Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Карпов Евгений Борисович
Должность: Ректор
Дата подписания: 18.07.2022 14:14:24
Уникальный программный ключ:
34e81b9ebf022d792ddf4ba544335e3bff5ea8f9d7bcf1d2f098d273e86a810b

МЕЖДУНАРОДНАЯ ПОЛИЦЕЙСКАЯ АКАДЕМИЯ ВПА
Автономная некоммерческая организация высшего образования
АНО ВО МПА ВПА

УТВЕРЖДАЮ
Проректор по УМР
Л.М. Окунева
24 декабря 2021 г.

Гуманитарные аспекты информационной безопасности. Информационное противоборство

рабочая программа дисциплины (модуля)

Учебный план 10.03.01 Информационная безопасность
Учебный год начала подготовки 2022-2023

Форма обучения **очно-заочная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 26
самостоятельная работа 82

Виды контроля в семестрах:
зачеты 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	12 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	12	4	12	4
Практические	14	8	14	8
Итого ауд.	26	12	26	12
Контактная работа	26	12	26	12
Сам. работа	82	96	82	96
Итого	108	108	108	108

Рабочая программа дисциплины

Гуманитарные аспекты информационной безопасности. Информационное противоборство

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:

10.03.01 Информационная безопасность

утвержденного учёным советом вуза от 23.12.21 протокол № 3.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цель дисциплины: ознакомить студентов с принципами и методами создания, хранения, редактирования, представления и защиты информации, а также с по-следними достижениями в этих областях, при этом особое внимание акцентируется на изучение специализированного применения технологий обработки информации, необхо-димого студентам в последующей профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Базы данных, системы управления базами данных
2.1.2	Внедрение и эксплуатация средств защиты информации
2.1.3	Организационное обеспечение аттестации объектов информатизации
2.1.4	Современные средства и технологии исследования личности
2.1.5	Технические средства охраны
2.1.6	Технология больших данных и основы информационного противоборства
2.1.7	Производственная (эксплуатационная) практика
2.1.8	Профайлинг в различных сферах деятельности
2.1.9	Системы конфиденциального электронного документооборота
2.1.10	Современные информационные социальные сервисы
2.1.11	Технологии обеспечения информационной безопасности
2.1.12	Основы экономики и экономической деятельности в сфере информатизации и информационной безопасности
2.1.13	Учебная (ознакомительная) практика
2.1.14	Организационное и правовое обеспечение информационной безопасности
2.1.15	Основы информационной безопасности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Преддипломная практика
2.2.2	Информационная безопасность критических информационных структур
2.2.3	Риски информационной безопасности и философские основы искусственногоинтеллекта
2.2.4	Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-1.1: Знает стратегию и основные направления развития современного информационного общества
ОПК-1.2: Адекватно оценивает роль информации и информационной безопасности в современном информационном обществе и в условиях цифровой экономики
ПК-3: Способен разрабатывать и применять методики осуществления аналитической деятельности в средствах социальной коммуникации в ходе организации и решения задач информационного противоборства
ПК-3.1: Выполняет анализ и обработку рисков информационной безопасности в средствах социальной коммуникации в ходе организации и решения задач информационного противоборства
ПК-3.2: Принимает участие в построении моделей угроз и нарушителей

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Основы теории информационной безопасности, классификацию и основное содержание нормативных документов в данной области.
3.2	**Уметь:**
3.2.1	Использовать полученные навыки по реализации технологий, направленных на обеспечение информационной безопасности в условиях операционной системы Windows, ее приложений, локальных и общемировых сетей.
3.3	**Владеть:**
3.3.1	Опытом (навыком) работы с антивирусными пакетами, настройки параметров информационной безопасности в приложениях – браузерах сети Internet.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)			
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**
	Раздел 1. Гуманитарные аспекты информационной безопасности. Информационное противоборство		
1.1	Информационная безопасность и ее аспекты. /Лек/	8	0,5
1.2	Общие положения теории информационной безопасности. /Лек/	8	0,5
1.3	Стратегии защиты информации. /Лек/	8	0,5
1.4	Угрозы информационной безопасности. /Лек/	8	0,5
1.5	Методы криптографии. /Пр/	8	1
1.6	Центр обеспечения безопасности Windows. /Пр/	8	1
1.7	Локальная политика безопасности при администрировании Windows. /Пр/	8	1
1.8	Информационная безопасность и ее аспекты. /Ср/	8	5
1.9	Общие положения теории информационной безопасности. /Ср/	8	5
1.10	Стратегии защиты информации. /Ср/	8	5
1.11	Нарушители и нарушения информационной безопасности. /Ср/	8	5
1.12	Защита информационной безопасности. /Ср/	8	16
1.13	Угрозы информационной безопасности. /Ср/	8	16
1.14	Стандарты и спецификации в области информационной безопасности. /Лек/	8	0,5
1.15	Административный уровень информационной безопасности /Лек/	8	0,5
1.16	Общие сведения о стандартах и спецификациях в области информационной безопасности. /Лек/	8	0,5
1.17	Безопасность локальных объектов и локальных сетей. /Лек/	8	0,5
1.18	Информационная безопасность в условиях локальных сетей. /Пр/	8	1
1.19	Сеансовое конфигурирование Windows. /Пр/	8	3
1.20	Информационная безопасность в СУБД Access. /Пр/	8	1
1.21	Стандарты и спецификации в области информационной безопасности. /Ср/	8	8
1.22	Административный уровень информационной безопасности. /Ср/	8	8
1.23	Общие сведения о стандартах и спецификациях в области информационной безопасности. /Ср/	8	8
1.24	Безопасность локальных объектов и локальных сетей. /Ср/	8	8
1.25	Обеспечение информационной безопасности в общемировых сетях. /Ср/	8	8
1.26	/ЗачётСОц/	8	4

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Вопросы для самоконтроля и текущей аттестации

Понятие информационной безопасности.
Концепция информационной безопасности.
Место информационной безопасности экономических систем в национальной безопасности страны.
Важность и сложность проблемы информационной безопасности.
Информационная безопасность в условиях функционирования в России глобальных сетей.
Теория информационной безопасности информационных систем, ее основные составляющие и задачи.
Моделирование процессов защиты информации.
Модели безопасности и их применение.
Понятие стратегии защиты. Виды стратегий защиты.
Критерии обоснования стратегии защиты.
Понятие угрозы безопасности информации и общие подходы к ее классификации.
Классификация угроз безопасности информации по способам их возможного негативного воздействия.
Угрозы доступности, целостности, конфиденциальности.
Происхождение угроз безопасности информации.
Предпосылки появления угроз.
Понятие нарушителя безопасности информации.
Виды противников или нарушителей безопасности информации.
Виды возможных нарушений информационной системы.
Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
Анализ способов нарушений информационной безопасности.
Вирус как типичное нарушение информационной безопасности. Виды вирусов.
Понятие системы защиты информации.

Типизация и стандартизация систем защиты информации.
Центры защиты информации и их функции.
Основные технологии построения защищенных ЭИС.
Использование защищенных ЭИС.
Понятие криптографии. Методы криптографии.
Политика безопасности.
Программа безопасности.
Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
Международные стандарты информационного обмена.
Стандарты и спецификации в области информационной безопасности и их классификация.
«Оранжевая книга».
Гармонизированные критерии европейских стран.
Спецификация internet-сообщества RFC 1510 «сетевой сервис аутентификации kerberos (v5)».
Руководящие документы (РД) Гостехкомиссии России.
X.800 «архитектура безопасности для взаимодействия открытых систем».
Технические спецификации IPSEC, TLS.
Рекомендация «как выбирать поставщика internet-услуг».
Британский стандарт BS 7799 «управление информационной безопасностью. Практические правила».
Безопасность операционных систем.
Безопасность систем управления базами данных.
Безопасность виртуальных частных сетей.
Безопасность виртуальных локальных сетей.
Безопасность смарт – карт.
Архитектура средств безопасности IP-уровня.
Контексты безопасности и управление ключами.
Обеспечение аутентичности IP-пакетов.
Обеспечение конфиденциальности сетевого трафика.
Роль поставщика internet-услуг в реагировании на нарушения безопасности.
Меры по защите internet-сообщества.
Обеспечение безопасности маршрутизаторов.
Особенности использования управляющих протоколов.
Безопасное размещение сетевого оборудования потребителя.
Защита системной инфраструктуры.

5.2. Темы письменных работ (контрольных и курсовых работ, рефератов)

Учебным планом не предусмотрены.

5.3. Оценочные средства для промежуточной аттестации

ФОС представлен в УМК дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год, эл. адрес
Л1.1	Артемов А. В.	Информационная безопасность: курс лекций: Учебная литература для ВУЗов	Орел: МАБИВ, 2014 http://biblioclub.ru/index.php?page=book&id=428605&sr=1
Л1.2	Башлы П. Н. , Баранова Е. К. , Бабаш А. В.	Информационная безопасность: Учебно-практическое пособие	М.: Евразийский открытый институт, 2011 http://biblioclub.ru/index.php?page=book_red&id=90539

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год, эл. адрес
Л2.1	Колябин А.Ю.	Информационная безопасность и защита информации: сборник студенческих работ	Москва: Студенческая наука,, 2012 https://biblioclub.ru/index.php?page=book_red&id=227774&sr=1

6.2.1 Перечень программного обеспечения

6.3.1.1	Microsoft Windows, OpenOffice, доступ в сеть Интернет.

6.2.2 Перечень современных профессиональных баз данных и информационных справочных систем

6.3.2.1	Каталог документов по направлению Информационная безопасность https://cisoclub.ru/doc/
6.3.2.2	Журнал «Информационная безопасность» https://www.itsec.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей). Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно - образовательную среду.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ И КРИТЕРИЯМ ОЦЕНИВАНИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.

Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание -обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

Главная задача лекционного курса - сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Основные функции лекций: 1. Познавательно-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. информационная.

Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

При подготовке важны не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

При проведении учебных занятий обеспечиваются развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Для контроля знаний студентов по данной дисциплине необходимо проводить оперативный, рубежный и итоговый контроль.

Оперативный контроль осуществляется путем проведения опросов студентов на семинарских занятиях, проверки выполнения практических заданий, а также учета вовлеченности (активности) студентов при обсуждении мини-докладов, организации ролевых игр и т.п.

Контроль за самостоятельной работой студентов по курсу осуществляется в двух формах: текущий контроль и итоговый. Рубежный контроль (аттестация) подразумевает проведение тестирования по пройденным разделам курса. В тестирование могут быть включены темы, предложенные студентам для самостоятельной подготовки, а также практические задания.

Уровень сформированности профессиональных компетенций каждого обучающегося оценивается по следующей шкале (от 1 до 5):
1 – не справляется с выполнением типовых профессиональных задач, не проявляет ни один из навыков, входящих в компетенцию;
2 – не справляется с выполнением типовых профессиональных задач, проявляет отдельные навыки, входящие в компетенцию;
3 – выполняет типовые профессиональные задачи при консультационной поддержке: пороговый (критический) уровень готовности;
4 – самостоятельно выполняет типовые профессиональные задачи. Для решения нестандартных задач требуется консультационная помощь: пороговый (допустимый) уровень готовности;
5 – все профессиональные (типовые и нестандартные) профессиональные задачи выполняет самостоятельно: повышенный уровень готовности.
Бально-рейтинговая оценка по промежуточной аттестации проводимой в форме экзамена и (или) дифференцированного зачета выставляется в соответствии со следующей шкалой:
50–71 – «удовлетворительно»;
71–92 – «хорошо»;
92–100 – «отлично».
Далее приводятся критерии оценки результатов ответов. Например:
Оценка "ОТЛИЧНО" ставится обучающемуся, показавшему повышенный уровень готовности.
Оценка "ХОРОШО" ставится обучающемуся, показавшему пороговый (допустимый) уровень готовности.
Оценка "УДОВЛЕТВОРИТЕЛЬНО" ставится обучающемуся, показавшему пороговый (критический) уровень готовности.
Бально-рейтинговая оценка по промежуточной аттестации проводимой в форме зачета выставляется в соответствии со следующей шкалой:
51–100 – «зачтено».
Далее приводятся критерии оценки результатов ответов. Например:
Оценка "зачтено" ставится обучающемуся, минимально показавшему пороговый (критический) уровень готовности.