МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра общенаучных дисциплин

Авторы-составители: **Рихтер Татьяна Васильевна**

Рабочая программа дисциплины

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Код УМК 91595

Утверждено
Протокол №7
от «02» апреля 2026 г.

Пермь, 2026

1. Наименование дисциплины

Основы кибербезопасности

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « Б.1 » образовательной программы по направлениям подготовки (специальностям):

Направление подготовки: **44.03.01** Педагогическое образование
направленность Начальное образование

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Основы кибербезопасности** у обучающегося должны быть сформированы следующие компетенции:

44.03.01 Педагогическое образование (направленность : Начальное образование)

УК.1 Способен осуществлять поиск, анализ и синтез информации, применять системный подход для разрешения проблемных ситуаций

Индикаторы

УК.1.2 Работает с противоречивой информацией из разных источников, находит пробелы в необходимой для разрешения проблемы информации, определяет варианты устранения пробелов

УК.9 Знает правовые и этические нормы, способен оценивать последствия нарушения этих норм

Индикаторы

УК.9.2 Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения

УК.13 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма и противодействовать им в профессиональной деятельности

Индикаторы

УК.13.1 Определяет основные признаки экстремистской и террористической деятельности

УК.13.2 Выявляет информацию, призывающую к осуществлению экстремистской и террористической деятельности

УК.13.3 Осуществляет взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма, владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности

ОПК.10 Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

Индикаторы

ОПК.10.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности

4. Объем и содержание дисциплины

Направление подготовки	44.03.01 Педагогическое образование (направленность: Начальное образование)
форма обучения	заочная
№№ триместров, выделенных для изучения дисциплины	13,14
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	12
Проведение лекционных занятий	4
Проведение практических занятий, семинаров	8
Самостоятельная работа (ак.час.)	96
Формы текущего контроля	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (5)
Формы промежуточной аттестации	Зачет (14 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Общие сведения о безопасности ПК и Интернета

Интернет как средство для поиска полезной информации. Архитектура компьютера. Сохранение полезной информации. Обмен данными при совместной работе – скайп, IP-телефония, ICQ. Безопасный обмен данными. Компьютер и Интернет в промышленности. Вредоносные сайты. Облачные сервисы. Поиск документов в сети. Информационная перегрузка. Виды Интернет-общения. Дистанционное обучение. Программное и аппаратное обеспечение. Компьютер и системы безопасности. Понятие кибербезопасности. Угрозы для мобильных устройств. Виды защиты киберпространства (несанкционированный доступ, разрушение и утрата информации, искажение информации). Защита киберпространства. Геоинформационные системы. Информационная безопасность. Защита персональных данных. Категории персональных данных. Биометрические персональные данные. Источники данных в Интернете: почта, сервисы обмена файлами и др. Хранение данных в Интернете. Возможности и проблемы социальных сетей. Безопасный профиль в социальных сетях. Компьютерная и информационная безопасность, обнаружение проблем в сети, восстановление параметров систем, средства защиты от несанкционированного доступа к данным, криптографическая защита информации. Защищенная информаци-онная среда. Защита каналов передачи данных, средства предот-вращения утечки информации, защита информации от НСД (анти-вирусная защита, средства контроля защищенности, средства обна-ружения и предупреждения атак), средства аутентификации. Орга-низационно-технические меры защиты информационной среды. Системы охранной сигнализации, видеонаблюдение, контроль и управление доступом, средства уничтожения информации, средст-ва резервного копирования и восстановления. Требования к безо-пасности информации: сохранение целостности, конфиденциальности и доступности. Типовые требования и показатели качества функционирования информационных систем. Признаки нарушения целостности программ и данных. Способы нарушения целостности информации. Признаки и способы нарушения конфиденциальности. Признаки и способы нарушения доступности информации. Безопасность мобильных устройств в информационных системах. Источники заражения мобильных устройств (веб-ресурсы, магазины приложений, ботнеты). Угрозы безопасности в сетях WiFi. Мтоды защиты сетей WiFi. Угрозы информации (техногенные, случайные и преднамеренные; природные). Меры кибербезопаснсти для конечных пользователей. Использование рекомендованных версий операционных систем и приложений, использование антивирусных средств, настройка веб-браузеров, блокировка скриптов, использование фильтров фишинга, межсетевых экранов. Автоматическое обновление ПО. Киберугрозы Интернета (кибервойны, манипулирование людьми, зависимость, вирусные атаки, отсутствие приватности). Кибертерроризм и кибервойны. Кибератаки и техногенные катастрофы. Защита IT-инфраструктур критически важных объектов. Категории информационной безопасности. Шифрование при передаче конфиденциальной информации. Цифровая подпись. Риски интернета (контентные, электронные, коммуникационные, потребительские). Безопасный серфинг. Безопасные ресурсы для поиска. Проблемы электронной торговли. Проблемные сайты. Ложные ресурсы сети. Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях. Опасная информация в сети. Социальные последствия безответственного поведения в интернете. Угрозы для IOS-устройств. Угрозы для Android-устройств. Проблемы безопасности информационных систем. Методы обеспечения защиты данных в СУБД. Защита государственных информационных систем. Безопасность при удаленном доступе к ресурсам компьютера. Хакерские атаки. Новые технологии и новые угрозы информационной безопасности (применение робототехники и т.п.). Кибершпионаж. КибероружиеСпециальности, связанные с защитой киберпространства.

Техника безопасности и экология

Правила работы с ПК и электронными книгами. Компьютер и домашние животные. Мультимедиа, правила

безопасной работы. Воздействие компьютера на зрение и др. органы. Гигиена при работе с компьютером. Гигиена компьютера. Компьютер и кровообращение. Польза и вред компьютерных игр. Компьютер и ЗОЖ. Физическое и психическое здоровье. Правила поведения в компьютерном классе. Интернет в системе безопасности. Техника безопасности при работе с компьютером. Компьютер и мобильные устройства в чрезвычайных ситуациях. Медицинская информация в Интернете. Компьютеры и мобильные устройства в экстремальных условиях. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM). Комплекс упражнений при работе за компьютером. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов. Кибератаки на инфраструктуру. Компьютер в режиме труда и отдыха. Влияние компьютера на репродуктивную систему. Вредные факторы работы за компьютером и их последствия. Организация рабочего места

Пробемы Интернет-зависимости

Интернет-сообщество. Интернет-зависимость. Социальные сети. Детские социальные сети. Виртуальная личность. Зависимость от Интернет-общения. Развлечения в Интернете. Признаки игровой зависимости. Сетевые игры. Сайты знакомств. ЗОЖ и компьютер. Виды зависимости. Деструктивная информация в Интернете. Виды Интернет-зависимости. Киберкультура (массовая культура в сети) и личность. Психологическое воздействие информации на человека. Управление личностью через сеть. Интернет и компьютерная зависимость (аддикция). Критерии зависимости (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив). Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения). Классификация интернет-зависимостей

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы

Контент-фильтры. Поисковые серверы. Признаки заражения ком-пьютера. Антивирусная защита. Защита файлов. Права пользовате-лей. Защита при загрузке и выключении компьютера. Безопасность при скачивании файлов. Защита программ и данных от несанкцио-нированного копирования. Организационные, юридические, про-граммные и программно-аппаратные меры защиты. Защита про-грамм и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п. Непереме-щаемые программы. Защита от копирования контента сайта. Ис-точники заражения ПК. Антивирусное ПО, виды и назначение. Методы защиты от вирусов. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.). Проверка подлинности (аутентификация) в Интернете. Меры безопасности для пользователя WiFi. Настройка безопасности. Вирусы для мобильных устройств (мобильные банкеры и др.). Настройка компьютера для безопасной работы. Ошибки пользователя. Меры личной безопасности при сетевом общении. Предотвращение несанкционированного доступа к ПК. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей. Простые и динамически изменяющиеся пароли. Борьба с утечками информации. Средства контроля доступа. Права пользователей. Способы разграничения доступа. Средства защиты в сети: межсетевые экраны, криптомаршрутиза-торы, серверы аутентификации и т.д. Обманные системы для защи-ты информации в сетях. Защита сайтов. Системы обнаружения атак. Безопасность хостинга. Типы вирусов. Отличия вирусов и закладок. Антивирусные программы для ПК: сканеры, ревизоры и др. Выявление неизвестных вирусов. Основные меры кибербезопасности. Безопасность приложений, серверов, конечных пользователей.

Защита от атак, повышение готовности. Аппаратная защита ПО и сети (электронные ключи, аппаратные брандмауэры). Защита ПК на этапе загрузки. Параметры безопасности ПК. Обновления. За-щита файловой системы. Файловые таблицы. Права доступа. Ре-зервное копирование и

восстановление данных. Восстановление ОС. Аппаратные и программные средства. Признаки заражения компьютерных программ. ОС и их возможности в борьбе с вируса-ми (Windows. Linux). Разновидности вирусов. Черви, трояны, скрипты и др. Шпионские программы. Шифровальщики. Хакер-ские утилиты. Сетевые атаки. Наиболее известные антивирусные программы. Kaspersky Internet Security. Dr.Web Security Space. ESET NOD32 Smart Security. Коммерческое и бесплатное антиви-русное ПО. Онлайн сервисы для безопасности пользователя в ин-тернете (проверка компьютера и файлов на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимо-сти СМС и др.). Настройки безопасности почтовых программ. За-щита в поисковых системах (фильтры для ограничения потенци-ально опасного содержимого). Настройки безопасности веб-браузеров (Internet Explorer, Firefox и т.п.). Электронная почта и системы мгновенного обмена сообщениями. Настройки безопасно-сти Скайп, ICQ и пр. Способы обеспечения безопасности веб-сайта.

Мошеннические действия в Интернете. Киберпреступления

Киберпреступления. Виды интернет-мошенничества (письма, рек-лама, охота за личными данными и т.п.). Опасности мобильной связи. Предложения по установке вредоносных приложений. Мо-шеннические СМС. Утечка и обнародование личных данных. Подбор и перехват паролей. Взломы аккаунтов в социальных сетях. Виды мошенничества в Интернете. Фишинг (фарминг). Азартные игры. Ложные антивирусы. Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники. Электронный кошелек. Мошенничество при распространении «бесплатного» ПО. Технологии манипулирования в Интернете. ТБ при интернет-общении. ТБ при регистрации на веб-сайтах. Компьютерное пиратство. Плагиат. Кибернаемники и кибердетективы. Оценка ущерба от киберпреступлений.

Сетевой этикет. Психология и сеть

Интернет-этикет. Правила общения в Интернете. Основы сетевого этикета. Переписка в сети. Правила поведения в скайпе. Форум. Общение в сети и его последствия. Агрессия в сети. Анонимность в сети. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах. Этика дискуссий. Взаимное уважение при интернет-общении. Этикет и безопасность. Реальная и виртуальная личность. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибермоббинг, троллинг, бул-лицид. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.). Тер-мины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др. Примеры этических нарушений. Значение сетевого этикета.

Правовые аспекты защиты киберпространства

Собственность в Интернете. Авторское право. Интеллектуальная собственность. Платная и бесплатная информация. Защита прав потребителей при использовании услуг Интернет. Защита прав по-требителей услуг провайдера. Ответственность за интернет-мошенничество. Правовые акты в области информационных технологий и защиты киберпространства. Ответственность за киберпреступления. Конституционное право на поиск, получение и распространение информации. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию» (действует с 1 сентября 2012 года). Информационное законодательство РФ. Закон РФ «Об информации, информационных технологиях и о защите информации». Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 237 УК РФ). Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo). Правовые основы для защиты от спама. Правовая охрана программ для ЭВМ и БД. Лицензионное ПО. Виды лицензий (OEM, FPP, корпоративные лицензии,

подписка). ПО с открытым кодом (GNU GPL, FreeBSD). Право на информацию, на сокрытие данных, категории информации. Персо-нальные и общедоступные данные, ограниченный доступ. Закон «О персональных данных». Указ президента РФ о создании действенной системы противодействия компьютерным атакам от 15 января 2013 г. Уголовный кодекс РФ, раздел «Преступления в сфере компьютерной информации».

Государственная политика в области кибербезопасности

Защита киберпространства государством. Кибервойна. Право на информацию в Конституции РФ. Защита государства и защита киберпространства. Доктрина информационной безопасности. Кибервойска. Защита киберпространства как одна из задач вооруженных сил. Информационная война. Информационное оружие. Патриотизм и интернет. Информационное воздействие. Военная, государственная, коммерческая тайна. Защита сайтов государственных органов (электронное правительство).

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. https://www.iprbookshop.ru/128406

2. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2024. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. https://urait.ru/bcode/557730

3. Басыня, Е. А. Сетевая информационная безопасность : учебник / Е. А. Басыня. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. https://www.iprbookshop.ru/132693

Дополнительная:

1. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. https://www.iprbookshop.ru/108227

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. https://urait.ru/bcode/449350

3. Киренберг, А. Г. Информационная безопасность современных операционных систем : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. https://www.iprbookshop.ru/128393

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://window.edu.ru Информационная система «Единое окно доступа к образовательным ресурсам»
http://www.iprbookshop.ru Электронная библиотечная система
http://elibrary.ru Научная электронная библиотека eLIBRARY.RU
http://www.solgpi.ru Электронная Библиотечная Система
http://www.antiplagiat.ru Система Антиплагиат
http://www.rsl.ru Российская государственная библиотека
http://www.pedlib.ru Педагогическая библиотека
http://cyberleninka.ru Киберленинка
http://window.edu.ru Информационная система «Единое окно доступа к образовательным ресурсам»
http://www.iprbookshop.ru Электронная библиотечная система
http://elibrary.ru Научная электронная библиотека eLIBRARY.RU
http://www.solgpi.ru Электронная Библиотечная Система
http://www.antiplagiat.ru Система Антиплагиат
http://www.rsl.ru Российская государственная библиотека
http://www.pedlib.ru Педагогическая библиотека
http://cyberleninka.ru Киберленинка

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Основы кибербезопасности** предполагает использование следующего программного обеспечения и информационных справочных систем:
- презентационные материалы;
- доступ в режиме online в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета;
- Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, сервисы онлайн конференций и т.д.)

Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:
- ОС Microsoft Windows
– пакет офисных приложений.
- Справочно-правовая система «КонсультантПлюс»
- Антивирусник
- ОС «Альт Образование».
- При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru)
Специального программного обеспечения не требуется.

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для занятий лекционного типа, для занятий семинарского (практического) типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – Компьютерный класс № 32 (корп.1).
Основное оборудование: специализированная мебель, персональные компьютеры, принтер, доска меловая, доска интерактивна, принтер, сканер.
Аудитория для самостоятельной работы, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченной доступом в электронную информационно-образовательную среду университета; помещение библиотеки СГПИ филиал ПГНИУ для обеспечения самостоятельной работы обучающихся.

Помещение библиотеки СГПИ филиал ПГНИУ оснащено компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ПГНИУ (ЕТИС (student.psu.ru), оборудованное специализированной мебелью, меловой доской, проектором, экраном, ноутбуками, телевизором.
Программное обеспечение: ОС Microsoft Windows; пакет офисных приложений Microsoft Office (версия согласно лицензионным соглашениям); Kaspersky Endpoint Security for Business; Справочно-правовая система «КонсультантПлюс»; Яндекс.Браузер (свободно распространяемое ПО) и/или Google Chrome (свободно распространяемое ПО); ОС «Альт Образование».

Помещение библиотеки СГПИ филиал ПГНИУ для обеспечения самостоятельной работы обучающихся оснащено:
компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду ПГНИУ (ЕТИС (student.psu.ru).
Библиотека оборудована: специализированной мебелью, меловой доской, проектором, экраном, компьютерами, ноутбуками, телевизором.
Все компьютеры, установленные в помещении библиотеки, оснащены следующим программным обеспечением:
Операционная система ALT Linux;
Офисный пакет Libreoffice;
Kaspersky Endpoint Security for Business;
Справочно-правовая система «КонсультантПлюс»;
Яндекс.Браузер (свободно распространяемое ПО).

Фонды оценочных средств для аттестации по дисциплине
Основы кибербезопасности

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

УК.1

Способен осуществлять поиск, анализ и синтез информации, применять системный подход для разрешения проблемных ситуаций

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
УК.1.2 Работает с противоречивой информацией из разных источников, находит пробелы в необходимой для разрешения проблемы информации, определяет варианты устранения пробелов	Знает: общие сведения о безопасности ПК и Интернета; требования к безопасности информации; признаки нарушения целостности программ и данных; меры кибербезопаснсти для конечных пользователей. Умеет: работать с противоречивой информацией из разных источников, находить пробелы в необходимой для разрешения проблемы информации. Владеет навыками: определения вариантов устранения пробелов; техники безопасности и экологии.	**Неудовлетворительно** Не знает: общие сведения о безопасности ПК и Интернета; требования к безопасности информации; признаки нарушения целостности программ и данных; меры кибербезопаснсти для конечных пользователей. Не умеет: работать с противоречивой информацией из разных источников, находить пробелы в необходимой для разрешения проблемы информации. Не владеет навыками: определения вариантов устранения пробелов; техники безопасности и экологии. **Удовлетворительно** Знает: общие сведения о безопасности ПК и Интернета; требования к безопасности информации; признаки нарушения целостности программ и данных; меры кибербезопаснсти для конечных пользователей. В основном умеет: работать с противоречивой информацией из разных источников, находить пробелы в необходимой для разрешения проблемы информации. Частично владеет навыками: определения вариантов устранения пробелов; техники безопасности и экологии. **Хорошо** Знает: общие сведения о безопасности ПК и Интернета; требования к безопасности информации; признаки нарушения целостности программ и данных; меры кибербезопаснсти для конечных пользователей. Умеет: работать с противоречивой информацией из разных источников, находить пробелы в необходимой для разрешения проблемы информации. В основном владеет навыками: определения

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо вариантов устранения пробелов; техники безопасности и экологии. **Отлично** Знает: общие сведения о безопасности ПК и Интернета; требования к безопасности информации; признаки нарушения целостности программ и данных; меры кибербезопаснсти для конечных пользователей. Умеет: работать с противоречивой информацией из разных источников, находить пробелы в необходимой для разрешения проблемы информации. Владеет навыками: определения вариантов устранения пробелов; техники безопасности и экологии.

УК.9

Знает правовые и этические нормы, способен оценивать последствия нарушения этих норм

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
УК.9.2 Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения	Знает: этические нормы поведения в разных видах профессиональной деятельности и последствиях их нарушения; сущность киберпреступлений; меры кибербезопаснсти для конечных пользователей; особенности психологической обстановки в Интернете. Умеет: использовать методы обеспечения безопасности ПК и Интернета; вести безопасную работу в сети в процессе сетевой коммуникации. Владеет навыками: сетевого этикета; защиты персональных данных.	**Неудовлетворительно** Не знает: этические нормы поведения в разных видах профессиональной деятельности и последствиях их нарушения; сущность киберпреступлений; меры кибербезопаснсти для конечных пользователей; особенности психологической обстановки в Интернете. Не умеет: использовать методы обеспечения безопасности ПК и Интернета; вести безопасную работу в сети в процессе сетевой коммуникации. Не владеет навыками: сетевого этикета; защиты персональных данных. **Удовлетворительно** Знает: этические нормы поведения в разных видах профессиональной деятельности и последствиях их нарушения; сущность киберпреступлений; меры кибербезопаснсти для конечных пользователей; особенности психологической обстановки в Интернете. В основном умеет: использовать методы обеспечения безопасности ПК и Интернета; вести безопасную работу в сети в процессе сетевой коммуникации. Частично владеет навыками: сетевого

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительно этикета; защиты персональных данных. **Хорошо** Знает: этические нормы поведения в разных видах профессиональной деятельности и последствиях их нарушения; сущность киберпреступлений; меры кибербезопаснсти для конечных пользователей; особенности психологической обстановки в Интернете. Умеет: использовать методы обеспечения безопасности ПК и Интернета; вести безопасную работу в сети в процессе сетевой коммуникации. В основном владеет навыками: сетевого этикета; защиты персональных данных. **Отлично** Знает: этические нормы поведения в разных видах профессиональной деятельности и последствиях их нарушения; сущность киберпреступлений; меры кибербезопаснсти для конечных пользователей; особенности психологической обстановки в Интернете. Умеет: использовать методы обеспечения безопасности ПК и Интернета; вести безопасную работу в сети в процессе сетевой коммуникации. Владеет навыками: сетевого этикета; защиты персональных данных.

УК.13

Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма и противодействовать им в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
УК.13.1 Определяет основные признаки экстремистской и террористической деятельности	Знать: признаки и способы нарушения доступности информации; меры кибербезопаснсти для конечных пользователей; категории информационной безопасности. Уметь: определять основные признаки экстремистской и террористической деятельности; вести безопасную работу в сети в процессе сетевой коммуникации. Владеть навыками: сетевого этикета.	**Неудовлетворительно** Не знает: признаки и способы нарушения доступности информации; меры кибербезопаснсти для конечных пользователей; категории информационной безопасности. Не умеет: определять основные признаки экстремистской и террористической деятельности; вести безопасную работу в сети в процессе сетевой коммуникации. Не владеет навыками: сетевого этикета. **Удовлетворительно** Знает: признаки и способы нарушения доступности информации; меры

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительно кибербезопаснсти для конечных пользователей; категории информационной безопасности. В основном умеет: определять основные признаки экстремистской и террористической деятельности; вести безопасную работу в сети в процессе сетевой коммуникации. Частично владеет навыками: сетевого этикета. **Хорошо** Знает: признаки и способы нарушения доступности информации; меры кибербезопаснсти для конечных пользователей; категории информационной безопасности. Умеет: определять основные признаки экстремистской и террористической деятельности; вести безопасную работу в сети в процессе сетевой коммуникации. В основном владеет навыками: сетевого этикета. **Отлично** Знает: признаки и способы нарушения доступности информации; меры кибербезопаснсти для конечных пользователей; категории информационной безопасности. Умеет: определять основные признаки экстремистской и террористической деятельности; вести безопасную работу в сети в процессе сетевой коммуникации. Владеет навыками: сетевого этикета.
УК.13.2 Выявляет информацию, призывающую к осуществлению экстремистской и террористической деятельности	Знать: типы вирусов; антивирусные программы для ПК; признаки заражения компьютера. Уметь: выявлять информацию, призывающую к осуществлению экстремистской и террористической деятельности. Владеть навыками: защиты персональных данных.	**Неудовлетворительно** Не знает: типы вирусов; антивирусные программы для ПК; признаки заражения компьютера. Не умеет: выявлять информацию, призывающую к осуществлению экстремистской и террористической деятельности. Не владеет навыками: защиты персональных данных. **Удовлетворительно** Знает: типы вирусов; антивирусные

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительно программы для ПК; признаки заражения компьютера. В основном умеет: выявлять информацию, призывающую к осуществлению экстремистской и террористической деятельности. Частично владеет навыками: защиты персональных данных. **Хорошо** Знает: типы вирусов; антивирусные программы для ПК; признаки заражения компьютера. Умеет: выявлять информацию, призывающую к осуществлению экстремистской и террористической деятельности. В основном владеет навыками: защиты персональных данных. **Отлично** Знает: типы вирусов; антивирусные программы для ПК; признаки заражения компьютера. Умеет: выявлять информацию, призывающую к осуществлению экстремистской и террористической деятельности. Владеет навыками: защиты персональных данных.
УК.13.3 Осуществляет взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма, владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности	Знает: общие сведения об экстремизме и терроризме. Умеет: осуществлять взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма. Владеет: навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности.	**Неудовлетворительно** Не знает: общие сведения об экстремизме и терроризме. Не умеет: осуществлять взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма. Не владеет: навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности. **Удовлетворительно** Знает: общие сведения об экстремизме и терроризме. В основном умеет: осуществлять взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма. Частично владеет: навыками аргументации противодействия экстремизму и терроризму

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительно в профессиональной деятельности. **Хорошо** Знает: общие сведения об экстремизме и терроризме. Умеет: осуществлять взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма. В основном владеет: навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности. **Отлично** Знает: общие сведения об экстремизме и терроризме. Умеет: осуществлять взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма. Владеет: навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности.

ОПК.10

Способен понимать принципы работы современных информационно-коммуникационных технологий и использовать их для решения профессиональных задач с учетом требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.10.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Знает: особенности использования информационно-коммуникационных технологий в профессиональной деятельности. Умеет: обоснованно выбирать информационно-коммуникационные технологии. Владеет навыками: использования информационно-коммуникационных технологий в профессиональной деятельности с учетом требований информационной безопасности.	**Неудовлетворительно** Не знает: особенности использования информационно-коммуникационных технологий в профессиональной деятельности. Не умеет: обоснованно выбирать информационно-коммуникационные технологии. Не владеет: использования информационно-коммуникационных технологий в профессиональной деятельности с учетом требований информационной безопасности. **Удовлетворительно** Знает: особенности использования информационно-коммуникационных технологий в профессиональной деятельности. В основном умеет: обоснованно выбирать информационно-коммуникационные технологии.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительно Частично владеет: использования информационно-коммуникационных технологий в профессиональной деятельности с учетом требований информационной безопасности. **Хорошо** Знает: особенности использования информационно-коммуникационных технологий в профессиональной деятельности. Умеет: обоснованно выбирать информационно-коммуникационные технологии. В основном владеет: использования информационно-коммуникационных технологий в профессиональной деятельности с учетом требований информационной безопасности. **Отлично** Знает: особенности использования информационно-коммуникационных технологий в профессиональной деятельности. Умеет: обоснованно выбирать информационно-коммуникационные технологии. Владеет: использования информационно-коммуникационных технологий в профессиональной деятельности с учетом требований информационной безопасности.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : заочное

Вид мероприятия промежуточной аттестации : Не предусмотрено
Максимальное количество баллов : 100

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Общие сведения о безопасности ПК и Интернета **Входное тестирование**	Знать основы кодирования информации, сущность информационной безопасности, уметь кодировать информацию, владеть навыками криптографии. Входной контроль проводится в виде теста, состоящего из 10 вопросов
УК.9.2 Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения	Пробемы Интернет-зависимости **Письменное контрольное мероприятие**	Знать: виды и типы Интернет-зависимости. Уметь: находить деструктивную информацию в Интернете. Владеть: навыками управления личностью через сеть.
УК.9.2 Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы **Письменное контрольное мероприятие**	Знать общие сведения о безопасности ПК и Интернета, требования к безопасности информа-ции, типовые требования и показатели качества функционирования информационных систем, признаки нарушения целостности программ и данных, способы нарушения целостности информации, признаки и способы нарушения доступности информации, категории информационной безопасности, проблемы Интернет-зависимости, типы вирусов, антивирусные программы для ПК, признаки заражения компьютера, организационные, юридические, программные и программно-аппаратные меры защиты информации, проблемы безопасности инфраструктуры Интернета, средства защиты в сети; уметь использовать методы обеспечения безопасности ПК и Интернета, использовать методы обеспечения защиты данных в СУБД; владеть навыками техники безопасности.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
УК.13.2 Выявляет информацию, призывающую к осуществлению экстремистской и террористической деятельности **УК.9.2** Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения	Мошеннические действия в Интернете. Киберпреступления **Письменное контрольное мероприятие**	Знать: виды интернет-мошенничества. Уметь: оценивать ущерб от киберпреступлений. Владеть: навыками использования технологии манипулирования в Интернете.

Спецификация мероприятий текущего контроля

Общие сведения о безопасности ПК и Интернета

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
Владеет навыками криптографии.	4
Знает основы кодирования информации, сущность информационной безопасности.	3
Умеет кодировать информацию.	3

Пробемы Интернет-зависимости

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знает виды и типы Интернет-зависимости	10
Владеет навыками управления личностью через сеть	10
Умеет находить деструктивную информацию в Интернете	10

Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знает общие сведения о безопасности ПК и Интернета, требования к безопасности информации, типовые требования и показатели качества функционирования информационных систем, признаки нарушения целостности программ и данных, способы нарушения целостности информации, признаки и способы нарушения доступности	10

информации, категории информационной безопасности, проблемы Интернет-зависимости, типы вирусов, антивирусные программы для ПК, признаки заражения компьютера, организационные, юридические, программные и программно-аппаратные меры защиты информации, проблемы безопасности инфраструктуры Интернета, средства защиты в сети	
Владеет навыками техники безопасности	10
Умеет использовать методы обеспечения безопасности ПК и Интернета, использовать методы обеспечения защиты данных в СУБД	10

Мошеннические действия в Интернете. Киберпреступления

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Умеет оценивать ущерб от киберпреступлений	15
Владеет навыками использования технологии манипулирования в Интернете	15
Знает виды Интернет-мошенничеств	10

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 43 до 60
«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
УК.9.2 Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения	Сетевой этикет. Психология и сеть **Письменное контрольное мероприятие**	Знать сущность киберпреступлений, меры кибербезопаснсти для конечных пользователей, осо-бенности мошеннических действий в Интернете, виды интернет-мошенничества, правила об-щения в Интернете, особенности психологической обстановки в Интернете; уметь вести безо-пасную работу в сети в процессе сетевой коммуникации, использовать методы обеспечения защиты данных в СУБД; владеть навыками сетевого этикета.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
УК.13.1 Определяет основные признаки экстремистской и террористической деятельности **УК.13.2** Выявляет информацию, призывающую к осуществлению экстремистской и террористической деятельности **УК.9.2** Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения	Правовые аспекты защиты киберпространства **Письменное контрольное мероприятие**	Знать: правовые акты в области информационных технологий и защиты киберпространства. Уметь: определять уголовную ответственность за создание, использование и распространение вредоносных компьютерных программ. Владеть: навыками защиты прав потребителей при использовании услуг Интернет.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
УК.1.2 Работает с противоречивой информацией из разных источников, находит пробелы в необходимой для разрешения проблемы информации, определяет варианты устранения пробелов **УК.13.3** Осуществляет взаимодействие на основе нетерпимого отношения к проявлениям экстремизма и терроризма, владеет навыками аргументации противодействия экстремизму и терроризму в профессиональной деятельности **УК.9.2** Ориентируется в этических нормах поведения в разных видах профессиональной деятельности и последствиях их нарушения **ОПК.10.2** Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности	Государственная политика в области кибербезопасности **Итоговое контрольное мероприятие**	Знать: общие сведения о безопасности ПК и Интернета, сущность киберпреступлений, требования к безопасности информации, типовые требования и показатели качества функционирования информационных систем, признаки нарушения целостности программ и данных, способы нарушения целостности информации, признаки и способы нарушения доступности информации, меры кибербезопаснсти для конечных пользователей, категории информационной безопасности, проблемы Интернет-зависимости, типы вирусов, антивирусные программы для ПК, признаки заражения компьютера, организационные, юридические, программные и программно-аппаратные меры защиты информации, проблемы безопасности инфраструктуры Интернета, средства защиты в сети, особенности мошеннических действий в Интернете, виды интернет-мошенничества, правила общения в Интернете, особенности психологической обстановки в Интернете, правовые аспекты защиты киберпространства, особенности государственной политики в области кибербезопасности; уметь: использовать методы обеспечения безопасности ПК и Интернета, вести безопасную работу в сети в процессе сетевой коммуникации, использовать методы обеспечения защиты данных в СУБД; владеть: навыками техники безопасности и экологии, навыками сетевого этикета, навыками защиты персональных данных.

Спецификация мероприятий текущего контроля

Сетевой этикет. Психология и сеть

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

Показатели оценивания	Баллы
Знает сущность киберпреступлений, меры кибербезопаснсти для конечных пользователей, особенности мошеннических действий в Интернете, виды интернет-мошенничества, правила общения в Интернете, особенности психологической обстановки в Интернете	10
Владеет навыками сетевого этикета	10
Умеет вести безо-пасную работу в сети в процессе сетевой коммуникации, использовать методы обеспечения защиты данных в СУБД	10

Правовые аспекты защиты киберпространства

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знает правовые акты в области информационных технологий и защиты киберпространства	10
Владеет навыками защиты прав потребителей при использовании услуг Интернет	10
Умеет определять уголовную ответственность за создание, использование и распространение вредоносных компьютерных программ	10

Государственная политика в области кибербезопасности

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Знает общие сведения о безопасности ПК и Интернета, сущность киберпреступлений, требования к безопасности информации, типовые требования и показатели качества функционирования информационных систем, признаки нарушения целостности программ и данных, способы нарушения целостности информации, признаки и способы нарушения доступности информации, меры кибербезопаснсти для конечных пользователей, категории информационной безопасности, проблемы Интернет-зависимости, типы вирусов, антивирусные программы для ПК, признаки заражения компьютера, организационные, юридические, программные и программно-аппаратные меры защиты информации, проблемы безопасности инфраструктуры Интернета, средства защиты в сети	10
Владеет навыками техники безопасности и экологии, навыками сетевого этикета, навыками защиты персональных данных	10
Умеет использовать методы обеспечения безопасности ПК и Интернета, вести безопасную работу в сети в процессе сетевой коммуникации, использовать методы обеспечения защиты данных в СУБД	10
Знает особенности мошеннических действий в Интернете, виды интернет-мошенничества, правила общения в Интернете, особенности психологической обстановки в Интернете, правовые аспекты защиты киберпространства, особенности государственной политики в области кибербезопасности	10