

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Цель освоения дисциплины

Формирование общепрофессиональных и профессиональных компетенций в области информационной безопасности личности, организации, общества, государства и основных мерах по её обеспечению.

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» относится к базовой части блока дисциплин. Для освоения дисциплины «Информационная безопасность» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Гимнастика с методикой преподавания», «Дорожная безопасность», «Концептуальные основы безопасности жизнедеятельности», «Легкая атлетика с методикой преподавания», «Нормативно-правовые основы профессиональной деятельности и антикоррупционное поведение», «Первая помощь пострадавшим», «Природные опасности и защита от них», «Спортивное ориентирование с методикой преподавания», «Спортивные и подвижные игры с методикой преподавания», прохождения практики «Учебная (по закреплению профессионально-прикладных умений и навыков) практика».

Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин «Безопасный отдых туризм», «Гражданская оборона», «Комплексная безопасность образовательной организации», «Методика преподавания предмета «Физическая культура»», «Организационно-правовые основы физкультурно-спортивной деятельности», «Основы национальной безопасности Российской Федерации», «Основы обороны государства и военной службы», «Охрана труда в образовательной организации», «Плавание с методикой преподавания», «Пожарная безопасность», «Правовое регулирование обеспечения безопасности жизнедеятельности», «Психологическая безопасность», «Спортивные и подвижные игры с методикой преподавания», «Теория и методика обучения безопасности жизнедеятельности», «Техногенные опасности и защита от них», «Экологическая безопасность», «Биомеханика», прохождения практик «Производственная (педагогическая по основам безопасности жизнедеятельности) практика», «Учебная (ознакомительная по основам безопасности жизнедеятельности) практика», «Учебная (предметно-содержательная) практика».

3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:

- способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики (ОПК-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

- виды и источники опасностей и угроз в сфере информационных процессов и систем;
- основы государственной политики обеспечения информационной безопасности;
- структуру и источники угроз информационной безопасности; роль и место информационной безопасности в системе национальной безопасности страны; федеральные нормативные акты, направленные на обеспечение информационной безопасности личности, общества и государства;
- нормативно-правовые акты по информационной безопасности в образовании;

- основные виды деструктивных влияний информации на личность;
- основные методы и средства информационного воздействия на человека;
- информационные средства и технологии, негативно влияющие на здоровье;

уметь

- анализировать роль информации в развитии общества;
- выявлять источники угроз информационной безопасности объектов;
- проводить оценку информации с точки зрения её соответствия нормативно-правовым актам;
- защититься от негативного информационного воздействия; принимать решения на основе анализа и оценки информации;
- анализировать и практически использовать нормативно-правовые акты по информационной безопасности в образовании;
- идентифицировать информационные опасности и противодействовать им в быту и в служебной обстановке;
- подготовить материал для проведения занятия по информационной безопасности;

владеть

- основными понятиями в области информационной безопасности;
- методами и средствами обеспечения информационной безопасности;
- навыками работы с законодательными и иными нормативно-правовыми актами по информационной безопасности в системе образования; способами предупреждения информационных правонарушений;
- методами формирования у учащихся знаний и умений в области информационной безопасности;
- основными методиками противодействия информационным угрозам личности;
- представлением об информационном мировоззрении молодёжи.

4. Общая трудоёмкость дисциплины и её распределение

количество зачётных единиц – 3,

общая трудоёмкость дисциплины в часах – 108 ч. (в т. ч. аудиторных часов – 42 ч., СРС – 30 ч.),

распределение по семестрам – 5,

форма и место отчётности – экзамен (5 семестр).

5. Краткое содержание дисциплины

Информация и информационная безопасность в современном мире.

Понятие информации и информационной безопасности. Окружающая среда как источник информации. Восприятие информации человеком. Роль информации в развитии общества. Понятие информационного общества. Образование в информационном обществе.

Обеспечение информационной безопасности РФ.

Информация как объект правового регулирования. Информационная безопасность РФ.

Правовое обеспечение информационной безопасности РФ. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 5 декабря 2016 г. № 646).

Защита государственной тайны. Конфиденциальная информация и её защита. Защита интеллектуальной собственности. Служебная тайна. Коммерческая тайна. Профессиональная тайна. Информационная война. Психологическая война.

Информационная безопасность личности.

Концепция информационной безопасности детей. ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". Нормативно-правовые акты по

информационной безопасности в образовании. Неприкосновенность частной жизни граждан. Персональные данные и их защита. Технологии идентификации человека. Применение паролей в механизме аутентификации человека. Влияние средств массовой информации на человека. Влияние рекламы на человека. Цифровая зависимость. Правила кибергигиены. Деструктивные течения и деятельность в Интернете и их профилактика. Опасный и запрещенный контент в Интернете и его признаки. Правила цифрового поведения, необходимого для предотвращения рисков и угроз при использовании Интернета (кибербуллинга, вербовки в различные организации и группы). Принятие решений в повседневной жизни и в чрезвычайных ситуациях. Информационные и компьютерные преступления.

Практическая подготовка.

Подготовка материала для проведения урока по основам информационной безопасности в старшей школе. Апробация и обсуждение материала на учебных практических занятиях. Разработка внеурочных ситуаций при пребывании в социальных сетях. Коллективное рассмотрение индивидуальных практических карт урока по информационной безопасности

6. Разработчик

Тарасов Анатолий Александрович, канд. техн. наук, доцент кафедры теории и методики обучения физической культуре и безопасности жизнедеятельности ФГБОУ ВО «ВГСПУ».