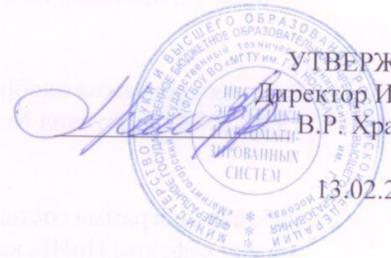




МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»



УТВЕРЖДАЮ

Директор ИЭиАС

В.Р. Храмшин

13.02.2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ОСНОВЫ БЕЗОПАСНОСТИ ЦИФРОВОГО ОБЩЕСТВА

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы

10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетика и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	1
Семестр	2

Магнитогорск
2024 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
09.02.2024, протокол № 4

Зав. кафедрой ИИЯ - И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
13.02.2024 г. протокол № 4

Председатель Храмшин В.Р. Храмшин

Рабочая программа составлена:

доцент кафедры ИиИБ, канд. техн. наук У.В. Кузьмина

Рецензент:

проректор по цифровизации, канд. техн. наук К.А. Рубан

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от _____ 20__ г. № ____
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью освоения дисциплины «Основы безопасности цифрового общества» является приобретение компетенций, позволяющих решать человеку поставленные задачи или достигать профессионального результата деятельности в условиях глобальной цифровизации общественных и бизнес-процессов.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Основы безопасности цифрового общества входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Информатика

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Основы Data инжиниринга

Основы информационной безопасности

Моделирование угроз информационной безопасности

Сети и системы передачи информации

Учебная - ознакомительная практика

Безопасность Интернета вещей

Проектная деятельность

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Основы безопасности цифрового общества» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
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	Оценивает роль информации в современном обществе
ОПК-1.2	Владеет современными информационными технологиями
ОПК-1.3	Применяет средства обеспечения информационной безопасности

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

- контактная работа – 51,95 акад. часов;
- аудиторная – 51 акад. часов;
- внеаудиторная – 0,95 акад. часов;
- самостоятельная работа – 56,05 акад. часов;
- в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Цифровое общество								
1.1 1. Индустрия 4.0: что такое четвертая промышленная революция? Понятие цифровых двойников и цифровых теней. 2. Понятие Интернета вещей (IoT).	2	4	4		4	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к тестированию	Тестирование	ОПК-1.1, ОПК-1.2, ОПК-1.3
1.2 1. Цифровые права граждан. 2. Понятия: Security-токен и utility-токен.		2	4		6	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к тестированию	Тестирование	ОПК-1.1, ОПК-1.2, ОПК-1.3
Итого по разделу		6	8		10			
2. Кибербезопасность как один из ключевых факторов устойчивого развития цифровой экономики								
2.1 1. Понятие кибербезопасности. Трансформация понятия информационная безопасность 2. Аналитика международного агентства по кибербезопасности и безопасности инфраструктуры (CISA) 3. Аналитика лаборатории Касперского 4. Кибербезопасность на	2	3	6		9	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к индивидуальному домашнему заданию(ИДЗ) и тестированию	ИДЗ, тестирование	ОПК-1.1, ОПК-1.2, ОПК-1.3

2.2 Кибергигиена: правила защиты личных персональных данных		3	7		9	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к ИДЗ и тестированию	ИДЗ, тестирование	ОПК-1.1, ОПК-1.2, ОПК-1.3
2.3 Социальная инженерия. Основные типы социальной инженерии и способы защиты		3	6		9	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к контрольной работе (КР)	КР	ОПК-1.1, ОПК-1.2, ОПК-1.3
2.4 Федеральный Закон «Об информации, информационных технологиях и защите информации». Понятие организационной защиты информации.		2	7		9	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к ИДЗ и тестированию	ИДЗ, тестирование	ОПК-1.1, ОПК-1.2, ОПК-1.3
Итого по разделу		11	26		36			
3. Зачет								
3.1 Подготовка к зачету	2				10,05	Подготовка к зачету; работа с ЭБС и нормативными документами; изучение материалов лекций	Зачет	ОПК-1.1, ОПК-1.2, ОПК-1.3
Итого по разделу					10,05			
Итого за семестр		17	34		56,05		зачёт	
Итого по дисциплине		17	34		56,05		зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

а) Вводная лекция – для целостного представления об учебном предмете и анализа учебно-методической литературы;

б) Обзорные лекции – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

в) Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя);

г) Семинар – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы;

д) Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму;

е) Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2) Раздельно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Раздельно-компетентностной технологии:

а) Кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе лично значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. Формы учебных занятий с использованием интерактивных технологий:

а) Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ

ошибок, совместный поиск вариантов рационального решения проблемы.

б) Методы ИТ – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: <https://doi.org/10.12737/1759-3>. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/1018901> (дата обращения: 27.04.2024)

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/422772> (дата обращения: 27.04.2024)

б) Дополнительная литература:

1. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: <https://new.znaniium.com/catalog/product/997105> (дата обращения: 27.04.2024)

2. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/414083> (дата обращения: 27.04.2024).

3. Баранкова И. И., Пермякова О.В. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/1858>. - ISBN 978-5-9967-1031-7. - Текст : электронный. – Макрообъект*.

***РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ**

1. Перейти по адресу электронной библиотеки МГТУ им. Г. И. Носова <https://host.megaprolib.net/MP0109/Web>.

2. Произвести авторизацию на портале (логин: Фамилия на русском языке, пароль: номер читательского билета)

3. Активизировать гиперссылку макрообъекта

в) Методические указания:

1. Методические указания по выполнению лабораторных работ (Приложение 1).

2. Методические указания по выполнению внеаудиторных самостоятельных работ (Приложение 2).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS Visual Studio 2017 Community Edition	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз безопасности информации ФСТЭК	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://host.megaprolib.net/MP0109/Web
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий East View Information Services, ООО	https://dlib.eastview.com/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- Мультимедийные средства хранения, передачи и представления информации.

Компьютерные классы:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для самостоятельной работы обучающихся:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

ПРИЛОЖЕНИЕ 1

По дисциплине «Основы безопасности цифрового общества» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные индивидуальные домашние задания (ИДЗ):

1. На основе статистики с интерактивной карты угроз на сайте Касперского за несколько лет спрогнозировать рост угроз на следующий год. Ответ оформить в виде гистограмм.
2. На основе статистики с международного агентства по кибербезопасности и безопасности инфраструктуры (CISA) за несколько лет спрогнозировать рост угроз на промышленные предприятия на следующий год. Ответ оформить в виде гистограмм.

Методические указания по выполнению лабораторных работ:

Лабораторные работы проводятся в компьютерных классах или специализированных лабораториях с целью получения практических умений для формирования и развития профессиональных навыков и соответствующих компетенций по дисциплине. При подготовке к выполнению заданий лабораторной работы используйте лекции, справочный материал программного обеспечения, рекомендованную литературу и цифровые образовательные ресурсы соответствующих методических материалов, размещенных в сети Интернет или локальной сети университета. Перед выполнением лабораторной работы необходимо получить свой вариант индивидуального задания у преподавателя. Прежде чем приступить к выполнению лабораторной работы, внимательно прочтите рекомендации к ее выполнению. Ознакомьтесь с перечнем рекомендуемой литературы, повторите теоретический материал, относящийся к теме работы. Ответьте на контрольные вопросы, выполните задания для самостоятельного выполнения. По результатам лабораторной работы предоставляется отчет. Отчет к лабораторным работам должен содержать:

- название лабораторной работы;
- цель и задачи работы;
- краткие теоретические сведения;
- задания по лабораторной работе;
- ход работы - описание последовательности действий при выполнении работы;
- выводы или результаты.

Результаты выполнения лабораторной работы могут быть представлены в электронном варианте или распечатанные. Результаты выполнения заданий лабораторной работы можно сохранить на образовательном портале в личном кабинете и использовать при подготовке к экзамену.

Защита работы и результаты оценивания.

Защита проводится в два этапа:

1. Демонстрируются результаты выполнения задания. В случае выполнения лабораторной работы, предусматривающей разработку программы, при помощи тестового примера доказывается, что результат, получаемый при выполнении программы, является правильным.

2. Для защиты работы студенту необходимо ответить на дополнительные вопросы преподавателя. Каждая лабораторная работа оценивается определенным количеством баллов исходя из 5-бальной системы оценок.

Лабораторная работа считается выполненной и защищенной, если выполнены все задания и даны правильные ответы преподавателю на заданные вопросы. Лабораторная работа считается выполненной и незащищенной, если выполнены все задания, но полученные результаты являются неверными или не даны правильные ответы преподавателю на заданные вопросы и ответы были не полные. Обучающемуся, не выполнившему в полном объеме все задания лабораторной работы, или пропустившему по уважительной причине лабораторную работу, необходимо выполнить ее самостоятельно в компьютерном классе или специализированной лаборатории, результаты выполненной работы сохранить на съемном носителе или на образовательном портале. Результаты предоставить в сроки, указанные преподавателем вместе с отчетом, демонстрацией

полученных результатов в компьютерном классе (или специализированной лаборатории) или предоставлением материалов на электронном образовательном ресурсе.

Правила по технике безопасности для обучающихся при проведении лабораторных работ:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ студенты допускаются только после прослушивания инструктажа по технике безопасности и противопожарным мерам.

2. Обучающийся должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах или специализированных лабораториях университета.

Примеры заданий:

Задание №1.

Разработать Personal Branding на английском языке в онлайн-сервисе. Ответ представить в виде ссылки на Personal Branding. Personal Branding должен содержать следующую информацию: фото, место работы/учебы, образование, увлечения/хобби, достижения, имеющийся опыт, навыки, ссылки на другие профили (соц сети, почта и т.д.).

Задание №2.

Разработать рекламу своей специальности в виде инфографики. В ней должна быть представлена информация о будущей профессии (получаемые компетенции и навыки), статистика роста потребности в таких специалистах, рост рынка НИИ "Сэйфнет" и короткая информация о вузе и кафедре.

Задание №3.

Разработать рекламу университета в виде инфографики. В ней должна быть представлена информация об университете, учебной, научной, общественной, спортивно и культурно-творческой деятельности университета.

Задание №4.

Разработать инфографику для объяснения что такое цифровое общество, кто к нему относится. Рассмотреть плюсы и минусы такого общества, его возможности и угрозы, ключевые даты/показатели/статистику/определения, связанные с цифровым обществом.

Задание №5.

Разработать инфографику по теме «Информационная безопасность в социальных сетях». Используя графические элементы и краткие текстовые блоки, изложить основные правила безопасного поведения в социальных сетях, опасности, которые могут угрожать пользователям, а также способы защиты от них.

Задание №6.

Разработать инфографику для объяснения обычному человеку для чего используются токены (цель токена и их применение), принцип их работы (технический уровень), базовые ценности и правовые статусы токенов. В инфо графике должны быть коротко приведены основные типы токенов и подробно разобран конкретный вариант токена (взять из списка предложенных по варианту).

Задание №7.

Разработать дорожную карту для разработки проекта умного дома, которая должен включать

в себя следующие пункты: определение понятия «Умный дом», определение пользователей умного дома - указать тех, кто будет постоянным/временным пользователем умного дома; планирование функционала умного дома в зависимости от того, кто будет использовать умный дом и потребностей пользователей, указать, какой именно функционал будет использоваться, например, приготовление пищи, охрана квартиры и т.д; чем именно планируется управлять умным домом, каких целей хотите добиться домашней автоматизацией; как планируется управлять умным домом (удаленно управление всеми устройствами, частью устройств, управление с телефона, голосом и т.д.)
Разработать схему состава, а также планировку квартиры.

Задание №8.

В онлайн редакторе построить диаграмму Исикавы для решения вашей насущной проблемы. Темы выдаются преподавателем.

Задание №9.

Написать квест на языке C# для определения цифровой грамотности пользователя. В процессе выполнения квеста пользователь должен формировать в графическом виде карту своей цифровой грамотности. (в качестве ответов на вопросы и задачи квеста пользователь должен получать анимированную реакцию от приложения).

Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Компетенция / Индикатор достижения компетенции	Оценочные средства
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 Оценивает роль информации в современном обществе	<p>Вопросы для зачета:</p> <ol style="list-style-type: none"> 1. Понятия информация, информационные технологии и защита информации. 2. Угрозы информационной безопасности для личных персональных данных. 3. Трансформация понятия информационная безопасность. 4. Понятие цифровые права гражданина РФ. 5. Понятие кибергиены. <p>Роль кибербезопасности в развитии цифровой экономики.</p> <ol style="list-style-type: none"> 6. Понятия: Security-токен и utility-токен. 7. Основные типы социальной инженерии и способы защиты от них. 8. Организационные требования защиты информации. 9. Каким наиболее важным аспектам кибербезопасности уделяется должное внимание со стороны государства, а каким необходимо уделять больше внимания.
ОПК-1.2 Владеет современными информационными технологиями	<ol style="list-style-type: none"> 1. Найти перечень основных нормативно-правовых документов по кибербезопасности и провести их анализ. 2. Найти перечень основных нормативно-правовых документов по цифровизации и провести их анализ. 3. Провести майндмэппинг и командный мозговой штурм с использованием MindMeister на темы: <ol style="list-style-type: none"> 1. Угрозы безопасности личности, осуществляемые через цифровую среду. 2. Угрозы национальной безопасности, осуществляемые через цифровую среду. 3. Принципы ведения информационных войн.
ОПК-1.3 Применяет средства обеспечения информационной безопасности	<ol style="list-style-type: none"> 1. На основе проведенного анализа нормативно-правовых документов в области цифровизации найти слабые места, требующие внимания. 2. Написать приложение на языке C# для определения уровня цифровой грамотности респондента. 3. На основе статистики с интерактивной карты угроз на сайте Касперского за несколько лет спрогнозировать рост угроз на следующий год. Ответ оформить в виде гистограмм. 4. На основе статистики с международного агентства по кибербезопасности и безопасности инфраструктуры (CISA) за несколько лет спрогнозировать рост угроз на промышленные предприятия на следующий год. Ответ оформить в виде гистограмм.

Критерии оценки

- на оценку **«зачтено»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;
- на оценку **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

ПРИЛОЖЕНИЕ 3

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

- 1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
 - a) предоставляемыми преподавателем на лекционных занятиях;
 - b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
 - c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
- 2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
- 3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
- 4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы со студентами группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами

информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторские контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.