Автономная некоммерческая организация высшего образования
«Открытый университет экономики, управления и права»
(АНО ВО ОУЭП)

РАБОЧАЯ ПРОГРАММА

учебной дисциплины

Б1.О.22 Защита информации

Образовательная программа направления подготовки
09.03.01 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»,
направленность (профиль): «Информатика и вычислительная техника»
Квалификация: бакалавр

Рассмотрено к утверждению на заседании кафедры
информатики
(протокол № 15-01 от 15.01.2021г.)

Разработчик:
Артюшенко В.М., д.тех., проф.

Москва 2021

1. Цели и задачи дисциплины

Цель дисциплины - формирование у обучающихся теоретических знаний и практических навыков применения методов и средств защиты информации в профессиональной деятельности.

Задачи дисциплины:

– формирование системы знаний в сфере источников угроз безопасности информации в компьютерной системе;

– формирование системы знаний в сфере юридических основ правового обеспечения безопасности компьютерных систем;

– формирование системы знаний о технических и программных средствах обеспечения безопасности компьютерных систем.

2. Место дисциплины в структуре ОП

Блок 1 «Дисциплины (модули)», обязательная часть.

3. Планируемые результаты обучения по дисциплине

В результате изучения дисциплины обучающийся должен освоить:

общепрофессиональную компетенцию:

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 безопасности.

Результаты освоения дисциплины, установленные индикаторы достижения компетенций

Наименование компетенции	**Индикаторы достижения компетенции**	**Показатели (планируемые) результаты обучения**
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 безопасности	ОПК-3.1. Знает: общие характеристики технических средств, применяемых в информационных и автоматизированных системах, методы работы с информацией и общие требования к составлению библиографического описания документов, основные положения правовой базы в области защиты информационных систем и ресурсов организаций	**Знать:** • способы разграничения доступа и средства их реализации;
	ОПК-3.2. Умеет: использовать средства информационно-коммуникационных технологий в профессиональной деятельности с учетом основных требований к информационной безопасности	**Уметь:** • проводить анализ защищенности компьютера и сетевой среды с использованием сканера безопасности
	ОПК-3.3. Владеет: навыками работы с компьютерными технологиями в рамках профессиональной деятельности с учетом основных требований к информационной безопасности, навыками эффективного мониторинга обеспечения информационной безопасности в профессиональной деятельности	**Владеть:** • методами аудита безопасности информационных систем,

Знания, умения и навыки, приобретаемые обучающимися в результате изучения дисциплины «Защита информации», являются необходимыми для последующего поэтапного формирования компетенций и изучения дисциплин.

4. Объем дисциплины и виды учебной работы

Учебным планом предусматриваются следующие виды работы по дисциплине:

№ п/п	Виды учебных занятий	Всего часов по формам обучения, ак. ч			
		Очная		Заочная	
		всего	в том числе	всего	в том числе
1	**Контактная работа (объем работы обучающихся во взаимодействии с преподавателем) (всего)**			**12,2**	
1.1	занятия лекционного типа (лекции)	16		4	
1.2	занятия семинарского типа (практические)*, в том числе:	48		6	
1.2.1	семинар-дискуссия, практические занятия		0 48		0 6
1.2.2	занятия семинарского типа: лабораторные работы (лабораторные практикумы)			-	
1.2.3	курсовое проектирование (выполнение курсовой работы)			-	
1.3	контроль промежуточной аттестации и оценивание ее результатов, в том числе:	2,2		2,2	
1.3.1	консультация групповая по подготовке к промежуточной аттестации		2		2
1.3.2	прохождение промежуточной аттестации		0,2		0,2
2	**Самостоятельная работа (всего)**	**98**		**161**	
2.1	работа в электронной информационно-образовательной среде с образовательными ресурсами учебной библиотеки, компьютерными средствами обучения для подготовки к текущей и промежуточной аттестации, к курсовому проектированию (выполнению курсовых работ)	98		161	
2.2	самостоятельная работа при подготовке к промежуточной аттестации	**15,8**		**6,8**	
3	**Общая трудоемкость дисциплины**	**5 з.е. / 180 час.**			
	Форма промежуточной аттестации	экзамен			

*
_____
Семинар – семинар-дискуссия
ГТ - практическое занятие - глоссарный тренинг
ТТ - практическое занятие - тест-тренинг
ПЗТ - практическое занятие - позетовое тестирование
ЛС - практическое занятие - логическая схема
УД - семинар-обсуждение устного доклада
РФ – семинар-обсуждение реферата
Асессмент реферата - семинар-асессмент реферата
ВБ - вебинар
УЭ - семинар-обсуждение устного эссе
АЛТ - практическое занятие - алгоритмический тренинг

5. Содержание дисциплины
5.1. Содержание разделов и тем

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в информационную безопасность	**Особенности обеспечения информационной безопасности Российской Федерации** (роль и место информационной безопасности в общей системе национальной безопасности РФ. Основные цель и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ. Внешние и внутренние источники угроз информационной безопасности в РФ). **Информация как объект защиты** (определение, виды и источники информации, подлежащей защите. Информация как объект права

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		собственности. Виды защищаемой информации. Угрозы и возможные каналы утечки конфиденциальной информации. Обзор способов реализации угроз информации. Анализ моделей нарушителя. Категории потенциальных нарушителей). **Анализ существующих подходов к обеспечению безопасности информации** (особенности современных информационных систем, существенные с точки зрения безопасности. Законодательный, административный и процедурный уровни информационной безопасности. Основные понятия политики безопасности. Структура политики безопасности организации. Программно-технический уровень информационной безопасности. Сервисы безопасности. Место сервисов безопасности в архитектуре информационных систем)
2	Организационно-правовое обеспечение защиты информации	**Международные и отечественные стандарты в сфере защиты информации** (роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернет. Отечественные стандарты безопасности информационных технологий). **Сертификация и аттестация в области защиты информации** (назначение и общая характеристика. Проведение сертификационных испытаний. Аттестация объектов информатизации. Сертификация на региональном и международном уровнях). **Организационные меры по защите информации** (концепция безопасности предприятия и ее содержание. Политика информационной безопасности предприятия. Назначение, содержание и структура политики безопасности. Служба безопасности предприятия). **Основы правового обеспечения защиты информации** (международный опыт правового обеспечения информационной безопасности. Государственная система правового обеспечения информационной безопасности. Содержание основных законов РФ в области информационной безопасности. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации)
3	Методы и средства технической защиты информации	**Виды и методы технической защиты информации** (пассивные и активные методы защиты информации. Средства технической защиты информации. Защита помещений. Системы охранной сигнализации на территории и в помещениях. Системы видеонаблюдения. Системы контроля доступа. Системы контроля вскрытия аппаратуры). **Технические каналы утечки информации** (общая характеристика технических каналов утечки информации и их классификация. Каналы утечки речевой информации. Технические средства и методы получения информации по этим каналам. Утечка информации по проводным коммуникациям и за счет побочных электромагнитных излучений и наводок. Технические средства и методы получения информации с использованием этих каналов). **Методы и средства защиты информации от утечки по техническим каналам** (основные методы, используемые при создании систем защиты информации. Заземление технических средств передачи информации. Использование сетевых фильтров. Экранирование помещений. Методы защиты от утечек по акустическим каналам. Защита средств связи и телекоммуникаций)
4	Программно-технические средства защиты информации	**Защита информации от несанкционированного доступа** (идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Идентификация и аутентификация субъектов “пользователь” и “процесс” при запросах на доступ к компьютерным ресурсам. Использование простого и динамически изменяющегося паролей. Биометрическая идентификация. Предотвра-щение несанкционированного доступа к компьютерным ресурсам и защита программных средств. Разграничение доступа. Защита программных средств от несанкциони-рованного копирования и модификации). **Защита от компьютерных вирусов** (основные виды вирусов и схемы их функционирования. Основные каналы распространения вирусов и других

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		вредоносных программ. Обнаружение вирусов и меры по защите и профилактике. Антивирусные программы и комплексы). **Технологии межсетевых экранов** (функции межсетевых экранов. Фильтрация трафика. Выполнение функций посредничества. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе межсетевых экранов. Схемы подключения межсетевых экранов. Персональные и распределенные межсетевые экраны. Обзор современных межсетевых экранов)
5	Криптографические средства защиты информации	**Принципы криптографической защиты информации** (основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированные криптосистемы шифрования. Электронная цифровая подпись и функция хэширования. Правовые аспекты применения электронной цифровой подписи). **Криптографические алгоритмы. Средства криптографиической защиты информации** (классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Блочные алгоритмы шифрования. Асимметричные алгоритмы шифрования. Алгоритм шифрования RSA. Алгоритм Диффи-Хеллмана. Алгоритмы цифровой подписи. Средства криптографической защиты информации. Правовые основы разработки и использования средств криптографической защиты информации). **Компьютерная стеганография** (принципы компьютерной стеганографии. Секретные средства связи и передачи информации. Методики стеганографии. Стегосистема. Контейнер. Стегоключ)

6. Методические указания по освоению дисциплины

6.1 Учебно-методическое обеспечение дисциплины

Методические указания для преподавателя

Изучение дисциплины проводится в форме лекций, практических занятий, организации самостоятельной работы студентов, консультаций. Главное назначение лекции - обеспечить теоретическую основу обучения, развить интерес к учебной деятельности и конкретной учебной дисциплине, сформировать у студентов ориентиры для самостоятельной работы над курсом.

Основной целью практических занятий является обсуждение наиболее сложных теоретических вопросов курса, их методологическая и методическая проработка. Они проводятся в форме опроса, диспута, тестирования, обсуждения докладов и пр.

Самостоятельная работа с научной и учебной литературой, дополняется работой с тестирующими системами, тренинговыми программами, с информационными базами, образовательным ресурсов электронной информационно-образовательной среды и сети Интернет.

Оценочные материалы по компетенциям представлены на сайте в разделе «оценочные материалы».

6.2 Методические материалы обучающимся по дисциплине, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Методические материалы доступны на сайте «Личная студия» в разделе «Методические указания и пособия».

1. Методические указания «Введение в технологию обучения».
2. Методические указания по проведению учебного занятия «Вебинар».
3. Методические указания по проведению занятия «Семинар-обсуждение устного эссе», «Семинар-обсуждение устного доклада».
4. Методические указания по проведению занятия «Семинар – асессмент реферата».
5. Методические указания по проведению занятия «Семинар – обсуждение реферата».
6. Методические указания по проведению учебного занятия с компьютерным средством обучения «Практическое занятие - тест-тренинг».
7. Методические указания по проведению учебного занятия с компьютерным средством обучения «Практическое занятие - глоссарный тренинг».
8. Методические указания по проведению занятия «Практическое занятие - позетовое тестирование».
9. Положение о реализации электронного обучения, дистанционных образовательных технологий.

10. Методические указания по проведению занятия «Практическое занятие - алгоритмический тренинг».

Указанные методические материалы для обучающихся доступны в Личной студии обучающегося, в разделе ресурсы..

6.3 Особенности реализации дисциплины в отношении лиц из числа инвалидов и лиц с ограниченными возможностями здоровья

Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала.

Подбор и разработка учебных материалов должны производится с учетом того, чтобы предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

Выбор средств и методов обучения осуществляется самим преподавателям. При этом в образовательном процессе рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.

Разработка учебных материалов и организация учебного процесса проводится с учетом следующих нормативных документов и локальных актов образовательной организации:

- Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» // СЗ РФ. 2012. № 53 (ч. 1). Ст. 7598;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации» // СЗ РФ. 1995. № 48. Ст. 4563;
- Федерального закона от 03.05.2012 № 46-ФЗ «О ратификации Конвенции о правах инвалидов» // СЗ РФ. 2012. № 19. Ст. 2280;
- Приказа Минобрнауки России от 09.11.2015 № 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2016. № 4;
- Приказ Министерства науки и высшего образования РФ от 5 апреля 2017 г. N 301 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры".;
- Методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн;
- Положения об организации и осуществлении образовательной деятельности по реализации образовательных программ высшего образования с применением электронного обучения, дистанционных образовательных технологий (локальный нормативный акт утв. приказом АНО ВО ОУЭП от 20.01.2021 № 10;
- Положения об обучении инвалидов и лиц с ограниченными возможностями здоровья (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5);
- Положения о текущем контроле успеваемости и промежуточной аттестации обучающихся (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5).
- Порядка разработки оценочных материалов и формирования фонда оценочных материалов для проведения промежуточной и итоговой (государственной итоговой) аттестации и критерии оценивания при текущем контроле успеваемости (локальный нормативный акт утв. приказом АНО ВО ОУЭП от 20.01.2021 № 10);
- Положения об экзаменационной комиссии (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5).
- Правил подачи и рассмотрения апелляций по результатам вступительных испытаний (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5);
- Положения о разработке и реализации адаптированных учебных программ АНО ВО ОУЭП (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Студенческим советом протокол от 20.01.2021 № 13 и Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5);
- Положения об организации обучения обучающихся по индивидуальному учебному плану (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5);

- Положения об оказании платных образовательных услуг для лиц с ограниченными возможностями (локальный нормативный акт утв. приказом от 20.01.2021 № 10. Рассмотрено и одобрено Ученым советом АНО ВО ОУЭП, протокол от 20.01.2021 № 5).

В соответствии с нормативными документами инвалиды и лица с ограниченными возможностями здоровья по зрению имеют право присутствовать на занятиях вместе с ассистентом, оказывающим обучающемуся необходимую помощь; инвалиды и лица с ограниченными возможностями здоровья по слуху имеют право на использование звукоусиливающей аппаратуры.

При проведении промежуточной аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении государственной итоговой аттестации;
- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);
- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении аттестации с учетом их индивидуальных особенностей;
- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут;

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья организация обеспечивает выполнение следующих требований при проведении аттестации:

а) для слепых:

- задания и иные материалы для сдачи экзамена оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;
- письменные задания выполняются обучающимися с использованием клавиатуры с азбукой Брайля, либо надиктовываются ассистенту;

б) для слабовидящих:

- задания и иные материалы для сдачи экзамена оформляются увеличенным шрифтом и\или использованием специализированным программным обеспечением Jaws;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

- имеется в наличии информационная система "Исток" для коллективного использования слабослышащими;
- по их желанию испытания проводятся в электронной или письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата:

- тестовые и тренинговые задания по текущей и промежуточной аттестации выполняются обучающимися на компьютере через сайт «Личная студия" с использованием электронного обучения и дистанционных технологий;
- в процессе обучения студентам предоставляется возможность использования электронных образовательных ресурсов, разработанных в Университете, а так же разработана доступная электронная информационно-образовательная среда;
- по их желанию испытания проводятся в устной форме.

О необходимости обеспечения специальных условий для проведения аттестации обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

6.4 Методические рекомендации по самостоятельной работе студентов

Цель самостоятельной работы - подготовка современного компетентного специалиста и формирование способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Реализация поставленной цели предполагает решение следующих задач:

- качественное освоение теоретического материала по изучаемой дисциплине, углубление и расширение теоретических знаний с целью их применения на уровне межпредметных связей;

- систематизация и закрепление полученных теоретических знаний и практических навыков;

- формирование умений по поиску и использованию нормативной, правовой, справочной и специальной литературы, а также других источников информации;

- развитие познавательных способностей и активности, творческой инициативы, самостоятельности, ответственности и организованности;

- формирование самостоятельности мышления, способностей к саморазвитию, самообразованию, самосовершенствованию и самореализации;

- развитие научно-исследовательских навыков;

- формирование умения решать практические задачи (в профессиональной деятельности), используя приобретенные знания, способности и навыки.

Самостоятельная работа является неотъемлемой частью образовательного процесса.

Самостоятельная работа предполагает инициативу самого обучающегося в процессе сбора и усвоения информации, приобретения новых знаний, умений и навыков и ответственность его за планирование, реализацию и оценку результатов учебной деятельности. Процесс освоения знаний при самостоятельной работе не обособлен от других форм обучения.

Самостоятельная работа должна:

- быть выполнена индивидуально (или являться частью коллективной работы). В случае, когда СР подготовлена в порядке выполнения группового задания, в работе делается соответствующая оговорка;

- представлять собой законченную разработку (этап разработки), в которой анализируются актуальные проблемы по определенной теме и ее отдельных аспектов;

- отражать необходимую и достаточную компетентность автора;

- иметь учебную, научную и/или практическую направленность;

- быть оформлена структурно и в логической последовательности: титульный лист, оглавление, основная часть, заключение, выводы, список литературы, приложения,

- содержать краткие и четкие формулировки, убедительную аргументацию, доказательность и обоснованность выводов;

- соответствовать этическим нормам (правила цитирования и парафраз; ссылки на использованные библиографические источники; исключение плагиата, дублирования собственного текста и использования чужих работ).

6.4.1 Формы самостоятельной работы обучающихся по разделам дисциплины

Раздел 3 «Методы и средства технической защиты информации»

Темы устного доклада

1. Источники, риски и формы атак на информацию.
2. Защита компьютерной информации: основные понятия и определения.
3. Классификация угроз безопасности информации.
4. Программные закладки как форма атак на объекты информационных систем.
5. Модели воздействия программных закладок на компьютеры.
6. Троянские программы как форма атак на объекты информационных систем.
7. Клавиатурные шпионы как форма атак на объекты информационных систем.
8. Анализ угроз и каналов утечки информации.
9. Анализ рисков утечки информации.
10. Управление риском утечки информации.
11. Принципы политики информационной безопасности.
12. Виды политики информационной безопасности.
13. Организация политики информационной безопасности на основе дискретных компонент.
14. Организация политики информационной безопасности на основе анализа угроз системе.
15. Модели конечных состояний.
16. Классификация способов защиты информации.
17. Структура системы защиты информации.
18. Документы Государственной технической комиссии России по безопасности информации.
19. Критерии безопасности компьютерных систем Министерства обороны США («Оранжевая книга»).
20. Европейские критерии безопасности информационных технологий.
21. Федеральные критерии безопасности информационных технологий.
22. Общие критерии безопасности информационных технологий.
23. Группы требований к системам защиты информации.
24. Общие и организационные требования к системам защиты информации.
25. Конкретные требования к подсистемам защиты информации.

Раздел 5 «Криптографические средства защиты информации»

Деловая игра по четвертому разделу на тему: «Защита от компьютерных вирусов»

Цели деловой игры:

- познакомить учащихся с термином «компьютерный вирус», видами таких вирусов, принципами их действия, причинами распространения, средствами защиты;
- формировать навыки логического мышления (вывод, анализ, обобщение, выделение главного);
- воспитывать умение работать с партнером, уважать чужое мнение, быть дисциплинированным, проявлять толерантность;
- закрепить умения работы в программе OpenOffice.org Impress.

Материально-техническое обеспечение:

- программа OpenOffice.org Impress, позволяющая создавать профессиональные слайд-шоу, которые могут включать в себя диаграммы, рисованные объекты, текст, мультимедиа и множество других элементов;
- ручки, карандаши, бумага.

Роли и функции участников:

Специалисты по компьютерной вирусологии – отвечают на заданные вопросы и осуществляют помощь журналистам в подготовке статьи.

Журналисты – задают вопросы специалистам по компьютерной вирусологии и готовят статью для своего издания.

1-2 эксперта приглашаются из числа руководителей производственных практик, работающих специалистов, выпускников высших образовательных организаций.

Ведущий игры – преподаватель.

План занятия:

1. Объяснение правил игры, деление на группы, придумывание названия своему изданию.
2. Специалисты по компьютерной вирусологии знакомятся с теоретическим материалом, а журналисты на компьютере делают заготовку для будущей статьи (в программе OpenOffice.org Impress).
3. Пресс-конференция (вопрос – ответ).
4. Написание статьи (доклада).
5. Представление статьи аудитории.
6. Подведение итогов (краткое повторение ключевых моментов занятия, оценка деятельности каждого участника игры).

Сценарий деловой игры:

Перед участниками игры ставится следующая ситуация: в компьютерном мире вновь возникла вирусная эпидемия. В связи с этим организуется пресс-конференция, на которую приглашены специалисты по компьютерной вирусологии для разъяснения общих вопросов по компьютерным вирусам. Журналисты после проведения пресс-конференции должны подготовить статью или доклад по обсуждаемой теме.

Вопросы для обсуждения:

1. Когда и кем был введен термин компьютерный вирус?
2. Что такое компьютерный вирус?
3. Расскажите принцип действия вируса.
4. Какие вирусы бывают?
5. Как действуют файловые вирусы?
6. Как действуют макровирусы?
7. Как действуют сетевые вирусы?
8. Каковы причины распространения вирусов?
9. Как защитить компьютер от заражения вирусами?

Деление учеников на специалистов по компьютерной вирусологии и журналистов происходит с помощью жеребьевки. Журналисты придумывают название изданию, которое они представляют.

На первом этапе специалистам по компьютерной вирусологии предоставляется теоретический материал для ознакомления. Пользуясь этим материалом, они будут отвечать на вопросы журналистов. Тем временем, журналисты получают задание: сделать на компьютере заготовку для будущей статьи или доклада в программе OpenOffice.org Impress. Журналисты представляют в статье разные моменты обсуждаемой темы (например, файловые вирусы, макровирусы, сетевые вирусы и т.д.).

На втором этапе организуется пресс-конференция. Журналистам раздаются полоски с вопросами, которые пронумерованы. Желающий задать вопрос поднимает руку, после разрешения называет свое издание, называет имя того специалиста, кому задает вопрос и озвучивает вопрос. Для записи ответов журналистам предоставляются рабочие листы с заготовками вопросов, которыми они будут пользоваться при написании статьи. Их задача - кратко записать услышанный ответ. Если что-то не понятно, то можно переспрашивать.

После обсуждения всех вопросов на третьем этапе организуется написание статьи (доклада). Все участники игры делятся таким образом, чтобы за компьютером работало два человека. Журналистам в помощь предоставляется специалисты по вирусологии.

На четвертом этапе происходит представление каждой парой своей работы. Другие участники могут дополнять и задавать вопросы.

На завершающем этапе подводятся итоги игры, проводятся анализ усвоенных знаний, обмен мнениями по поводу проведения игры, дисциплины, удачных и неудачных выступлений.

Задания для подготовки к участию в деловой игре:

- провести теоретический анализ специальной научной литературы;
- подготовить вопросы для участия в обсуждении темы**;**
- подобрать актуальные темы для исследования (теоретический материал).

7. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине

Фонд оценочных средств по дисциплине для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложение 1 к настоящей рабочей программе дисциплины.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Рекомендуемая литература

Основная литература

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html

2. Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 c. — ISBN 978-5-9227-0757-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/74381.html

3. Никифоров, С. Н. Защита информации. Пароли, скрытие, удаление данных : учебное пособие / С. Н. Никифоров, М. М. Ромаданов. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 108 c. — ISBN 978-5-9227-0783-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/80747.html

Дополнительная литература

1. Никифоров С.Н. Защита информации. Защищенные сети [Электронный ресурс] : учебное пособие / С.Н. Никифоров. — Электрон. текстовые данные. — СПб. : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 80 c. — 978-5-9227-0762-6. — Режим доступа: http://www.iprbookshop.ru/74382

2. Алексеев А.П. Многоуровневая защита информации [Электронный ресурс] / А.П. Алексеев. — Электрон. текстовые данные. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. — 128 c. — 978-5-904029-72-2. — Режим доступа: http://www.iprbookshop.ru/75387

8.2. Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://window.edu.ru/ - единое окно доступа к образовательным ресурсам
2. https://uisrussia.msu.ru/ - база данных и аналитических публикаций университетской информационной системы Россия
3. http://www.iprbookshop.ru - Электронно-библиотечная система IPRbooks (ЭБС IPRbooks) –электронная библиотека по всем отраслям знаний
4. https://www.elibrary.ru/ - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
5. http://www.consultant.ru/ - справочная правовая система КонсультантПлюс
6. https://www.garant.ru/ - справочная правовая система Гарант
7. https://gufo.me/ - справочная база энциклопедий и словарей
8. https://slovaronline.com - справочная база, полная поисковая система по всем доступным словарям, энциклопедиям и переводчикам в режиме Онлайн
9. Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» https://reestr.digital.gov.ru/
10. Общество с ограниченной ответственностью «Интерактивные обучающие технологии» https://htmlacademy.ru/tutorial/php/mysql
11. Web-технологии https://htmlweb.ru/php/mysql.php

9. Материально-техническое обеспечение дисциплины

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине представлено в приложении 8 «Сведения о материально-техническом обеспечении программы высшего образования – программы бакалавриата направления подготовки 09.03.01 «Информатика и вычислительная техника».

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая программное обеспечение, в том числе отечественного производства

Программное обеспечение АНО ВО ОУЭП, являющееся частью электронной информационно-образовательной среды и базирующееся на телекоммуникационных технологиях:

- тренинговые и тестирующие программы;
- интеллектуальные роботизированные системы оценки качества выполнения работ.

Информационные и роботизированные системы, программные комплексы, программное обеспечение для доступа к компьютерным обучающим, тренинговым и тестирующим программам:

- ПК «КОП»;
- ИР «Каскад».

Программное обеспечение, необходимое для реализации дисциплины:

Лицензионное программное обеспечение (в том числе, отечественного производства):

Операционная система Windows Professional 10

ПО браузер – приложение операционной системы, предназначенное для просмотра Web-страниц

Платформа проведения аттестационных процедур с использованием каналов связи (отечественное ПО)

Платформа проведения вебинаров (отечественное ПО)

Информационная технология. Онлайн тестирование цифровой платформы Ровеб (отечественное ПО)

Электронный информационный ресурс. Экспертный интеллектуальный информационный робот Аттестация асессоров (отечественное ПО)

Информационная технология. Аттестационный интеллектуальный информационный робот контроля оригинальности и профессионализма «ИИР КОП» (отечественное ПО)

Электронный информационный ресурс «Личная студия обучающегося» (отечественное ПО)

Свободно распространяемое программное обеспечение (в том числе отечественного производства):

Мой Офис Веб-редакторы https://edit.myoffice.ru (отечественное ПО)

ПО OpenOffice.Org Calc.

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО OpenOffice.Org.Base

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО OpenOffice.org.Impress

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО OpenOffice.Org Writer

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО Open Office.org Draw

http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html

ПО «Блокнот» - стандартное приложение операционной системы (MS Windows, Android и т.д.), предназначенное для работы с текстами

Приложение 1

Автономная некоммерческая организация высшего образования
«Открытый университет экономики, управления и права»
(АНО ВО ОУЭП)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Текущего контроля и промежуточной аттестации
по дисциплине

Б1.О.22 Защита информации

Образовательная программа направления подготовки
09.03.01 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»,
направленность (профиль): «Информатика и вычислительная техника»
Квалификация: бакалавр

Москва 2021

7.1. Оценочные средства

Назовите понятия:

№	Определение	Ответ
1.	Организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации компьютерной системы для обеспечения защиты информации.	Методы и средства защиты информации
2.	Набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.	Политика безопасности
3.	Событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации.	Угроза безопасности информации
4.	Неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками.	Утечка
5.	Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.	Уязвимость информации
6.	Неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.	Целостность информации
7.	Субъект с полномочиями владения, пользования и распоряжения информационных ресурсов, систем и технологий	Собственник
8.	Доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати).	Разглашение
9.	Воздействие на защищаемую информацию из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий (например, уничтожение документов в результате отказа накопителя на жестком магнитном диске компьютера).	Непреднамеренное воздействие
10.	Известность содержания информации только имеющим соответствующие полномочия субъектам.	Конфиденциальность информации

Вопросы открытого типа:

№	Вопрос	Ответ
1.	Что представляет собой несанкционированные действия обслуживающего персонала компьютерной сети (например, ослабление политики безопасности администратором,	Умышленная угроза информационной

	отвечающим за безопасность компьютерной сети)?	безопасности
2.	К какому типу угроз компьютерных систем можно отнести следующие действия: К непреднамеренным угрозам относятся: ошибки в проектировании; ошибки в разработке программных средств; случайные сбои в работе аппаратных средств , линий связи, энергоснабжения; ошибки пользователей; воздействие на аппаратные средства компьютерных сетей физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.?	Непреднамеренные угрозы компьютерных систем
3.	Как называются перечисленные каналы утечки информации? Хищение носителей информации, сбор производственных отходов с информацией (бумажных и магнитных носителей), копирование носителей информации, намеренное использование для несанкционированного доступа к информации незаблокированных терминалов других пользователей компьютерных сетей, маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т. п.), обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.	Непосредственные каналы утечки информации
4.	К какому виду каналов утечки информации можно отнести перечисленные виды: использование подслушивающих (радио закладных) устройств, дистанционное видеонаблюдение, перехват побочных электромагнитных излучений и наводок?	Косвенные каналы утечки информации
5.	Методы и средства организационной защиты информации включают в себя: − ограничение физического доступа к объектам КС и реализация режимных мер; − ограничение возможности перехвата ПЭМИН (перехват побочных электромагнитных излучений и наводок); − разграничение доступа к информационным ресурсам и процессам КС (установка правил разграничения доступа, шифрование информации при ее хранении и передаче, обнаружение и уничтожение аппаратных и программных закладок); − резервное копирование наиболее важных с точки зрения утраты массивов документов; − профилактику заражения компьютерными вирусами.	Что включают в себя организационные методы защиты информации?
6.	Как называется процесс проверки и исправления ошибок в данных?	Коррекция ошибок

7.	К какому типу информации относятся перечисленные виды информации: служебная тайна (врачебная, адвокатская, тайна суда и следствия и т.п.), коммерческая тайна, персональные данные (сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность)?	Конфиденциальная информация
8.	Как называется угроза раскрытия параметров подсистемы защиты информации, входящей в состав компьютерной сети?	Опосредованная угроза безопасности информации
9.	Какая функция проверяет подлинность пользователя?	Аутентификация
10.	Какая функция отвечает за контроль доступа к данным?	Авторизация

Тестовые задания:

1	Упорядоченная совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы, называется: **a) информационной системой;** b) политикой безопасности; c) информационной технологией; d) информационным процессором.
2	Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, называется **Защитой информации**
3	Получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней, называется **Несанкционированным доступом**
4	Набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа, называется: a) защитой информации; **b) политикой безопасности;** c) стратегией защиты информации; d) правилами поведения.
5	Информация, содержание которой может быть понятно любому субъекту, называется:

	a) сказкой; b) инструкцией хакера; c) криптосистемой; **d) открытым текстом.**
6	Доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати): a) компьютерным шпионажем; **b) разглашением;** c) вредительством; d) предательством.
7	Субъект с полномочиями владения информационными ресурсами, их пользования и распоряжения, называется a) сетевым администратором; **b) собственником информационных ресурсов;** c) программистом; d) пользователем.
8	Неконтролируемое распространение защищаемой информации путем ее разглашения, несанкционированного доступа к ней и получения разведками: a) расползанием информации; b) информационным предательством; c) вредительством; **d) утечкой.**
9	Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации, называется**:** a) устареванием политики безопасности; b) сбоем системы защиты информации; **c) уязвимостью информации;**

	d) обходом защиты информации.
10	Воздействие на защищаемую информацию из-за ошибок пользователя, сбоя технических или программных средств, природных явлений, иных нецеленаправленных воздействий, называется: **a) непреднамеренным воздействием;** b) самоатакой; c) глюком.

Ключ к тестовым заданиям

1	2	3	4	5
a	зашитой информации;	несанкционированным доступом;	b	d
6	**7**	**8**	**9**	**10**
b	b	d	c	a

7.2. Система оценивания результатов текущего контроля успеваемости и промежуточной аттестации и критерии выставления оценок, описание шкал оценивания

Критерии и описание шкал оценивания приведены в Порядке разработки оценочных материалов и формирования фонда оценочных материалов для проведения промежуточной и итоговой (государственной итоговой) аттестации и критерии оценивания при текущем контроле успеваемости (локальный нормативный акт утв. приказом АНО ВО ОУЭП 20.01.2021 № 10)

№ п/п	Наименование формы проведения текущего контроля успеваемости и промежуточной аттестации	Описание показателей оценочного материала	Представление оценочного материала в фонде	Критерии и описание шкал оценивания *(шкалы: 0 – 100%, четырехбалльная, тахометрическая)*
1	Позетовое тестирование (ПЗТ)	Контрольное мероприятие по учебному материалу каждой темы (раздела) дисциплины, состоящее в выполнении обучающимся системы стандартизированных заданий, которая позволяет автоматизировать процедуру измерения уровня знаний и умений	Система стандартизированных заданий	- от 0 до 49,9 % выполненных заданий – не удовлетворительно; - от 50% до 69,9% - удовлетворительно; - от 70% до 89,9% - хорошо; - от 90% до 100% - отлично.

		обучающегося. Модульное тестирование включает в себя следующие типы заданий: задание с единственным выбором ответа из предложенных вариантов, задание на определение верных и неверных суждений; задание с множественным выбором ответов.		
2	*Экзамен*	1-я часть экзамена: выполнение обучающимися практико-ориентированных заданий (аттестационное испытание промежуточной аттестации, проводимое устно с использованием телекоммуникационных технологий)	Практико-ориентированные задания	*Критерии оценивания преподавателем практико-ориентированной части экзамена:* – соответствие содержания ответа заданию, полнота раскрытия темы/задания (оценка соответствия содержания ответа теме/заданию); – умение проводить аналитический анализ прочитанной учебной и научной литературы, сопоставлять теорию и практику; – логичность, последовательность изложения ответа; – наличие собственного отношения обучающегося к теме/заданию; – аргументированность, доказательность излагаемого материала. *Описание шкалы оценивания практико-ориентированной части экзамена* Оценка «*отлично*» выставляется за ответ, в котором содержание соответствует теме или заданию, обучающийся глубоко и прочно усвоил учебный материал, последовательно, четко и логически стройно излагает его, демонстрирует собственные суждения и размышления на заданную тему, делает соответствующие выводы; умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, не затрудняется с ответом при видоизменении заданий, приводит материалы различных научных источников, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения задания, показывает должный уровень сформированности компетенций.

				Оценка «*хорошо*» выставляется обучающемуся, если ответ соответствует и раскрывает тему или задание, показывает знание учебного материала, грамотно и по существу излагает его, не допуская существенных неточностей при выполнении задания, правильно применяет теоретические положения при выполнения задания, владеет необходимыми навыками и приемами его выполнения, однако испытывает небольшие затруднения при формулировке собственного мнения, показывает должный уровень сформированности компетенций. Оценка «*удовлетворительно*» выставляется обучающемуся, если ответ в полной мере раскрывает тему/задание, обучающийся имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении учебного материала по заданию, его собственные суждения и размышления на заданную тему носят поверхностный характер. Оценка *«неудовлетворительно*» выставляется обучающемуся, если не раскрыта тема, содержание ответа не соответствует теме, обучающийся не обладает знаниями по значительной части учебного материала и не может грамотно изложить ответ на поставленное задание, не высказывает своего мнения по теме, допускает существенные ошибки, ответ выстроен непоследовательно, неаргументированно. Итоговая оценка за экзамен выставляется преподавателем в совокупности на основе оценивания результатов электронного тестирования обучающихся и выполнения ими практико-ориентированной части экзамена
		2-я часть экзамена: выполнение электронного тестирования (аттестационное испытание промежуточной аттестации с использованием информационных	Система стандартизирован-ных заданий (тестов)	*Описание шкалы оценивания электронного тестирования:* – от 0 до 49,9 % выполненных заданий – неудовлетворительно; – от 50 до 69,9% – удовлетворительно;

		тестовых систем)		– от 70 до 89,9% – хорошо; – от 90 до 100% – отлично