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

РАБОЧАЯ ПРОГРАММА

учебной дисциплины

Б1.В.ДЭ.05.01 Техническая 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 № 14-01 от 14.01.2022г.)

Разработчик:
Чернышенко С.В., д.б.н.; д.ф.-м. н., проф.

Москва 2022

1. Цели и задачи дисциплины

Цель дисциплины - формирование у студентов знаний по основам технической защиты информации, а также навыков и умения в применении знаний для конкретных условий.

Задачи дисциплины:

• получение фундаментальных знаний о концепции инженерно-технической защиты информации;

• дать знания по физическим, организационным основам инженерно-технической защиты информации;

• получение знаний о средствах и методах добывания и средствах и методах защиты конфиденциальной информации;

• методическое обеспечение инженерно-технической защиты информации.

2. Место дисциплины в структуре ОП

Блок 1 «Дисциплины (модули)», часть формируемая участниками образовательных отношений, элективные дисциплины.

3. Планируемые результаты обучения по дисциплине

В результате изучения дисциплины обучающийся должен освоить:

Обобщенную трудовую функцию (ОТФ):

Выполнение работ и управление работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

С24/6 Развертывание ИС у заказчика

Трудовые действия:

Настройка ИС для оптимального решения задач заказчика

профессиональную компетенцию:

ПК-6. Способен находить оптимальные решения при проектировании и разработке информационных систем, обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности..

Результаты освоения дисциплины, установленные индикаторы достижения компетенций

Наименование компетенции	**Индикаторы достижения компетенции**	**Показатели (планируемые) результаты обучения**
ПК-6. Способен находить оптимальные решения при проектировании и разработке информационных систем, обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности.	ПК-6.1. Знает: предметную область автоматизации, инструменты и методы оценки качества и эффективности информационной системы, инструменты и методы оптимизации информационных систем, современные инструменты и методы управления организацией, в том числе методы планирования деятельности, распределения поручений, контроля исполнения, принятия решений	**Знать:** ● способы разграничения доступа и средства их реализации; ● предметную область автоматизации, инструменты и методы оценки качества и эффективности информационной системы
	ПК-6.2. Умеет: находить оптимальные решения при проектировании и разработке информационных систем, обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	**Уметь:** ● проводить анализ защищенности компьютера и сетевой среды с использованием сканера безопасности ● осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности
	ПК-6.3. Владеет: методами оптимизации информационных систем, методами принятия решений, методиками проведения экспериментов по проверке корректности и эффективности проектных решений	**Владеть:** ● технологиями установки и настройки конфигурацию компьютерных сетей и сетевого оборудования с целью обеспечения технической защиты информации

Знания, умения и навыки, приобретаемые обучающимися в результате изучения дисциплины «Техническая 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)**	**54,2**		**8,2**	
	В том числе в форме практической подготовки		**2**		***2***
1.1	занятия лекционного типа (лекции)	12		2	
1.2	занятия семинарского типа (практические)*, в том числе:	40		4	
1.2.1	семинар-дискуссия, практические занятия		0 40		0 4
	в форме практической подготовки		2		*2*
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)**	**74**		**129**	
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)	74		129	
2.2	самостоятельная работа при подготовке к промежуточной аттестации	**15,8**		**6,8**	
3	**Общая трудоемкость дисциплины**	**4 з.е. / 144 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	Технические каналы утечки информации	Технические каналы утечки информации: структура, классификация и основные характеристики.

		Технические каналы утечки информации, обрабатываемой техническими средствами приема информации. Физическая природа побочных электромагнитных излучений. Элементарный электрический излучатель. Элементарный магнитный излучатель. Электромагнитные каналы утечки информации. Электрические каналы утечки информации. Параметрические каналы утечки информации. Технические каналы утечки информации при передаче ее по каналам связи. Электрические линии связи. Каналы утечки информации за счет паразитных связей. Электрические каналы утечки информации. Электромагнитные каналы утечки информации. Индукционные каналы утечки информации. Технические каналы утечки речевой информации. Акустические каналы утечки речевой информации. Выброакустические каналы утечки речевой информации. Акустоэлектрические каналы утечки речевой информации. Оптико-электронные каналы утечки речевой информации. Параметрические каналы утечки речевой информации. Технические каналы утечки видовой информации.
2	Средства обнаружения каналов утечки информации	Индикаторы электромагнитного поля. Сканирующие радиоприемники. Анализаторы спектра, радиочастотомеры. Многофункциональные комплексы для выявления каналов утечки информации. Средства обнаружения средств съема информации и выявления каналов ее утечки. Комплексы измерения ПЭМИН. Нелинейные локаторы. Металлодетекторы. Досмотровые эндоскопы.
3	Скрытие и защита информации от утечки по техническим каналам	Концепция и методы инженерно-технической защиты информации. Экранирование электромагнитных волн. Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления. Фильтрация информационных сигналов. Пространственное и линейное зашумление. Способы предоставления утечки информации через ПЭМИН ПК. Устройства контроля и защиты слаботочных линий и сети. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам. Скрытие речевой информации в телефонных системах с использованием криптографических методов. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах.
4	Методы и средства инженерной защиты и технической охраны объектов	Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов. Система охранно-тревожной сигнализации. Система контроля и управления доступом. Телевизионные системы. Система пожарной сигнализации. Периметровая охрана.

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 – 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 06 апреля 2021 г. N 245 "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 1 Технические каналы утечки информации

Темы устного доклада

1. Особенности информации как предмета защиты.
2. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения информации.
3. Каналы утечки речевой информации.
4. Каналы утечки информации при ее передаче по каналам связи.
5. Технические каналы утечки информации, возникающей при работе вычислительной техники за счет ПЭМИН.
6. Элементарный электрический излучатель.
7. Элементарный магнитный излучатель.
8. Электромагнитные каналы утечки информации ТСПИ
9. Электрические каналы утечки информации.
10. Параметрический канал утечки информации.
11. Каналы утечки информации за счет паразитных связей.

12. Индукционный канал утечки информации.
13. Звукоизоляция помещений.
14. Акустические каналы утечки речевой информации.
15. Виброакустические технические каналы утечки речевой информации.
16. Акустоэлектрические каналы утечки речевой информации.
17. Оптико-электронный технический канал утечки речевой информации.
18. Параметрические технические каналы утечки речевой информации.
19. Технические каналы утечки видовой информации.
20. Способы скрытого видеонаблюдения и съемки.

Раздел 2 Средства обнаружения каналов утечки информации
Темы устного доклада

1. Демаскирующие признаки объектов.
2. Демаскирующие признаки радиоэлектронных средств.
3. Индикаторы электромагнитного поля.
4. Сканирующие радиоприемники.
5. Анализаторы спектра, радиочастотомеры.
6. Многофункциональные комплекты для выявления каналов утечки информации.
7. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки ПКУ-6М.
8. Портативный комплект для обнаружения средств съема информации и выявления каналов ее утечки «Пиранья».
9. Комплексы измерения ПЭМИН.
10. Принцип действия и назначение нелинейного локатора.
11. Комплекс для измерения характеристик акустических сигналов «Спрут-7».
12. Металлодетекторы.
13. Портативная рентгенотелевизионная установка «НОРКА».
14. Досмотровые эндоскопы.
15. Схема исследования виброакустических сигналов.
16. Выявление микрофонного эффекта и обнаружение скрытых микрофонов.
17. Комплекс RS turbo.
18. Типы нелинейных локаторов.
19. Рентгенотелевизионные устройства.
20. Виды средств обнаружения радиозакладных устройств.

Раздел 3 Скрытие и защита информации от утечки по техническим каналам
Темы устного доклада

1. Средства перехвата сигналов.
2. Средства противодействия подслушиванию.
3. Средства противодействия наблюдению.
4. Звукопоглощающие материалы и конструкции.
5. Звукоизоляция помещений.
6. Методические подходы к оценке эффективности защиты речевой информации.
7. Оценка защищенности по виброакустическому каналу.
8. Основные виды датчиков перехвата информации виброакустического канала и их характеристики.
9. Направленные и лазерный микрофоны.
10. Основные направления защиты от съема информации с телефонной линии.
11. Зоны перехвата информация и виды подключений закладных устройств в каналах телефонной связи.
12. Метод «синфазной низкочастотной маскирующей помехи» для защиты телефонных линий.
13. Метод «высокочастотной маскирующей помехи» для защиты телефонных линий.
14. Метод «ультразвуковой маскирующей помехи» для защиты телефонных линий.
15. Метод «низкочастотной маскирующей помехи» и «компенсационный» метод для защиты телефонных линий.
16. Методы «повышения напряжения» и «понижения напряжения» для защиты телефонных линий.
17. Пространственное и линейное зашумление.
18. Безопасность оптоволоконных кабельных систем.
19. Устройства контроля и защиты слаботочных линий и сети.
20. Экранированные помещения.

Раздел 4 Методы и средства инженерной защиты и технической охраны объектов
Темы устного доклада

1. Категории объектов защиты.

2. Особенности задач охраны различных типов объектов.
3. Общие принципы обеспечения безопасности объектов.
4. Основные задачи, решаемые физическими средствами зазиты.
5. Базовые принципы инженерно-технической защиты информации.
6. Основные направления инженерно-технической защиты информации.
7. Основные задачи инженерно-технической защиты информации.
8. Показатели эффективности инженерно-технической защиты информации.
9. Система охранно-тревожной сигнализации.
10. Система контроля и управления доступом.
11. Система пожарной сигнализации.
12. Периметровая охрана.
13. Охранные извещатели.
14. Электронная проходная.
15. Применение телевизионных систем для защиты объектов.
16. Пожарные извещатели.
17. Тепловизионнные охранные системы.
18. Инфракрасные охранные системы.
19. Требования к системам периметровой охраны.
20. Автоматизированное управление системами по тревогам СКУД.

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. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 c. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89451.html

2. 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: http://www.iprbookshop.ru/87995.html

3. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 368 c. — ISBN 978-5-4497-0931-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102069.html

Дополнительная литература

1. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 c. — ISBN 978-5-4488-0074-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87992.html

2. Голиков, А. М. Защита информации от утечки по техническим каналам : учебное пособие / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. — 256 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72090.html

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. https://basegroup.ru/community/camp - Кампус BaseGroup Labs площадка для обмена аналитиками опытом: вопросы и ответы, статьи, книги, база знаний, блоги, презентации, выступления. Описание методик, алгоритмов, практических кейсов и проектного опыта в области программных продуктов.
11. https://www.sciencedirect.com/browse/journals-and-books?contentType=JL&subject=computer-science – коллекция журналов в открытом доступе по информатике
12. https://reestr.digital.gov.ru/ - официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет»
13. https://htmlweb.ru/php/mysql.php - Web-технологии
14. https://basegroup.ru/community/camp - кампус BaseGroup Labs - площадка для обмена аналитиками опытом: вопросы и ответы, статьи, книги, база знаний, блоги, презентации, выступления (описание методик, алгоритмов, практических кейсов и проектного опыта в области программных продуктов)
15. http://expert.ru/dossier/story/tehnologii/ - статьи журнала «Эксперт» в области информационных технологий
16. http://www.emanual.ru/ - сайт, посвящённый всем значимым событиям в IT-индустрии: новейшие разработки, уникальные методы и горячие новости
17. https://www.securitylab.ru/ - платформа "Безопасность в ИТ" здесь публикуются статьи, новости, аналитика и обзоры в области информационной безопасности и киберзащиты.
18. https://xakep.ru/ - Сайт Журнала "Хакер" это популярный ресурс о кибербезопасности, на котором можно найти статьи, видеоматериалы и обсуждения тем, связанных с защитой информации

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.В.ДЭ.05.01 Техническая защита информации

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

Москва 2022

7.1. Оценочные средства

Назовите основные понятия:

№	Определение	Ответ
1.	Электронные и электронно-механические устройства, включаемые в состав технических средств компьютерной системы и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности.	Аппаратные средства защиты информации
2.	Отпечатки пальцев, геометрическая форма руки, узор радужной оболочки глаза, рисунок сетчатки глаза, геометрическая форма и размеры лица, тембр голоса, геометрическая форма и размеры уха и др.	Биометрические характеристики пользователей компьютерной системы
3.	Физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства.	Инженерно-технические средства защиты информации
4.	Автономно функционирующая программа, обладающую одновременно тремя свойствами: способностью к включению своего кода в тела других файлов и системных областей памяти компьютера, последующему самостоятельному выполнению, самостоятельному распространению в компьютерных системах.	Компьютерный вирус
5.	Действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.	Атака на компьютерную систему
6.	Специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.	Антивирусная программа
7.	Маскировка злоумышленника под легального пользователя с применением похищенной или полученной обманным путем (с помощью так называемой социальной инженерии) идентифицирующей информации.	Маскарад
8.	Программные средства, которые определяют условия прохождения пакетов данных из одной части распределенной компьютерной системы (открытой) в другую (защищенную) по особым правилам.	Межсетевые экраны
9.	Создание условий для связи по компьютерной сети легального пользователя с терминалом нарушителя, выдающего себя за легальный объект компьютерной системы (например, одного из ее серверов).	Мистификация
10.	Угроза безопасности информации в компьютерной системе – событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации.	Угроза безопасности информации

Вопросы открытого типа:

№	Вопрос	Ответ
1	К какому виду средств защиты информации относятся перечисленные? − защита территории и помещений от проникновения нарушителей; − защита аппаратных средств и носителей информации от хищения; − предотвращение возможности перехвата (перехват побочных электромагнитных излучений и наводок), вызванных работающими техническими средствами и линиями передачи данных; − минимизация материального ущерба от потерь информации, возникших в результате стихийных бедствий и техногенных аварий.	Средства инженерно-технической защиты информации
2	Что представляют собой специальные программы, включаемые в состав программного обеспечения исключительно для выполнения защитных функций? Такие как: − программы идентификации и аутентификации пользователей; − программы разграничения доступа пользователей к ресурсам; − программы шифрования информации; − программы защиты информационных ресурсов от несанкционированного изменения, использования и копирования.	Программные средства защиты информации
3	К какому виду характеристик относятся следующие характеристики, используемые при их аутентификации: отпечатки пальцев, геометрическая форма руки, узор радужной оболочки глаза, рисунок сетчатки глаза, геометрическая форма и размеры лица, тембр голоса, геометрическая форма и размеры уха и др.?	Биометрические характеристики
4	При каком виде аутентификации пользователь для входа в систему должен не только ввести пароль, но и предъявить элемент аппаратного обеспечения, содержащий подтверждающую его подлинность ключевую информацию?	При двухфакторной аутентификации
5	Как называется тип вредоносных программ, разработанных специально для нанесения ущерба компьютеру или системе?	Деструктивные компьютерные вирусы
6	Как называется способ, посредством которого вирус или другая вредоносная программа попадает на компьютер или систему и начинает свою деструктивную или вредоносную деятельность?	Канал заражения вирусами
7	Как называется резидентная программа, которая контролирует опасные действия, характерные для вирусных программ, и запрашивает подтверждение на их выполнение?	Антивирусная программа фильтр
8	Что представляет собой антивирусная программа, которая обеспечивает поиск и обнаружение вирусов в	Антивирусная программа детектор

	оперативной памяти и на внешних носителях?	
9	Как называется антивирусная программа, позволяющая обнаруживать и обезвреживать вирусы? При обезвреживании вирусов среда обитания может восстанавливаться или не восстанавливаться.	Антивирусная программа доктор
10	Как называется программа, запоминающая исходное состояние программ, каталогов и системных областей и периодически сравнивающую текущее состояние с исходным? Сравнение может выполняться по параметрам: длина и контрольная сумма файла и т.п.	Антивирусная программа ревизор

Тестовые задания:

1	Подтверждение того, что предъявленное имя соответствует данному субъекту, называется a) изоляцией; b) аутизмом; **c) аутентификацией;** d) персонализацией.
2	Способность обеспечения беспрепятственного доступа субъектов к интересующей их информации, называется: **a) доступностью информации;** b) защитой информации; c) легализацией информации; d) симметричностью информации.
3	Аутентификация, при которой пользователь для входа в систему должен не только ввести пароль, но и предъявить элемент аппаратного обеспечения, содержащий подтверждающую его подлинность ключевую информацию, называется: a) двойной проверкой; b) двойной защитой; **c) двухфакторной аутентификацией;** d) симметричной криптосистемой.
4	Специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ, восстановления заражённых такими программами файлов и предотвращения заражения файлов или операционной системы вредоносным кодом,

	называется: a) системной программой; **b) антивирусной программой;** c) лечебной программой; d) операционной системой.
5	Вирусы, которые заражают главный загрузочный сектор жесткого диска (Master Boot record, MBR) или загрузочный сектор раздела жесткого диска, подменяя находящиеся в них программы начальной загрузки и загрузки операционной системы своим кодом, называются: a) **загрузочными вирусами**; b) рекламными вирусами; c) полифагом; d) fire wall.
6	Вирусы в файлах документов, созданных программами пакета Microsoft Office, которые распространяются с помощью включенных в них макросов (процедур на языке программирования Visual Basic for Applications, VBA, или WordBasic, WB), называются: **макровирусами**
7	Маскировка злоумышленника под легального пользователя с применением похищенной или полученной обманным путем (с помощью так называемой социальной инженерии) идентифицирующей информации, называется: **маскарадом**
8	Автономно функционирующая программа, обладающую одновременно тремя свойствами: способностью к включению своего кода в тела других файлов и системных областей памяти компьютера, последующему самостоятельному выполнению, самостоятельному распространению в компьютерных системах, называется: **a) компьютерным вирусом;** b) автопрограммой; c) криптографией; d) резидентной программой.

9	Событие или действие, которое может вызвать изменение функционирования компьютерной системы, связанное с нарушением защищенности обрабатываемой в ней информации, называется: a) **угрозой безопасности информации**; b) хакерской атакой; c) вирусной атакой; d) потерей протокола безопасности.
10	Программные средства, которые определяют условия прохождения пакетов данных из одной части распределенной компьютерной системы (открытой) в другую (защищенную) по особым правилам, называются: **a) межсетевыми экранами;** b) защитными ширмами; c) подсмотрщиками; d) антишпионами.

Ключ к тестовым заданиям

1	**2**	**3**	**4**	**5**
c	a	c	b	a
6	**7**	**8**	**9**	**10**
макровирусами	маскарадом	a	a	a

7.2. Система оценивания результатов текущего контроля успеваемости и промежуточной аттестации, а также 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	*Тест-тренинг*	Вид тренингового учебного занятия, задачей которого является закрепление учебного материала, а также проверка знаний обучающегося как по дисциплине в целом, так и по отдельным темам (разделам) дисциплины .	Система стандартизированных заданий	- от 0 до 69,9 % выполненных заданий – не зачтено; - 70 до 100 % выполненных заданий – зачтено.
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 тестовых систем)	Система стандартизирован-ных заданий (тестов)	*Описание шкалы оценивания электронного тестирования:* – от 0 до 49,9 % выполненных заданий – неудовлетворительно; – от 50 до 69,9% – удовлетворительно; – от 70 до 89,9% – хорошо; – от 90 до 100% – отлично