# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

## 1. Цель освоения дисциплины

Формирование универсальных и профессиональных компетенций у обучающихся, готовности к использованию методов и технологий информационной безопасности при решении задач профессиональной деятельности в области обучения информатике.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к базовой части блока дисциплин.
Для освоения дисциплины «Информационная безопасность и защита информации» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Алгебра», «Геометрия», «Дискретная математика», «Дифференциальные уравнения», «Информационные системы», «Компьютерное моделирование», «Математическая логика и теория алгоритмов», «Математический анализ», «Методика обучения математике», «Методы исследовательской / проектной деятельности», «Методы математической обработки данных», «Практикум по решению предметных задач», «Программирование», «Программное обеспечение систем и сетей», «Теоретические основы информатики», «Теория вероятностей и математическая статистика», «Теория функций действительного переменного», «Теория функций комплексного переменного», «Теория чисел», «Технологии искусственного интеллекта», «Технологии цифрового образования», «Философия», «Численные методы», «Числовые системы», «Элементарная математика», «3D-моделирование и печать», «Вводный курс математики», «Компьютерная алгебра», «Компьютерные сети», «Образовательная робототехника», «Практикум решения школьных математических задач», прохождения практик «Производственная (педагогическая по информатике) практика», «Учебная (научно-исследовательская работа, получение первичных навыков научно-исследовательской работы) практика», «Учебная (ознакомительная по информатике) практика», «Учебная (ознакомительная по математике) практика», «Учебная (ознакомительная по элементарной математике) практика».

## 3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:
– способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);
– способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач (ПК-1).

**В результате изучения дисциплины обучающийся должен:**

***знать***
– сущность понятия информационной безопасности и базовые принципы ее обеспечения;
– основные законодательные акты в сфере информационной безопасности в Российской Федерации;
– типы угроз информационной безопасности; механизм межсетевого экранирования;
– перечень и сущность технических средств обеспечения информационной безопасности; угрозы информационной безопасности личности в цифровой образовательной среде;
– основы криптографических методов защиты информации, структуру криптосистем, методы шифрования;

***уметь***
– определять цели, задачи и направления информационной безопасности;
– классифицировать нарушения в сфере информационной безопасности;
– применять антивирусные средства к защите информации; выбирать межсетевые экраны для защиты от несанкционированного доступа в информационных системах;
– реализовывать различные этапы обеспечения информационной безопасности; применять методы и технологий по защите информации в образовательных учреждениях;
– использовать электронную цифровую подпись для проверки целостности данных;

***владеть***
– навыками профилактических мер по защите от компьютерных вирусов; приемами реализации механизмов идентификации и аутентификации для защиты информации;
– навыком определения возможных средств и способов защиты информации в организации; приемами обеспечения информационной безопасности личности в цифровой образовательной среде;
– способами управления криптосистемами.

## 4. Общая трудоёмкость дисциплины и её распределение

количество зачётных единиц – 2,
общая трудоёмкость дисциплины в часах – 72 ч. (в т.ч. аудиторных часов – 32 ч., СРС – 36 ч.),
распределение по семестрам – 10,
форма и место отчётности – зачёт (10 семестр).

## 5. Краткое содержание дисциплины

Основные понятия «информационной безопасности».
Персональные данные как вид защищаемой информации. Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Базовые принципы обеспечения информационной безопасности

Правовые основы информационной безопасности и защиты персональных данных. Законодательство о безопасности и защите информации, его структура и содержание. Авторское право. Интеллектуальная собственность.

Программные средства защиты информации.
Компьютерные вирусы и антивирусная защита. Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства родительского контроля

Технические средства защиты и комплексное обеспечение информационной безопасности. Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в образовательных организациях. Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи

Элементы криптографии.
Понятие шифра. Симметричное и асимметричное шифрование. Односторонние функции.

Метод RSA. Электронная подпись

**6. Разработчик**

Сергеев Алексей Николаевич, доктор педагогических наук, профессор кафедры информатики и методики преподавания информатики ФГБОУ ВО "ВГСПУ".