

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Белгородский Валерий Савельевич
Должность: Ректор
Дата подписания: 15.09.2023 16:16:50
Уникальный программный ключ:
8df276ee93e17c18e7bee9e7cad2d0ed9ab82473

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации

Уровень образования	бакалавриат
Направление подготовки/Специальность	09.03.02 Информационные системы и технологии
Направленность (профиль)/Специализация	Интеллектуальные системы управления и цифровые двойники
Срок освоения образовательной программы по очной форме обучения	4 года
Форма(-ы) обучения	очная

Учебная дисциплина «Защита информации» изучается в третьем семестре.
Курсовая работа/Курсовой проект – не предусмотрен(а)

1.1. Форма промежуточной аттестации

Экзамен.

1.2. Место учебной дисциплины в структуре ОПОП

Учебная дисциплина «Защита информации» относится к обязательной части программы.
Результаты обучения по учебной дисциплине, используются при изучении следующих дисциплин и прохождения практик:

- Основы проектирования баз данных;
- Проектирование информационных и автоматизированных систем;
- Цифровые двойники технологических процессов и производств.

Результаты освоения учебной дисциплины в дальнейшем будут использованы при прохождении учебной практики и выполнении выпускной квалификационной работы.

1.3. Цели и планируемые результаты обучения по дисциплине

Современный специалист в области информационных технологий должен обладать знаниями и навыками обеспечения информационной безопасности. Связано это с тем, что в информационных системах предприятий и организаций хранится и обрабатывается критически важная информация, нарушение конфиденциальности, целостности или доступности которой может привести к нежелательным последствиям. Поэтому вопросам обеспечения информационной безопасности должно уделяться внимание на всех этапах разработки и эксплуатации информационных систем.

Целями изучения дисциплины «Защита информации» являются:

- изучение базовых понятий, связанных с обеспечением информационной безопасности: виды основных угроз и меры противодействия им;
 - изучение основных понятий криптографии: алгоритмы симметричного и асимметричного шифрования, процесс создания инфраструктуры открытых ключей;
 - изучение протоколов криптографической защиты данных, передаваемых по телекоммуникационным сетям, использующим стек протоколов TCP/IP, использование межсетевых экранов для защиты сетей;
- рассмотрение современных методик анализа и управления рисками, связанными с информационной безопасностью.

Формируемые компетенции и индикаторы достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
<p>ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной</p>	<p>ИД-ОПК-3.3 Соблюдение требований по информационной безопасности</p>	<ul style="list-style-type: none"> – Применяет логико-методологический инструментарий для критической оценки получаемой информации и выбирает оптимальное решение поставленной задачи на основе системного подхода. – Использует математический аппарат и цифровые информационные технологии для сбора и обработки данных необходимых для анализа и постановки задачи цифровизации технологических процессов; использует цифровые сертификаты. – Применяет навыки работы с нормативной документацией на электронных ресурсах Консультант, Гарант, Каталог ГОСТ www.internet-law, в поисковых системах Web of Science, PatSearch и базах данных Global Patent Index для оформления прав интеллектуальной собственности на научные разработки в сфере цифровых технологий.
<p>ПК-4 Способен проектировать отдельные элементы и подсистемы автоматизированных систем управления предприятием (АСУП)</p>	<p>ИД-ПК-4.4 Выбор средств защиты информации</p>	<ul style="list-style-type: none"> – Владеет сутью общенаучных и конкретно-научных методов и принципов исследования. – Владеет базовыми понятиями, связанными с обеспечением информационной безопасности, видами основных угроз и мерами противодействия им; – Применяет методы и алгоритмы симметричного и ассиметричного шифрования данных; – Использует протоколы криптографической защиты данных, передаваемых по телекоммуникационным сетям, использующим стек протоколов TCP/IP, межсетевые экраны для защиты сетей; – Владеет современными методиками анализа и управления рисками, связанными с информационной безопасностью.

Общая трудоёмкость учебной дисциплины (модуля) по учебному плану составляет:

по очной форме обучения –	4	з.е.	144	час.
---------------------------	---	------	-----	------