачет, экзамен
Модуль «Высшая математика»	Математический анализ	Подготовка специалиста с развитым логическим и алгоритмическим мышлением, владеющего основными методами исследования и решения математических задач и способного самостоятельно расширять математические знания и проводить постановку и математический анализ прикладных задач.	*Цель модуля:* сформировать навыки применения математических методов для построения и исследования математических моделей прикладных и инженерных задач. *Результаты обучения позволят:* - применять аппарат дифференциального и интегрального исчисления, методы аналитической геометрии и линейной алгебры для построения математических моделей и решения прикладных задач;	432	256	12	зачет, экзамен

	Аналитическая геометрия и линейная алгебра	Формирование у студентов компетенций в области аналитических методов обработки информации на основе изучения основных геометрических фигур, алгебраических объектов и структур.	- Строить вероятностные модели в прикладных задачах, вычислять вероятности сложных случайных событий и исследовать важнейшие характеристики случайных величин, использовать методы математической статистики для решения задач оценивания параметров и проверки гипотез, применять методы анализа основных моделей случайных процессов	216	136	6	экзамен
	Дифференциальные уравнения	Формирование у студентов умения решать задачи дифференциального исчисления, использовать методы дифференциального исчисления при построении и исследовании математических моделей естественнонаучных процессов		108	68	3	экзамен
	Теория вероятностей и математическая статистика	Освоение основ теории вероятностей, необходимых для решения прикладных задач, а также приобретение навыков самостоятельного изучения литературы по данной учебной дисциплине и ее приложениям; развитие логического и алгоритмического мышления.		198	76	6	экзамен
Модуль «Программирование»	Программирование на C++	Формирование практических навыков построения, анализа и реализации алгоритмов и структур данных для решения прикладных задач; освоение методов конструирования ПО с использованием языков программирования высокого уровня, популярных сред и платформ разработки.	*Цель модуля: с*формировать практические навыки построения, анализа и реализации алгоритмов и структур данных для решения прикладных задач; освоение методов конструирования ПО с использованием языков программирования высокого уровня, популярных сред и платформ разработки. *Результаты обучения позволят:* - решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий; - Строить, анализировать и тестировать алгоритмы и программы решения типовых задач	396	192	12	зачет, экзамен

			обработки информации с использованием структурного, объектно-ориентированного и иных парадигм программирования				
Модуль «Информатика и компьютерные системы»	Базы данных	Приобретение устойчивых теоретических знаний и практических навыков в области разработки и эксплуатации баз данных, использования средств автоматизированного проектирования баз данных и программных продуктов, реализующих функционирование баз данных и управление ими.	*Цель модуля:* формирование системного подхода к пониманию и использованию фундаментальных принципов структурной организации, архитектурных принципов, принципов управления и функционированию компьютерных систем, в том числе архитектуры современных компьютеров, использования операционных систем, компьютерных сетей и баз данных. *Результаты обучения позволят:* - проектировать и разрабатывать реляционные базы данных средствами современных систем управления базами данных; - применять знания в области принципов функционирования, архитектур и программных реализаций операционных систем для организации вычислительных процессов; - использовать, конфигурировать и проектировать проводные и беспроводные компьютерные сети.	108	60	3	зачет
	Курсовой проект по дисциплине «Базы данных»	В процессе выполнения студенты усваивают теоретические основы организации баз данных, включая принципы их построения на концептуальном, логическом и физическом уровнях, учатся ставить и решать практические задачи проектирования и сопровождения баз данных, развивают навыки использования современных CASE-средств, СУБД и прикладных сред разработки для создания информационных систем с базами данных.		40	0	1	защита курсового проекта
	Архитектура компьютеров	Ознакомление с принципами создания и типами организации классических и альтернативных архитектур современных компьютеров, а также наиболее значительными их реализациями. Изучение внутренней организации вычислительной системы.		108	58	3	экзамен

	Операционные системы	Формирование фундаментальных знаний об основных концепциях построения и функционирования операционных систем, их общих характеристиках и наиболее значимых реализациях на современных платформах.		108	60	3	экзамен
	Компьютерные сети	Освоение теоретических основ построения и принципов функционирования современных компьютерных сетей, а также получения практических навыков по их использованию при постановке задачи, проектировании и эксплуатации сетей.		108	68	3	экзамен
Модуль «Безопасность информационных технологий»	Основы кибербезопасности	Изучение дисциплины позволит студентам углубить свои знания в области кибербезопасности, а также о технологиях и процедурах, используемых для защиты сетей. Позволит убедиться в правильности выбора дальнейшей работы в качестве сетевого специалиста или специалиста в области сетевой безопасности начального уровня.	*Цель модуля:* формирование специалиста, владеющего фундаментальными знаниями и практическими навыками в области основ кибербезопасности, криптографических методов защиты информации, понимающего проблемы и методы защиты компьютерных информационных систем, пользователей и их данных. *Результаты обучения позволят:* - 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; - определять уязвимости и предотвращать киберугрозы, владеть методами и средствами защиты от атак злоумышленников на компьютерные системы, включая информационные системы и сети, мобильные устройства; уметь обнаруживать вторжения и обеспечивать защиту персональных данных;	90	36	3	экзамен
	Криптографические методы защиты информации	Дисциплина знакомит студентов с методами построения криптографических преобразований, а также методами опенки их надежности, дает представление об основных типах криптографических систем: блочных, поточных, криптосистемах с открытым ключом, систем электронной цифровой подписи, функций хэширования.		108	60	3	зачет

	Безопасность информационных систем	Формирование фундаментальных знаний и приобретение практических навыков в области разработки программных продуктов, ориентированных на обеспечение безопасности систем обработки данных, защищенных от несанкционированного использования	- знать характеристики, уметь применять с учетом особенностей и назначения, оценивать надежность криптографических алгоритмов и криптосистем, в том числе функций хэширования и систем электронной цифровой подписи; - применять методы и средства администрирования и мониторинга для управления пользователями и ресурсами информационных систем с целью обеспечения требуемой производительности и безопасности.	306	144	9	зачет, экзамен
Компонент учреждения образования							
Социально-гуманитарный модуль-2	Политология	Формирование знаний о политике, политической системе и политических процессах, нормах конструктивной политической гражданской культуры и общественно значимых ценностях идеологии белорусского государства.	*Цель модуля:* формирование системы знаний о политической системе и политических процессах и общественно значимых ценностях идеологии белорусского государства, о социально-психологических особенностях и закономерностях поведения личности, а также межличностных и групповых феноменах и процессах. *Результаты обучения позволят:* - знать и уметь характеризовать сущность, структуру политических институтов и процессов в современном мире и Республике Беларусь; - знать принципы, цели и основные задачи внутренней политики Республики Беларусь; - участвовать в формировании политической системы белорусского общества как избиратель, проявлять культуру конструктивного политического участия; - владеть навыками определения и анализа внешне- и внутриполитических задач современного государства; - знать основные области прикладных социально-психологических исследований;	72	36	2	диф. зачет
	Межличностная коммуникация	Усвоение сущности, закономерностей, принципов, условий и факторов формирования межличностной коммуникации; освоение умений организации совместной деятельности, общения людей, предупреждения и решения конфликтов, обучения и повышение квалификации персонала; управление коллективом, освоение навыков и умений подготовки публичного выступления; подготовки визуальных, звуковых и текстовых информационных материалов, установления контакта с аудиторией; развитие профессиональной культуры поведения и др.		72	36	2	диф. зачет

	Дисциплины по выбору: 1. Социальная психология 2. Психология организационных коммуникаций	Формирование системы знаний о социально-психологических особенностях и закономерностях поведения личности, а также межличностных и групповых феноменах и процессах.	- уметь определять социально-психологические характеристики личности и группы и учитывать их при решении личных, социальных и профессиональных задач; - владеть навыками анализа различных форм социального поведения личности и группы, методами анализа влияния социального контекста на поведение, социально-психологическими методами решения воспитательных, профессиональных и управленческих задач.	72	36	2	диф. зачет
		Получение теоретических знаний и диагностических умений в области анализа организационных коммуникаций; раскрытие социально-психологической проблематики изучения организационных коммуникаций; осмысление феноменологии делового взаимодействия, эффектов восприятия и понимания в деловой коммуникации; специфики информационного обмена в организации; формирование у студентов интерпретативного подхода к анализу и пониманию организационного поведения сотрудников; обозначение перспективы дальнейшего развития психологии организационных коммуникаций в свете достижений современной науки и практики.		72	36	2	диф. зачет
Модуль «Программирование-2»	Язык программирования Python	В настоящее время Python - самый популярный язык программирования в мире. На Python пишут веб-приложения и нейронные сети, решают задачи кибербезопасности, проводят научные исследования и автоматизируют процессы. Знание языка Python является необходимым атрибутом не только для специалистов по	*Цели модуля:* 1. Формирование практических навыков построения, анализа и реализации алгоритмов и структур данных для решения прикладных задач; освоение методов конструирования ПО с использованием языков программирования высокого уровня, популярных сред и платформ разработки;	108	62	3	экзамен

		искусственному интеллекту и кибербезопасности, но и для любого успешного ИТ-специалиста.	2. Формирование систематизированного представления о международных стандартах и методах программной инженерии, применяемых для проектирования, разработки, сопровождения и документирования тиражируемых программных продуктов, соответствующих требованиям заказчика; *Результаты обучения позволят:* - строить, анализировать и тестировать алгоритмы и программы решения типовых задач обработки информации с использованием структурного, объектно-ориентированного и иных парадигм программирования; - анализировать и тестировать программы типовых задач на основе бинарного кода с использованием средств декомпиляции и дисассемблирования; - применять язык программирования Python для разработки компьютерных и мобильных приложений, владеть базовыми навыками программирования с целью дальнейшего использования языка в машинном обучении и анализе данных;				
	Разработка кросс-платформенных приложений	Ознакомление с теорией и практикой разработки платформенно-независимых приложений, объектно-ориентированным языком Java и формирование целостного представления о принципах использования Java-технологии в различных областях программирования.		216	92	6	экзамен
	Машинно-ориентированное программирование	Систематизированная подготовка специалиста, владеющего технологиями создания и использования формализованных языков, предназначенных для описания программ и алгоритмов решения задач на ЭВМ.		108	34	3	зачет
	Промышленное программирование	Систематизированная подготовка специалиста, способного осуществлять промышленную разработку программного обеспечения, масштабных высокобюджетных проектов, рассчитанных на широкую аудиторию и различные бизнес-потребности, с использованием средств и фреймворков платформы .NET.		216	136	6	зачет, экзамен
	Технологии программирования	Формирование знаний основ методологии в области разработки программного обеспечения; систематизация и углубление знаний и умений в области информационных технологий; изучение основных приёмов и методов разработки программных продуктов;		108	68	3	зачет

		освоение оценки качества программного обеспечения.					
Модуль «Дискретная математика и алгоритмы»	Дискретная математика и математическая логика	Обучение методам решения задач, характерных для дискретной математики, и соответствующему логико-комбинаторному стилю мышления, формирование современного математического кругозора, овладение навыками логико-комбинаторного мышления.	*Цель модуля:* формирование навыков формализации и решения прикладных задач с помощью численных методов, методов дискретной и конструктивной математики, методов анализа алгоритмов и структур данных. *Результаты обучения позволят:* - понимать предмет и объекты дискретной математики и математической логики; - использовать основные приемы разработки эффективных алгоритмов и знания об основных структурах данных для решения прикладных задач.	216	128	6	зачет, экзамен
	Алгоритмы и структуры данных	Изучение подходов к разработке эффективных алгоритмов для разнообразных задач дискретной и комбинаторной оптимизации.		108	68	3	зачет
Юридический модуль	Основы управления интеллектуальной собственностью	Изучение общих вопросов оформления, регистрации и реализации прав на результаты интеллектуальной деятельности, а также в привитии навыков проведения патентно-информационного поиска, в том числе с использованием Интернет.	*Цель модуля:* формирование представления о юридических аспектах управления интеллектуальной собственностью и правовом обеспечении информационной деятельности в соответствии с законодательством Республики Беларусь об информации, информатизации и защите информации. *Результаты обучения позволят:* - знать процедуры оформления, регистрации и реализации прав на результаты интеллектуальной деятельности; - владеть навыками проведения патентных исследований, в том числе с использованием Интернет; - владеть навыками подготовки договоров, заключаемых в сфере интеллектуальной собственности; - знать и применять основы правового регулирования отношений в информационной сфере; - определять правовой статус средств распространения информации; - использовать правовые способы и средства защиты информации.	72	34	2	зачет
	Организационно-правовое обеспечение информационной безопасности	Обучение правилам построения и использования современных защищенных информационных компьютерно-коммуникационных систем, правилам защиты информационных ресурсов.		72	68	2	зачет

Модуль «Обеспечение безопасности компьютерных систем»	Инструментальные средства обеспечения безопасности	Ознакомление со средствами обеспечения безопасности и анализа системы; средствами для атак и исследования систем в сети; средствами системного и сетевого аудита, а также средствами, используемыми в судебной практике и при расследовании инцидентов, связанных со взломом компьютерных систем.	*Цель модуля:* формирование фундаментальных знаний и практических навыков в области аппаратного и программного обеспечения компьютерных систем, инструментальных средств обеспечения безопасности, организации и функционирования и безопасности систем на основе блокчейна и Интернета вещей. *Результаты обучения позволят:* - решать профессиональные задачи с учетом архитектурных особенностей компьютерных систем, принципов их организации и функционирования; - применять современные специализированные средства для исследования безопасности сетевых ресурсов, сетевого аудита, расследования инцидентов, связанных с нарушением защиты компьютерных систем; - применять технологию блокчейн для решения широкого круга задач; разрабатывать децентрализованные приложения и смарт-контракты; анализировать и оценивать криптовалютные платежные системы; - использовать базовые технологии Интернета Вещей для подключения объектов к сети Интернета Вещей, для проектирования и создания полноценных IoT-решений и систем; - применять стратегии минимизации рисков, использовать современные инструменты для анализа уязвимостей решений и сетей Интернета Вещей, выявлять проникновения; - применять стеганографические методы и алгоритмы для решения задач защиты информации в компьютерных системах, осуществлять стеганографический анализ для обнаружения и противодействия несанкционированной передаче данных.	80	48	2	зачет
	Основы защиты информации	Получение базовых знаний по вопросам обеспечения защиты информации в условиях различных по виду, происхождению и характеру реализации угроз.		80	64	2	экзамен
	Технологии Интернета Вещей (IoT)	Получение представлений о концепции Умного дома, о цифровой трансформации бизнеса, о беспрецедентных экономических возможностях концепции Умного города, как Интернет вещей изменяет такие сферы как здравоохранение, городское хозяйство и заводы-автоматы.		80	50	2	экзамен
	Безопасность систем Интернета Вещей	Получение представлений как уменьшить уровень риска и использовать современные инструменты для анализа уязвимостей решений и сетей Интернета Вещей, какие устройства выбрать для домашней автоматизации или для промышленной системы.		120	64	3	экзамен
	Основы криптоанализа	Приобретение знаний о важнейших разделах криптоанализа и формирование достаточно глубоких знаний о моделях угроз, криптоанализе исторических		108	50	3	зачет

		шифров, основных методах современного криптоанализа и возможностях его применения.					
	Технология блокчейн и криптовалюта	Ознакомление с современным состоянием, проблемами и достижениями в области применения технологии блокчейн, цифровых и криптовалютных платежных систем.		120	58	3	экзамен
Модуль «Обеспечение безопасности компьютерных систем». Дисциплины по выбору	Компьютерная стеганография	Изучение особенностей применения стеганографии и предъявляемых к ней требования, атаки на стегосистемы и технологии противодействия им, оценки стойкости стеганографических систем и условия их достижения, а также алгоритмы встраивания информации в тексты, изображения, видеопоследовательности и аудиосигналы.	*Цель модуля:* формирование базовых знаний в области классических методов криптоанализа и современных направлений развития компьютерной техники и связанных с этим новых подходов к защите информации. *Результаты обучения позволят:* - владеть методами криптоанализа для восстановления открытых текстов и/или ключей с целью обнаружения слабых мест в системах криптографической защиты информации в компьютерных системах; - обеспечивать передачу секретной информации на основе квантовых криптографических протоколов, использовать экспериментальные реализации квантовой криптографии	108	50	3	зачет
	Квантовая криптография	Обеспечение подготовки в новой области современных исследований - квантовой криптографии: освоение математического аппарата, используемого для задач квантовой криптографии; освоение принципов работы базовых квантовых криптографических протоколов распределения ключей; освоение принципов работы волоконно-оптических систем квантового распределения ключей, а также систем квантовой криптографии, работающих через открытое пространство.		108	50	3	зачет

Модуль «Обеспечение безопасности бизнеса»	Компьютерная криминалистика	Знакомство с методами оперативно-розыскной и следственной деятельности в области компьютерной криминалистики с целью раскрытия преступлений в сфере высоких технологий. Способами получения значимой информации, ее анализом и документированием. Ролью и методами компьютерно-технической экспертизы и экспертизы радиоэлектронных устройств в компьютерной криминалистике.	*Цель модуля:* формирование базовых знаний в области форензики (компьютерной криминалистики), аудита систем обеспечения безопасности и исследования информационных систем на наличие уязвимостей. *Результаты обучения позволят:* - владеть методами и инструментами для сбора и исследования цифровых доказательств с целью раскрытия преступлений в сфере высоких технологий, а также для восстановления данных; - выполнять объективную оценку уровня организационной и технической безопасности информационных ресурсов, соответствия стандартам информационной безопасности; обнаруживать уязвимости и слабые места; владеть методиками и инструментами проведения тестов на проникновение.	120	68	3	экзамен
	Аудит и тестирование безопасности	Получение базовых знаний по методам аудита и тестирования безопасности, необходимых для изучения современных подходов к построению безопасных информационных систем и сетей. В центре внимания дисциплины - принципы и методы пентеста (пентестинга) — тестирования безопасности на проникновение, понимаемого как комплекс мер, которые имитируют реальную атаку на сеть или приложение.		108	60	3	зачет
Модуль «Обеспечение безопасности бизнеса».	Оптимизация и обеспечение безопасности web-приложений	Подготовка специалистов, владеющих знаниями в области обеспечения базовой безопасности web-приложений. Приобретение теоретических знаний и практических навыков для разработки безопасных web-приложений. Изучение технологий JavaScript, MySQL, NoSQL DB, Python, Node.js для разработки web-приложений.	*Цель модуля:* формирование практических навыков разработки программного обеспечения для различных аппаратных платформ и операционных систем, навыков разработки веб-и мобильных приложений. *Результаты обучения позволят:* - выполнять анализ эффективности работы web-приложений и осуществлять оптимизацию с целью их продвижения в сети Интернет;	108	60	3	зачет

Дисциплины по выбору 1	Разработка, оптимизация и обеспечение безопасности сайтов	Подготовка специалистов, владеющих знаниями в области обеспечения базовой безопасности web-приложений. Приобретение теоретических знаний и практических навыков для разработки безопасных web-приложений. Изучение технологий JavaScript, MySQL, NoSQL DB, Python, Node.js для разработки web-приложений.	- осуществлять аудит безопасности и модернизацию web-приложений в соответствии с регламентами по безопасности; - применять современные технологии и инструментальные средства для разработки, оптимизации и обеспечения безопасности web-сайтов.	108	60	3	зачет
Модуль «Обеспечение безопасности бизнеса». Дисциплины по выбору 2	Интеллектуальные методы в решении задач защиты информации	Формирование теоретических и практических знаний в области интеллектуальных методов и машинного обучения, современных методов восстановления зависимостей по эмпирическим данным.	*Цель модуля:* формирование теоретических знаний и практических навыков использования и разработки интеллектуальных методов в сфере защиты информации, в сфере интеллектуальных технологий цифровизации бизнеса автоматизации, роботизации и Интернета вещей. *Результаты обучения позволят:* - проектировать и использовать системы интеллектуального анализа и принятия решений для идентификации уязвимостей и атак в области компьютерной и информационной безопасности; - обеспечивать цифровую трансформацию и реинжиниринг бизнес-процессов организации на основе внедрения интеллектуальных методов принятия решений и технологий Интернета Вещей с учетом вопросов их многоуровневой безопасности.	108	64	3	зачет
	Смарт-технологии автоматизации и реинжиниринга бизнеса	Формирование знаний о современном состоянии и лучшем опыте использования прорывных технологий цифровизации в бизнесе (искусственный интеллект, блокчейн, интернет вещей и др.); о разработке корпоративных стратегий, ключевых бизнес-моделей и кейсов цифровой трансформации на основе современных компетенций Agile, Lean Startup, DevOps с учетом безопасности и непрерывности бизнеса.		108	64	3	зачет
Модуль «Анализ данных и	Методология и инструменты анализа данных	Формирование теоретических и практических знаний в области технологий подготовки и анализа данных, машинного обучения, со-	*Цель модуля:* формирование теоретических знаний и практических навыков в области статистических методов обработки и анализа данных, ориентированных на профессиональную	120	84	3	экзамен

машинное обучение в системах защиты информации»	Курсовая работа по учебной дисциплине «Методология и инструменты анализа данных»	временных методов восстановления зависимостей по эмпирическим данным. Полученные практические навыки позволят использовать популярные инструменты для проведения исследования моделей и методов анализа данных на примере решения задач сегментации, кластеризации, классификации, прогнозирования.	деятельность специалиста по защите информации, их практическое применение, в том числе с использованием современных методологий, инструментов анализа данных, методов машинного обучения и нейросетевых технологий обработки информации *Результаты обучения позволят:* - использовать принципы, методы, модели и инструменты анализа данных для разработки алгоритмов и решения практических задач обработки информации; - проектировать, разрабатывать и применять системы интеллектуального анализа и принятия решений на основе нейронных сетей и методов машинного обучения в области компьютерной и информационной безопасности и искусственного интеллекта.	40	0	1	защита курсовой работы
	Машинное обучение и нейронные сети	Ознакомление с моделями для задач классификации, регрессии, кластеризации, методами обучения таких моделей, нейронными сетями различных архитектур, а также методами применения нейронных сетей в задачах компьютерного зрения и распознавания текстов естестсетвенного языка.		228	102	6	зачет, экзамен
	Курсовой проект по учебной дисциплине «Машинное обучение и нейронные сети»			72	0	2	защита курсового проекта
Модуль «Анализ данных и машинное обучение в системах защиты	Технологии компьютерного зрения	Изучение методов цифровой обработки изображений с элементами машинного обучения. Изучаемые в курсе алгоритмы применяются при проектировании автономных устройств (роботов), а также используются в системах интеллектуального видеонаблюдения и в задачах интеллектуальной обработки изображений. похожести.	*Цель модуля:* формирование теоретических знаний и практических навыков в области современных интеллектуальных информационных систем и технологий, основанных на технологиях распознавания образов, компьютерного зрения и интеллектуального видеонаблюдения, технологиях синтеза и анализа голоса и голосовой биометрии. *Результаты обучения позволят:*	120	70	3	зачет

информации». Дисциплины по выбору	Речевые технологии и голосовая биометрия	Получение знаний и навыков, позволяющих профессионально использовать технологии и системы распознавания голоса и синтеза речи. Решать задачи обеспечения безопасности объектов защиты на основе методов динамической биометрии и биометрической идентификации на основе голоса, задачи создания голосовых модулей для интеллектуальных и робототехнических систем.	- владеть технологиями искусственного интеллекта, связанными с анализом изображений и видео; - решать профессиональные задачи обеспечения безопасности объектов защиты на основе технологий компьютерного зрения и интеллектуального видеонаблюдения; - владеть технологиями и системами распознавания голоса, синтеза речи; - решать профессиональные задачи обеспечения безопасности объектов защиты на основе методов динамической биометрии и биометрической идентификации на основе голоса.	120	70	3	зачет
Модуль «Актуальные проблемы кибербезопасности»	Спецсеминар	Развитие профессионального кругозора, искусства публичных выступлений и коммуникационных навыков будущих специалистов по защите информации. Семинар проводится в форме публичных выступлений студентов по самым актуальным вопросам и сопровождается дискуссией. Участие в семинаре способствует активизации научных исследований, развивает навыки профессионального общения и ведения дискуссий в области профессиональных компетенций.	*Цель модуля:* формирование теоретических знаний и практических навыков в области современных систем и методов защиты информации, методов обеспечения доступа на основе биометрических технологий, разработки защищенных приложений. *Результаты обучения позволят:* - применять методы информационного поиска и научного исследования, развивать навыки профессионального общения и ведения дискуссий в области профессиональных компетенций; - владеть методами и алгоритмами биометрической идентификации; - разрабатывать решения в сфере контроля и управления доступом к защищенным объектам на основе методов биометрической идентификации; - использовать биометрические системы контроля и управления доступом; - применять методы и средства администрирования и мониторинга для управления пользователями и ресурсами информационных систем с целью обеспечения требуемой производительности и безопасности;	144	68	4	зачет
	Биометрия и управление доступом	Теоретическая и практическая подготовка студентов в области создания и применения биометрических систем контроля управления доступом на защищенные объекты и защиты информации биометрическими методами при ее создании, обработке, передаче и хранении. Закрепление теорети-		108	50	3	зачет

		ческого материала путем приобретения навыков выполнения экспериментов с устройствами биометрии, обработки и анализа полученных биометрических данных.	- решать профессиональные задачи обеспечения безопасности компьютерных сетей, сетевых устройств и данных, используя реальное сетевое оборудование и средства моделирования сетей; - обеспечивать защиту создаваемых приложений на всех этапах процесса создания программного обеспечения - от проектирования безопасных приложений и до тестирования для выявления уязвимостей и создания безопасной документации.				
	Безопасность компьютерных сетей	В рамках дисциплины ставится задача подготовки специалиста, владеющего основами обеспечения безопасности информационных систем от различного рода воздействий, которые способны привести к потере или искажению обрабатываемой, или управляющей информации, а также умеющего противодействовать удаленным сетевым атакам на компьютерные системы и применять методы комплексной защиты.		216	100	6	экзамен
	Разработка защищенных приложений	Обучение принципам и особенностям построения защищённых приложений. Особое внимание обращается на вопросы защиты приложений от взлома и компрометации. Задача – дать основы построения защищённых приложений, методов, способов, механизмов и средств защиты приложений.		108	44	3	зачет
Модуль «Актуальные проблемы	Актуальные проблемы защиты информации	Дисциплина направлена на усвоение студентами основ защиты личных данных в соответствии с требованиями современного информационного права и законодательства в информационной сфере; формирования у студентов навыков современных методов	*Цель модуля:* формирование знаний и практических навыков по обеспечению защиты информации в условиях современных угроз информационной безопасности, защиты промышленных предприятий и производственной сферы, защиты личных данных при их хранении, обработке и передаче. *Результаты обучения позволят:*	108	44	3	экзамен

кибербезопасности». Дисциплины по выбору		анализа понятий и категорий, институтов, правоотношений, связанных с ними проблем, и умение находить пути их разрешения; овладение студентами навыками определения места защиты личных данных и элементов информационного права.	- использовать в профессиональной деятельности современные и перспективные достижения в области защиты информации и компьютерной безопасности; - - использовать в профессиональной деятельности современные и перспективные достижения в области защиты производственной сферы промышленных предприятий и бизнеса, защиты и анализа корпоративных данных				
	Кибербезопасность промышленных сред и бизнеса	В рамках дисциплины рассматриваются методы защиты промышленных предприятий и критически важных объектов, технологических процессов и корпторитивных данных с использованием решений ведущих компний в области кибербезопасности.		108	44	3	экзамен
Модуль «Современные платформы программирования». Дисциплины по выбору	Современные платформы программирования	Введение в программирование на языке Java. Типы данных и переменные в языке Java. Выражения и операции. Массивы в Java. Классы и объекты. Инкапсуляция. Класс Object. Наследование. Классы обёртки. Абстрактные классы. Интерфейсы и перечисления. Обработка строк. Исключительные ситуации. Обобщенное программирование Стандартные коллекции. Потоки ввода/вывода. Работа с файловой системой. Основы программирования на языке C#. Делегаты, лямбды, события. Обработка исключений. Строки и работа с файловой системой. Коллекции. Технология LINQ. Основы юнит-тестирования. Технология ASP.NET Core	*Цель модуля:* 1) формирование навыков решения задач, требующих реализацию алгоритмов на современных языках программирования, навыков использования современных платформ и средств разработки программного обеспечения для создания интеллектуальных систем. 2) углублённое изучение теории квантовой обработки информации, теории квантовых вычислений и квантовых алгоритмов, так и необходимые разделы физики, лежащие в основе физических моделей квантовых вычислений. *Результаты обучения позволят:* - использовать для разработки и исполнения прикладных программ современные среды программирования с учётом накладываемых этими средами ограничений и предоставляемых возможностей; - использовать квантовые технологии, экспериментальные системы и облачные платформы	216	90	6	экзамен

	Квантовые системы и технологии	Ознакомление студентов с современными достижениями в области прикладных квантовых технологий; формирование понятий и представлений о перспективных информационных технологиях, основанных на фундаментальных принципах квантовой механики, использовании квантовых компьютеров и квантовых вычислений; дать навыки математического моделирования систем функционирующих по принципам квантовой механики.	для решения исследовательских и прикладных бизнес-задач с помощью квантовых вычислений.	216	90	6	экзамен
Модуль «Курсовое проектирование по специальности»	Курсовой проект	Развитие и проверка полученных навыков и знаний, закрепление их при исследовании различных аспектов, связанных как с теоретической, так и с практической сферами деятельности, связанных с содержанием большинства разделов дисциплин учебного плана.	*Цель модуля:* обеспечить развитие и проверку полученных навыков и знаний, закрепление их при исследовании различных аспектов, связанных как с теоретической, так и с практической сферами деятельности, связанных с содержанием большинства разделов дисциплин учебного плана. *Результаты обучения позволят:* - владеть основами исследовательской деятельности, осуществлять поиск, анализ и синтез информации; - решать стандартные задачи профессиональной деятельности на основе применения информационно-коммуникационных технологий; - обладать навыками саморазвития и совершенствования в профессиональной деятельности; - проявлять инициативу и адаптироваться к изменениям в профессиональной деятельности; - обладать навыками творческого аналитического мышления.	144	0	4	защита курсового проекта
	Курсовая работа			40	0	1	защита курсовой работы
Практики							
Учебные практики	По программированию	Закрепление полученных знаний за соответствующий год обучения через решение специальных	*Цель модуля:* профориентация и погружение в IT, формирование представления о профессиях			4	диф. зачет

		учебных заданий, участие в работе над общим коллективным проектом.	и направлениях специализации в IT-сфере, востребованных на рынке труда компетенциях, направлениях профессионального развития и карьерного роста в области кибербезопасности и защиты информации. *Результаты обучения позволят:* - ориентироваться в IT-профессиях и инструментах обучения выбранной специализации; - знать основные направления деятельности специализированных компаний и используемые технологии защиты и продукты; - владеть основами работы с системой контроля версий git, веб-сервисами для хостинга IT-проектов и их совместной разработки Github/GitLab.				
	Информационно-аналитическая	Освоение принципов организации и управления информационными системами; освоение методов и средств получения, хранения и обработки информации предприятия; изучение требований и ознакомление с конкретными проектами различных системных программ и средств ИС, методами с средствами обеспечения их безопасности.				4	диф. зачет
Производственные практики	Технологическая	Формирование в условиях производства профессиональных способностей студента на основе использования его теоретических знаний в различных ситуациях, свойственных будущей профессиональной деятельности специалиста.	*Цель модуля:* закрепить навыки исследовательской работы, глубоко анализа предметной области и постановки задачи, формирования требований к обеспечению кибербезопасности и защиты информации, обоснованного выбора математических, алгоритмических и технологических инструментов работы над проектом в сфере интеллектуальных и/или компьютерных систем, определения требований по защите информации, проектирования и программной реализации ПО. *Результаты обучения позволят:* - осуществлять анализ предметной области задачи, связанной с анализом защищенности и разработкой методов защиты объекта; - формулировать функциональные и нефункциональные требования к построению политики безопасности, моделей и средств защиты; - осуществлять обоснованный выбор средств и технологий моделирования, проектирования и разработки в соответствии с ресурсами и ограничениями проекта;			5	диф. зачет
	Преддипломная	Преддипломная практика является частью общего учебного процесса подготовки специалистов, продолжением учебного процесса в производственных условиях, проводится на промышленных предприятиях, в научных учреждениях, предприятиях, разрабатывающих программное обеспечение, банках и др.				15	диф. зачет

			- выполнять программную реализацию поставленных задач; - оценивать эффективность реализованных проектов.				

Раздел 3. План развития образовательной программы

3.1. Перечень мероприятий по развитию образовательной программы

3.1.1. Учебный процесс

3.1.1.1. Выпускающей кафедрой ведется интенсивная и результативная профориентационная работа по организации набора абитуриентов. Используются как традиционные средства (встречи, беседы, дни открытых дверей), так и проведение мероприятий на основе ИТ (видеоконференции, квесты, профильные олимпиады).

Основная задача в рамках этой инициативы – привлечь наиболее талантливых и мотивированных абитуриентов, проживающих не только в г.Гродно и Гродненской области. Для этого необходимо расширять географию как реального, так и виртуального присутствия ГрГУ им.Янки Купалы в других регионах Республики Беларусь (и странах ближнего и дальнего зарубежья). Но не менее важно сохранить качество привлекаемых абитуриентов и обеспечить большой конкурс на специальность.

Для реализации этой инициативы планируется взаимодействовать с агентствами в области образовательного рекрутинга студентов, участвовать в образовательных ярмарках; развивать интернет-школу при факультете математики и информатики, внедрить новые дистанционные форматы профессиональной ориентации и подготовки потенциальных абитуриентов; запустить летние и зимние программы профессиональной ориентации и новые конкурсы; обеспечить для региональных студентов – возможность академической мобильности и включения в международные лаборатории, а также, помимо повышения качества образовательных программ, возможность снижение оплаты за обучение и получения грантов Университета на оплату обучения и проживания.

План мероприятий в направлении профориентационной работы представлен в таблице 3.1.

Таблица 3.1. Перечень мероприятий в области профориентационной и маркетинговой деятельности.

№	Наименование мероприятия	Срок исполнения	Ответственный	Ресурсы, источник финансирования	Отметка о выполнении
1.	Исследование информации базы данных потенциальных абитуриентов	Постоянно, после получения информации о ходе РТ и ЦТ	ППС кафедры СПКБ	Не требуются	
2.	Взаимодействие с предприятиями-заказчиками кадров, приглашение к участию в профориентационных мероприятиях	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуются	
3.	Взаимодействие с рекрутинговыми агентствами и предприятиями-заказчиками кадров с целью информирования о компетенциях выпускников с квалификацией «Специалист по кибербезопасности»	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуются	

4.	Взаимодействие с предприятиями-заказчиками кадров, приглашение к участию в профориентационных мероприятиях	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуются	
5.	Взаимодействие с предприятиями-заказчиками кадров, приглашение к участию в профориентационных мероприятиях	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуются	
6.	Актуализация информации на сайтах республиканского уровня и сайте факультета с целью информирования абитуриентов о специальностях кафедры	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуются	
7.	Организация экскурсий школьников г. Гродно и области для знакомства со специальностями кафедры	По отдельному графику	ППС кафедры СПКБ, Зав. кафедрой СПКБ	Не требуются	
8.	Профориентационная работа в школах региона, проводимая иногородними студентами в «своих» школах	Согласно плану работы кафедры	ППС кафедры СПКБ	Не требуются	
9.	Геймификация профориентационной работы. Организация и проведение веб-квестов и веб-конкурсов для абитуриентов в формате CTF	Январь-май, ежегодно	Зав. кафедрой СПКБ	Издательские расходы, премирование за счет средств ФаМИ и спонсорской помощи	
10.	Разработка обновленных информационных материалов о специальности 6-05-0533-12 Кибербезопасность для профориентационных мероприятий	Февраль-март, 1 раз в 3 года	ППС кафедры СПКБ, Зав. кафедрой СПКБ	Оплата изготовления, средства ФаМИ	
11.	Организация и проведение профильной олимпиады ГрГУ им.Янки Купалы по направлению «Математика криптографии и защита информации»	Март-май, ежегодно	Зав. кафедрой СПКБ	Издательские расходы, премирование за счет средств спонсорской помощи	
12.	Подготовка и рассылка персональных приглашений учащимся выпускных классов	Апрель-май, ежегодно	ППС кафедры СПКБ	Почтовые и издатель-	

	для поступления на факультет			ские расходы, средства ФаМИ	
13.	Обеспечение участия школьников в тренировочных и отборочных этапах конкурса профессионального мастерства WorldSkills по компетенциям «Безопасность корпоративных информационных систем», «Кибербезопасность»	1 раз в 2 года	Зав. кафедрой СПКБ, ППС кафедры СПКБ	Премирование участников за счет средств ФаМИ и спонсорской помощи	

3.1.1.2. Для обеспечения учебного процесса по ряду читаемых дисциплин кафедра СПКБ располагает ранее разработанными электронными учебно-методическими комплексами для других специальностей, требующими незначительной доработки. В то же время, необходима разработка значительного количества новых обучающих ресурсов по дисциплинам, которые ранее не входили в учебные планы специальностей факультета. С этой целью были определены ответственные из числа ППС за разработку (модернизацию) электронных и цифровых учебно-методических комплексов (включая фонды оценочных средств) и размещение их на образовательном портале по каждой дисциплине. План разработки (модернизации) электронных и цифровых учебно-методических комплексов представлен в таблице 3.2.

Надо отметить, что задача создания, позиционирования и продвижения глобально ориентированных образовательных продуктов, т.е. продуктов, конкурентоспособных не только на внутреннем, но и на международном рынке, ставит нас перед целым рядом новых вызовов. Отдельные курсы, тематические модули этих курсов, образовательные программы должны быть привлекательны не только для внутренней, но и для иностранной аудитории по своему содержанию, а также доступны на английском языке – основном языке международного общения.

Таблица 3.2. План разработки (модернизации) электронных учебно-методических комплексов.

№	Наименование дисциплины	Срок исполнения	Ответственный	Отметка о выполнении
1.	Операционные системы	30.06.2028	Петров С.В.	
2.	Язык программирования Python	31.12.2027	Дирвук Е.В.	
3.	Инструментальные средства обеспечения безопасности	31.12.2027	Мысливец О.Р.	
4.	Технологии Интернета Вещей (IoT)	31.12.2026	Лявшук И.А.	
5.	Безопасность систем Интернета Вещей	31.12.2026	Ващило В.В.	
6.	Компьютерная стеганография	31.12.2027	Кадан А.М.	
7.	Биометрия и управление доступом	30.06.2028	Кадан А.М.	
8.	Технология блокчейн и криптовалюта	31.12.2026	Ливак Е..Н.	
9.	Квантовая криптография	31.12.2027	Лавыш А.В.	
10.	Компьютерная криминалистика	31.12.2027	Дайлида Е.С.	
11.	Аудит и тестирование безопасности	30.06.2027	Мысливец О.Р.	
12.	Интеллектуальные методы в решении задач защиты информации	31.12.2026	Марковская Н.В.	

13.	Машинное обучение и нейронные сети	31.12.2026	Марковская Н.В.	
14.	Технологии компьютерного зрения	31.12.2026	Дирвук Е.В.	
15.	Безопасность компьютерных сетей	31.12.2026	Ващило В.В.	
16.	Разработка защищенных приложений	30.06.2027	Ващило В.В.	
17.	Квантовые системы и технологии	30.06.2028	Лавыш А.В.	
18.	Алгоритмы и структуры данных	30.06.2025	Статкевич С.Э.	
19.	Математический анализ	30.06.2025	Павлючик П.Б.	
20.	ГрГУ им.Я.Купалы: миссия, история, структура	30.06.2025	Гецевич А.К.	

3.1.1.3. Очевидно, что одного только создания качественных образовательных продуктов недостаточно. Необходимо разработать инструменты, которые сделают их гибкими, способными подстраиваться под запросы академического рынка, а также механизмы, обеспечивающие комфортность получения образовательных услуг.

С целью реализации мировых тенденций в сфере высшего образования, для обеспечения и повышения качества учебного процесса на выпускающей кафедре СПКБ в настоящее время широко используются инновационные практико-ориентированные формы и методы преподавания: занятия в рамках практико-ориентированного и компетентсного подхода, форме самостоятельной деятельности; исследовательские; на основе групповой технологии; проблемные; на основе проектной деятельности; занятия-тренинги и игровые формы организации обучения: деловые и ролевые игры. Для реализации мировых тенденций в сфере высшего образования, активно используются методы и средства в рамках сотрудничества с мировыми лидерами в области ИТ-образования: международной программой Сетевых академий Cisco, проектом Google Apps for Education, образовательным центром компании InfoWatch.

Также надо отметить, что кафедра СПКБ является исполнителем договора о международном сотрудничестве, заключённого между ГрГУ им. Янки Купалы и АО «ИнфоВотч» (РФ, г.Москва), одной из ведущих компаний в области защиты информации. В рамках договора на кафедре создан учебный стенд для изучения современных систем защиты от утечек информации, производимых компанией АО «ИнфоВотч», который эффективно используется при подготовке студентов специальности 6-05-0533-12 Кибербезопасность. Учебные материалы компании внедрены в 3 учебных дисциплины кафедры. Сотрудники компании ежегодно принимают участие в работе Государственной экзаменационной комиссии на специальности 6-05-0533-12 Кибербезопасность. Выпускники специальности Компьютерная безопасность успешно работают в белорусском представительстве компании, расположенном в г.Минск.

Также, параллельно с созданием образовательных продуктов должен запускаться целый ряд сопутствующих процессов. Во-первых, это постоянная модернизация структуры и содержания учебных программ. При проектировании учебного плана специальности предусмотреть максимально возможное количество элективных дисциплин Мы должны обеспечить возможности для индивидуализации образовательных траекторий студентов как за счёт предоставления им большей свободы в выборе курсов, так и за счёт встраивания в учебный процесс академической проектной работы и таких инновационных образовательных продуктов, как массовые онлайн-курсы и т.п.

При этом необходимо, не перегружая студентов, дать им возможность полноценно изучать выбранные дисциплины. Гибкость программ обучения повысит доступность наших образовательных продуктов для иностранных студентов.

В попытке обеспечить качество учебного процесса и актуальность знаний, необходимо сбалансировать учебную нагрузку студента, не перегружая его значительными объемами информации и большим количеством заданий, время выполнения которых в совокуп-

ности ведет к перегруженности студента. Для этого кафедра должна работать в направлении выявления и формирования межпредметных связей, что в итоге даст возможность разрабатывать практические или проектные задания, покрывающие требования сразу нескольких дисциплин.

Таблица 3.3. План мероприятий по обеспечению качества учебного процесса.

	Наименование мероприятия	Срок исполнения	Ответственный	Ресурсы, источник финанси–рования	Отметка о выполнении
1.	На основе анализа удовлетворенности потребителей и заказчиков кадров осуществлять корректировку учебных и нормативных документов специальности	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуется	
2.	Закрепление тьюторов из числа ведущих ППС за талантливыми студентами	Сентябрь и февраль, ежегодно	Зав. кафедрой СПКБ	Не требуется	
3.	Внедрить инновационные методы обучения по дисциплинам специальности	Согласно графику разработки УМК	ППС кафедры СПКБ, зав. кафедрой СПКБ	Не требуется	
4.	Внедрить в учебный процесс образовательные технологии на основе современных LMS-систем и видеоконференций	30.12.2025	ППС кафедры СПКБ, Зав. кафедрой СПКБ	Не требуется	
5.	Внедрить в учебный процесс практику использования материалов платформ Coursera for Campus, Openedu.ru	Согласно учебному плану	ППС кафедры СПКБ, Зав. кафедрой СПКБ	Не требуется	
6.	Обеспечить современную информационно-коммуникационную среду учебного процесса	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуется	
7.	Внедрить элементы вендорных учебных программ и элементов сертифицированного обучения в учебный процесс (на платформе Сетевой академии Cisco)	30.06.2025	Зав. кафедрой СПКБ, ППС кафедры СПКБ	Не требуется	
8.	Разработать фонды оценочных средств по всем дисциплинам специальности	Согласно графику разработки ЭУМК	Зав. кафедрой СПКБ, ППС кафедры СПКБ	Не требуется	
9.	Обеспечить организацию ознакомительной и технологической практик во взаимодействии с базовыми	30.12.2026	Зав. кафедрой СПКБ	Не требуется	

	организациями и базами практики				
10.	Обеспечить использование в учебном процессе инновационной инфраструктуры и специализированных программно-аппаратных средств	30.06.2027	Зав. кафедрой СПКБ	Средства ФаМИ и спонсорской помощи	
11.	Реализовать междисциплинарные курсовые и дипломные работы совместно с представителями других специальностей ГрГУ им. Янки Купалы	30.06.2027	Зав. кафедрой СПКБ	Не требуется	
12.	Выполнить дипломные работы по заявкам предприятий и организаций, не менее 70% от общего числа дипломных работ	30.06.2027	Зав. кафедрой СПКБ	Не требуется	
13.	Обеспечить индивидуальный план обучения для студентов, трудоустроенных по специальности	30.06.2027	Зав. кафедрой СПКБ	Не требуется	
14.	Обеспечение участие студентов в программах академической мобильности (в том числе, виртуальной)	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуется	

3.1.1.4. Анализ развития студентоцентрированных подходов к обучению, преподаванию и оценке успеваемости, используемых факультетом математики и информатики и выпускающей кафедрой СПКБ, и оценка его потенциала, позволили выделить группы учащихся, требующие внимания и адаптации к учебному процессу, предоставления индивидуальных траекторий обучения, развития механизмов поддержки обучающихся с целью достижения каждым обучающимся планируемых результатов обучения. Соответствие квалификации ППС читаемым дисциплинам, подтверждает возможность успешной подготовки студентов специальности силами кафедры СПКБ и факультета математики информатики. Для качественной подготовки специалистов в области кибербезопасности определены мероприятия по развитию студентоцентрированных подходов к обучению, преподаванию и оценке успеваемости, приведённые в таблице3.4.

Таблица 3.4. Мероприятия по развитию студентоцентрированного обучения.

№	Наименование мероприятия	Срок исполнения	Ответственный	Ожидаемые результаты	Отметка о выполнении
1.	Участие преподавателей в тренингах и семинарах по студентоцентрированным методам преподавания	Согласно плану университета	Зав. кафедрой преподаватели	Вовлечение в процесс	
2.	Обмен лучшими практиками с коллегами	Постоянно	Зав. кафедрой преподаватели	Внедрение лучших практик	

3.	Использование цифровых технологий для повышения вовлеченности студентов в процесс обучения	Согласно плану работы кафедры	Зав. кафедрой, преподаватели, кураторы групп	Расширение сферы использования ИТ	
4.	Внедрение интерактивных методов обучения (проектное обучение, проблемно-ориентированное обучение, метод кейсов, работа в малых группах)	Согласно плану работы кафедры	Зав. кафедрой преподаватели	Повышение уровня результатов обучения	
5.	Создание условий для самостоятельной и исследовательской работы студентов	Согласно плану работы кафедры	Зав.кафедрой, преподаватели, научные руководители студентов	Повышение уровня результатов обучения	
6.	Организация наставничества и консультирования (регулярные встречи студентов с наставниками для обсуждения их прогресса и планов)	Ежегодно, сентябрь	Зав.кафедрой, научные руководители студентов	Повышение уровня результатов обучения	
7.	Обеспечение гибкости учебных планов с возможностью выбора элективных курсов, тем дипломных работ и мест прохождения практики	Ежегодно, декабрь	Зав.кафедрой, преподаватели	Повышение уровня результатов обучения	
8.	Внедрение формирующего оценивания (конструктивной обратной связи в течение учебного процесса)	Ежегодно, сентябрь, февраль	Зав. кафедрой преподаватели	Повышение уровня результатов обучения	
9.	Использование портфолио как инструмента оценки и мониторинга индивидуального прогресса студентов	Согласно плану работы кафедры	Зав. кафедрой, преподаватели, кураторы групп	Формирование академических и социальных ценностей	
10.	Обеспечение доступности образовательных ресурсов (цифровые библиотеки, онлайн-курсы и обучающие материалы)	Согласно плану работы кафедры	Зав. кафедрой, преподаватели, кураторы групп	Повышение уровня результатов обучения	
11.	Поощрение студенческих инициатив	Согласно плану работы кафедры	Зав. кафедрой преподаватели	Формирование академических и социальных ценностей	

12.	Совершенствование механизмов обратной связи (горячие линии, онлайн-платформы для анонимных отзывов, встречи с руководством образовательной программы)	Согласно плану работы кафедры	Зав.кафедрой, кураторы групп	Формирование академических и социальных ценностей	
13.	Поддержка академической честности и справедливого оценивания (использование четких стандартов и процедур для студентов и преподавателей)	Согласно плану работы кафедры	Зав.кафедрой, преподаватели, кураторы групп	Формирование академических и социальных ценностей	

3.1.2. Кадровый потенциал

Анализ кадрового обеспечения выпускающей кафедры СПКБ, его потенциал и соответствие квалификации ППС читаемым дисциплинам, подтверждает возможность успешной подготовки студентов специальности силами кафедры СПКБ и факультета математики информатики. Для качественной подготовки специалистов в области кибербезопасности определены мероприятия на повышение квалификации персонала, приведённые в таблице3.5.

Таблица 3.5. Перечень мероприятий по развитию кадрового потенциала.

№	Наименование мероприятия	Срок исполнения	Ответственный	Ресурсы, источник финансирования	Отметка о выполнении
1.	Повышение квалификации ППС по образовательным программам повышения квалификации	1 раз в 5 лет	ППС кафедры; Зав. кафедрой СПКБ	Бюджетные и внебюджетные средства университета	
2.	Стажировки по профилю читаемых курсов в УВО РБ и РФ	Согласно плану стажировок и повышения квалификации	Зав. кафедрой СПКБ	Бюджетные и внебюджетные средства университета	
3.	Непрерывное повышение квалификации ППС в режиме самообучения на доступных платформах дистанционного обучения	Согласно плану работы кафедры	ППС кафедры; Зав. кафедрой СПКБ	Не требуется	
4.	Повышение квалификации ППС в режиме участия в образовательных мero-	Согласно плану повышения квалификации	ППС кафедры; Зав. кафедрой СПКБ	Не требуется	

	приятиях и бизнес-конференциях (АО Инфовотч, Kaspersky Lab, Positive Technologies и др.)				
5.	Стажировки по профилю читаемых курсов в ИТ-компаниях РБ (ООО «Азати», ООО «ИнтэксСофт», ООО «Когнитек», ООО «АйТехАрт», ИООО «Эпам Системз», ООО «Сенла Групп», ООО «Экспозит»)	Согласно плану стажировок	Зав. кафедрой СПКБ	Бюджетные и внебюджетные средства университета	
6.	Привлечение специалистов-практиков к проведению занятий, не менее 2-х в год на каждом курсе, в объеме не менее 16 часов по читаемой дисциплине	Согласно учебному плану	Зав. кафедрой СПКБ	Фонд почасовой оплаты труда	
7.	Участие в работе курсов повышения квалификации в области иностранного языка	Согласно плану повышения квалификации	ППС кафедры СПКБ, Зав. кафедрой СПКБ	Бюджетные и внебюджетные средства университета	
8.	Обеспечение участия ППС кафедры в программах академической мобильности (в том числе, виртуальной)	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Бюджет программ мобильности	
9.	Участие ППС в составе рабочих групп международных образовательных проектов, проектов международной	Согласно регламенту инициированных проектов	Зав. кафедрой СПКБ	Бюджет проектов	

	технической помощи				
10.	Обеспечить подготовку и защиту кандидатской диссертации (Середа Е.В.)	31.06.2027	Зав. кафедрой СПКБ, ст. преподаватель Середа Е.В.	Не требуется	

3.1.3. Воспитательная деятельность в рамках формирования универсальных и профессиональных компетенций

Информация о мероприятиях, направленных на воспитание средствами учебных дисциплин, и соответствующие задания ежегодно обновляются в индивидуальных планах преподавателей и публикуются на образовательном портале университета.

Таблица 3.6. Перечень мероприятий по развитию воспитательной деятельности в рамках формирования универсальных и профессиональных компетенций.

№	Наименование мероприятия	Срок исполнения	Ответственный	Ресурсы, источник финансирования	Отметка о выполнении
1.	Комплект компьютерных тестов (ККТ) по направлению «История ИИ»	май 2025	Зав.кафедрой Кадан А.М.	Не требуются	
2.	ККТ по направлению «Роль женщин в развитии ИИ»	май 2025	Зав.кафедрой Кадан А.М.	Не требуются	
3.	ККТ по направлению «Этические нормы использования ИИ»	май 2025	Зав.кафедрой Кадан А.М.	Не требуются	
4.	ККТ по направлению «Роль женщин в развитии Кибербезопасности»	май 2025	Зав.кафедрой Кадан А.М.	Не требуются	
5.	Проведение дискуссий «О защите персональных данных в общедоступных информационных системах»	май 2025	Доцент Зайкрва С.А.	Не требуются	
6.	Написание эссе согласно предложенной тематике	июнь 2025	Старший преподаватель Середа Е.В.	Не требуются	
7.	Работа над проектом в рамках дисциплины «Квантовые системы и технологии»	декабрь 2024	Доцент Лавыш А.В.	Не требуются	
8.	Подготовка публичного выступления с докладом и презентацией на одну из предложенных тем в	март 2025	Доцент Лавыш А.В.	Не требуются	

	рамках дисциплины «Квантовая криптография»				
9.	Подготовка эссе «Правовой статус криптовалют и криптовалютных операций в Республике Беларусь Регулирование криптодеятельности в Беларуси»	май 2025	Доцент Ливак Е.Н.	Не требуются	
10.	Подготовка эссе «Использование технологии блокчейн в Беларуси Лучшие блокчейн-разработчики Беларуси»	май 2025	Доцент Ливак Е.Н.	Не требуются	
11.	Подготовка эссе «Беларусь как IT-страна Парк высоких технологий - гордость Республики Беларусь Достижения Беларуси в IT-сфере»	июнь 2025	Доцент Ливак Е.Н.	Не требуются	
12.	Просмотр видеоматериалов на тему «Архитектура современных систем защиты от утечек информации».	июнь 2025	Зав.кафедрой Кадан А.М.	Не требуются	
13.	Подготовка эссе «Защита информации офисных приложений от несанкционированного доступа»	декабрь 2024	Зав.кафедрой Кадан А.М.	Не требуются	
14.	Просмотр видеоматериалов на тему «Методы современных киберпреступников»	май 2025	Зав.кафедрой Кадан А.М.	Не требуются	

3.1.4. Научно-исследовательская и инновационная деятельность

Вовлечение студентов специальности 6-05-0533-12 Кибербезопасность в учебно-исследовательскую, научно-методическую и научную работу является одной из основных задач выпускающей кафедры. Исполнение нефинансируемой НИР «Цифровые технологии в прикладных исследованиях и образовании» за счет второй половины рабочего дня осуществляется всеми сотрудниками кафедры СПКБ.

Практически все преподаватели кафедры регулярно публикуются в научных изданиях с ненулевым импакт-фактором, большинство преподавателей с учёной степенью

имеют публикации в журналах из списков ВАК РБ и РФ, изданиях, индексируемых в базах данных Scopus и Web of Science.

В содружестве ООО «Вайзор Геймз», ведущим в Республике Беларусь производителем сетевых компьютерных игр, в 2017 году открыта совместная лаборатория «Искусственного интеллекта и компьютерной безопасности», в рамках которой ведется активная исследовательская и хоздоговорная деятельность. Исполнение нефинансируемой НИР за счет второй половины рабочего дня осуществляется всеми сотрудниками кафедры СПКБ.

Как отмечалось выше, с 2013 года кафедра СПКБ является исполнителем договора о международном сотрудничестве, заключённого между ГрГУ им. Янки Купалы и АО «Инфовотч» (РФ, г.Москва), одной из ведущих компаний в области защиты информации. Сотрудники компании оказывают активную помощь в проведении исследований, связанных с использованием DLP-систем защиты от внутренних угроз. В рамках договора на кафедре создан учебный стенд для изучения современных систем защиты от утечек информации, производимых компанией АО «Инфовотч».

Практически все преподаватели кафедры регулярно публикуются в научных изданиях с ненулевым импакт-фактором, большинство преподавателей с учёной степенью имеют публикации, индексируемые в базах данных Scopus и Web of Science.

С 2021 года ведется активное вовлечение студентов в стартап-движение и инновационную деятельность, использование инфраструктуры научно-технологического парка ГрГУ в учебном процессе и выполняемых на кафедре НИР и НИРС. На базе совместной с ООО «Вайзор Геймз» лаборатории «Искусственного интеллекта и компьютерной безопасности» создана СНИЛ «Интеллект-Безопасность», основным направлением которой определено проведение исследований в области применения интеллектуальных методов в защите информации.

Кафедра обеспечивает подготовку и представление дипломных работ студентов к участию в Республиканском конкурсе научных работ. Представленные работы студентов кафедры отмечаются дипломами лауреата, 1, 2 и 3 степени.

Публикационная активность студентов кафедры достаточно высокая. Ежегодно публикуются не менее 30 студенческих работ. Перечень мероприятий по развитию НИИД представлен в таблице 3.7.

Таблица 3.7. Перечень мероприятий по развитию НИИД.

№	Наименование мероприятия	Срок исполнения	Ответственный	Ресурсы, источник финансирования	Отметка о выполнении
1.	Вовлечь в работу СНИЛ «Интеллект-Безопасность» не менее 20% студентов специальности	31.12.2024	Зав. кафедрой СПКБ, рук. СНИЛ	Не требуется	
2.	Обеспечить подготовку к выставочной деятельности не менее одной разработки кафедры в год (в виде макета, прототипа, программы, презентации, стенда и т.д.), внесенной в каталоги	Ежегодно, с 01.09.2025	Зав. кафедрой СПКБ	Внебюджетные средства ГрГУ, средства ФаМИ для оплаты изготовления выставочного экспоната	

	научно-технической продукции				
3.	Вовлечь обучающихся в стартап-движение, обеспечив представление не менее трех бизнес-проектов от кафедры ежегодно на конкурсах различного уровня	Ежегодно, с 01.09.2025	Зав. кафедрой СПКБ; доцент Разова Е.Л.	Средства ФаМИ для премирования руководителей	
4.	Обеспечить реализацию хозяйственных договоров на разработку научно-технической продукции (оказание услуг) для предприятий и организаций региона, не менее двух договоров ежегодно	Ежегодно, с 01.09.2026	Зав. кафедрой СПКБ	Не требуется	
5.	Обеспечить публикации ППС кафедры, имеющих учёные степени и звания, в журналах из перечня ВАК и изданиях, индексируемых в БД Scopus и Web of Science, из расчёта не менее одной статьи в два года на одного преподавателя	Ежегодно, с 01.09.2026	Зав. кафедрой СПКБ	Не требуется	
6.	Обеспечить вовлечение в НИРС не менее 65% студентов 3–4 курсов	с 2026 г.	Научные руководители Зав. кафедрой СПКБ	Не требуется	
7.	Обеспечить ежегодное участие в профильных конференциях студентов специальности	с 2026 г.	Научные руководители Зав. кафедрой СПКБ	Оплата оргвзносов из средств ФаМИ	
8.	Обеспечить подготовку и представление на Республиканский конкурс научных работ студентов дипломных работ, защищенных на отметки 9 и 10 баллов	с 2026 г.	Научные руководители Зав. кафедрой СПКБ	Не требуется	

9.	Внедрить проектную модель организации НИРС по специальности	30.12.2025	Зав. кафедрой СПКБ	Не требуется	
10.	Привлекать студентов к участию в выполнении заданий научно-технических проектов и хоздоговорных работ	Согласно плану работы кафедры	Зав. кафедрой СПКБ	Не требуется	

3.1.5. Сотрудничество, в т.ч. международное

3.1.5.1. В настоящее время кафедра является исполнителем договора о международном сотрудничестве и договора о сотрудничестве ГрГУ им. Янки Купалы с организациями, работающими в сфере ИТ, а также двух договоров об организации филиала кафедры в ИТ-компаниях г.Гродно (см. таблицу 3.8).

Таблица 3.8. Партнеры кафедры СПКБ.

№	Наименование организации	Направления сотрудничества
1.	АО «ИнфоВотч» (РФ, г.Москва)	Договор о международном сотрудничестве. Обучение студентов с использованием продукции и учебных материалов компании, профориентационные мероприятия, участие представителей компании в работе ГЭК
2.	ООО «Вайзор Геймз» (РБ, г.Минск)	Договор о сотрудничестве. Организация совместной учебно-научно-исследовательской лаборатории «Искусственного интеллекта и компьютерной безопасности». Обучение студентов с использованием спонсорской помощи и учебных материалов компании, профориентационные мероприятия, проведение совместных конкурсов для студентов.
3.	ООО «Азати» (РБ, г.Гродно)	Договор об организации филиала кафедры. Совместное обучение студентов, проведение профильных семинаров, практика, профориентационные мероприятия, трудоустройство выпускников
4.	ООО «Интэкс-Софт» (РБ, г.Гродно)	Договор об организации филиала кафедры. Совместное обучение студентов, проведение профильных семинаров, практика, профориентационные мероприятия, трудоустройство выпускников

3.1.5.2. Факультетом математики и информатики и выпускающей кафедрой СПКБ определены мероприятия по заключению договоров на организацию практик, установлению договоренностей об организации учебного процесса, стажировок ППС, выполнении НИР со следующими предприятиями: ООО «Азати», ООО «ИнтэксСофт», ООО «Девкрафт», ООО «Когнитек», ООО «Инстинктулс», ООО «Скилсофт», ООО «МигСофт». Перечень мероприятий приведен в таблице 3.9.

Таблица 3.9. Перечень мероприятий по развитию сотрудничества.

№	Наименование мероприятия (с указанием организации - партнера)	Срок исполнения	Ответственный	Ресурсы, источник финанси–рования	Отметка о выполнении
1.	Проведение ознакомительных занятий и экскурсий на базе перечисленных организаций и предприятий	С 01.09.2024	Зав. кафедрой СПКБ	Не требуется	
2.	Организация практик на базе перечисленных организаций и предприятий	С 01.01.2026	Зав. кафедрой СПКБ	Не требуется	
3.	Заключение договоров предоставления безвозмездной (спонсорской) помощи для создания учебных лабораторий и организации профильных мероприятий	31.12.2026	Зав. кафедрой СПКБ	Не требуется	
4.	Обеспечение преподавания профильных дисциплин учебного плана специалистами организаций и предприятий г.Гродно	С 01.09.2024	Зав. кафедрой СПКБ	Не требуется	
5.	Организация стажировок ППС на базе перечисленных организаций и предприятий	Согласно отдельному графику	Зав. кафедрой СПКБ	Бюджетные и внебюджетные средства ГрГУ	

3.1.6. Инфраструктура и материально-техническая база

В настоящее время кафедра СПКБ имеет доступ к учебному оборудованию компьютерных классов и информационным ресурсам университета для проведения занятий по следующим дисциплинам, входящим в учебный план специальности 6-05-0533-12 Кибербезопасность: «Архитектура компьютеров», «Криптографические методы защиты информации», «Компьютерные сети». Обеспеченность библиотечными ресурсами – за счет научной литературы и учебных пособий в электронном виде. Недостаток печатных изданий компенсируется за счет учебных пособий в электронном виде.

Для обеспечения качества процесса подготовки и проведения занятий, организации лекционных и практических занятий необходимо запланировать закупку учебного лабораторного оборудования, информация о котором представлена в таблице 3.10.

Таблица 3.10. Планируемые закупки.

№	Название дисциплины	Дата закупки	Предмет закупки	Стоимость, источник финанси–рования	Отметка о выполнении
1.	«Основы кибербезопасности», «Обеспечение без-	Ежегодно июль	Приобретение учеб-	До 4000 BYN ежегодно.	

	опасности Интернета вещей», «Технологии компьютерного зрения», «Распознавание и синтез речи», «Технологии Интернета вещей», «Смарт-технологии автоматизации и реинжиниринга бизнеса», «Интеллектуальный анализ данных», «Основы защиты информации»		ного оборудования и материалов для лабораторного практикума по направлению «Интеллектуальная защита»	Спонсорская помощь	

3.1.7. Развитие культуры обеспечения качества в рамках образовательной программы

Для развития культуры обеспечения качества и эффективного управления образовательной программой необходимо внедрение ряда мероприятий, направленных на постоянное совершенствование содержания программы, учебного процесса и административных процедур. Ключевые мероприятия представлены в таблице 3.11.

Таблица 3.11. Мероприятия по развитию системы обеспечения качества

№	Наименование мероприятия	Срок исполнения	Ответственный	Ожида–емые результаты	Отметка о выполнении
	Развитие культуры обеспечения качества.				
1.	Вовлечение всех заинтересованных сторон (преподавателей, студентов, выпускников, работодателей)	постоянно	Зав.кафедрой	Повы–шение качества образования	
2.	Внедрение системы внутреннего аудита качества (регулярно оценивать эффективность программы на заседаниях кафедры, выявлять слабые места и принимать корректирующие меры)	31.12.2025	Зав.кафедрой		
	Механизмы управления образовательной программой				
3.	Создание рабочей группы (РГ) по управлению программой (координатора программы, академические наставников, представителей индустрии, студенты)	31.12.2025	Зав.кафедрой, РГ	Повы–шение качества образования	
4.	Введение системы контроля и мониторинга выполнения программы(оценка качества преподавания,	31.12.2025	Зав.кафедрой, РГ		

	успеваемости студентов, выполнения запланированных учебных мероприятий)				
5.	Интеграция современных инструментов управления образовательным процессом (LMS)	31.12.2025	Зав.кафедрой, преподаватели, РГ		
	Обеспечение актуальности и соответствия программы				
6.	Регулярный пересмотр образовательной программы на основе обратной связи от студентов, выпускников и работодателей	Согласно плану работы кафедры	Зав.кафедрой, РГ	Повы–шение качества образования	
7.	Мониторинг тенденций и новых технологий в области кибербезопасности	Согласно плану работы кафедры	Зав.кафедрой, преподаватели, РГ		
8.	Проведение консультаций с представителями индустрии и экспертами по кибербезопасности для обсуждения изменений в требованиях к специалистам и необходимости корректировки учебных планов	Согласно плану работы кафедры	Зав.кафедрой, РГ		
	Мероприятия по пересмотру плана и учебных материалов				
9.	Анализ учебных материалов и образовательного плана	Ежегодно, июнь	Зав.кафедрой, РГ	Повы–шение качества образования	
10.	Организация рабочих групп для разработки предложений по изменению учебного плана	Ежегодно, март-июнь	Зав.кафедрой, РГ		
	Оценка и улучшение образовательного процесса				
11.	Внедрение системы обратной связи от студентов по каждому курсу и преподавателю	31.12.2026	Зав.кафедрой, РГ	Повы–шение качества образования	
12.	Использование метрик и показателей эффективности	постоянно	Зав.кафедрой, РГ		
	Создание условий для инноваций и развития				
13.	Поддержка научно-исследовательской деятельности студентов и преподавателей (вклю-	Ежегодно, март-июнь	Зав.кафедрой, РГ	Повы–шение качества образования	

	чая интеграцию исследований в учебный процесс)				
14.	Развитие международного сотрудничества (участие в обменных программах, стажировках и совместных исследовательских проектах)	Согласно плану работы кафедры	Зав.кафедрой, РГ		
15.	Организация мероприятий по обмену опытом между различными образовательными учреждениями, кафедрами и лабораториями, занимающимися кибербезопасностью	Согласно плану работы кафедры	Зав.кафедрой, РГ		

3.1.8. Мероприятия по информированию общественности в рамках образовательной программы

Информирование общественности в рамках образовательной программы предполагает решение нескольких задач. Это, наряду с привлечением абитуриентов, работа с потенциальными работодателями выпускников специальности при организации проведения производственных практик и распределения, возможности трудоустройства выпускников во время учебы. А также поиск потенциальных заказчиков для заключения договоров на выполнение дипломных работ и ИНР, использующих методы и средства обеспечения кибербезопасности.

Таблица 3.12. Мероприятия по информированию общественности

№	Наименование мероприятия	Срок исполнения	Ответственный	Ожидаемые результаты	Отметка о выполнении
1	Участие в Днях университета / факультета / кафедры	Согласно плану университета/факультета/кафедры	Зав.кафедрой	Информирование заинтересованных лиц	
2	Проведение многопрофильной олимпиады ГрГУ им.Янки Купалы	Согласно плану университета	Зав.кафедрой	Привлечение лучших абитуриентов	
3	Проведение открытой олимпиады по кибербезопасности для студентов и школьников (турнир программистов по	ежегодно	Зав.кафедрой	Привлечение лучших абитуриентов	

4	перед школьниками общеобразовательных классов школ области	Ежегодно 1 полугодие	Зав.кафедрой	Привлечение лучших абитуриентов	
5	Выступления перед участниками республиканских олимпиад и учащимися специализированных классов	Ежегодно 1 полугодие	Зав.кафедрой	Привлечение лучших абитуриентов	
6	Публикации в СМИ	ежегодно	Зав.кафедрой	Привлечение абитуриентов	
7	Сопровождение сайта факультета (раздел кафедры СПКБ)	постоянно	Зав.кафедрой, специалист кафедры	Привлечение абитуриентов	

4. Оценка рисков при реализации плана развития специальности

Оценить возможные риски реализации программы и предложить мероприятия, направленные на их устранение (минимизацию).

Таблица 3.13. Риски реализации программы и мероприятия по их устранению

№	Наименование возможных рисков	Мероприятия по устранению рисков
1.	Снижение интереса абитуриентов к IT-профессиям, реструктуризация рынка труда	Усиление и индивидуализация профориентационной работы, формирование положительного имиджа специальности и факультета на уровне университета, Гродненской области и страны в целом
2.	Повышение активности столичных и зарубежных вузов в привлечении абитуриентов, рост конкуренции	
3.	Невозможность обеспечить качественное преподавание дисциплин специализации собственными силами	Подготовка кадров из числа молодых выпускников специальности, поиск мотивированных к научно-педагогической деятельности выпускников магистратуры и аспирантуры из профильных УВО РБ, привлечение внешних специалистов, в т.ч. из организаций-заказчиков кадров
4.	Недостаточно высокий уровень подготовки выпускников из-за отсутствия мотивации к обучению	Персонификация образовательной траектории, применение активных методов обучения, развитие научных исследований и технического творчества среди студентов
5.	Недостаточная ориентированность учебного процесса на потребности заказчиков кадров	Выявление потребностей, реализация корректировка образовательной программы, обучение на базе организаций-заказчиков кадров
6.	Отказ профильных предприятий и организаций в установлении партнёрских отношений	Поиск новых партнёров
7.	Несоответствие основных направлений научной работы кафедры профилю подготовки специалистов	Вовлечение ППС в формирование заявок на получение научных грантов и поиску заказов на разработку научно-технической продукции (услуг) по профилю

		специальности
8.	Снижение объёма бюджетных средств для финансирования развития материально-технической базы	Перераспределение ресурсов, оптимизация использования имеющихся ресурсов, привлечение ресурсов организаций-заказчиков кадров, разработка реализация проектов международной технической помощи

1.2. Целевые индикаторы

Таблица 3.14. Целевые индикаторы

№ п/п	Предмет оценки качества образовательной программы	Показатель оценки	Планируемое значение показателя			
			2024	2025	2026	2027
Оценка качества образовательной деятельности студентов и ее результатов						
1	Промежуточные результаты теоретического и практического обучения	Средний балл промежуточной аттестации по учебным дисциплинам (модулям), курсовым работам (проектам), практикам	6,7	6,8	6,9	7
2	Итоговые результаты	Доля дипломов с отличием, полученных на государственном экзамене и защите дипломной работы (проекта)	-	-	-	7
		Доля обучающихся, успешно завершивших обучение по ОП, от общего количества обучающихся, зачисленных на обучение	-	-	--	97
Оценка качества образовательных программ (образовательная среда и НМО)						
3	Практическая составляющая ОП	Доля учебных дисциплин, совместно реализованных с социальными партнерами	2,5	2,5	3	3
4	Научно-методическое обеспечение ОП	Процент обеспеченности зарегистрированными ЭУМК/ЦУМК дисциплин учебного плана	55	65	75	100

		Процент обеспеченности дисциплин учебного плана учебными изданиями с грифом	90	95	100	100
Кадровое обеспечение образовательной программы						
5	Остепененность педагогических работников, реализующих ОП	Доля ППС, работающего на постоянной основе, обеспечивающего реализацию образовательной программы	80	80	80	80
		Доля штатных работников из числа ППС, включая совместителей (работающих по трудовому договору), имеющих ученые и почетные степени и звания	80	80	80	80
6	Педагогическое мастерство	Результаты рейтинга ППС по разделу «учебная деятельность»	462	462	462	462
		Результаты рейтинга ППС по разделу «научно-исследовательская и инновационная деятельность»	122	122	122	122
7	Востребованность ОП	Проходной балл на специальность (дневная форма за счет средств бюджета), проходной балл (дневная форма на платной основе)	354. 244	354. 244	354. 244	354. 244
		Доля иностранных студентов, обучающихся на ОП (на 01.01.)	1	2	2	3
8	Удовлетворенность студентов	Уровень удовлетворенности студентов	4,39	4,25	4,25	4,25
9	Профессиональные качества преподавателя	Результаты опроса «Преподаватель глазами студентов»	4,76	4,8	4,8	4,8

10	Закрепляемость молодых специалистов в профессии	Уровень закрепляемости молодых специалистов по специальности	100	100	100	100

Проректор по учебной работе

_____ Л.Ю. Павлов

Декан факультета математики и информатики

_____ А.Ф. Проневич

Заведующий кафедрой системного программирования и компьютерной безопасности

_____ А.М. Кадан

Рекомендована к утверждению:

Научно-методическим советом университета
Протокол № 7.1 от 03.10 2024 г.

Советом факультета математики и информатики
Протокол № 4 от 24.09 2024 г.

Кафедрой системного программирования и компьютерной безопасности
Протокол № 11 от 30.08 2024 г.