РАБОЧАЯ ПРОГРАММА

модуля(курса)

«Актуальные вопросы информационной безопасности и кибербезопасности»

1. АННОТАЦИЯ

Дисциплина «Актуальные вопросы информационной безопасности и кибербезопасности» включает учебный материал, способствующий формированию у слушателей теоретических знаний и практических навыков, связанных с понятиями информационной безопасности и кибебезопасности, рисков и угроз в сфере защиты информации.

Цель дисциплины - обобщение и систематизация современных знаний и формирование практических навыков информационной безопасности и кибебезопасности, противодействия информационным угрозам. Дисциплина рассматривается, как один из курсов программы профессиональной переподготовки «Искусственный интеллект в журналистике и массовых коммуникациях».

2. СОДЕРЖАНИЕ

№ п/п	Наименование модуля, разделов и тем	Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, практических занятий (семинаров), самостоятельной работы с указанием кол-ва часов, используемых образовательных технологий и рекомендуемой литературы
1.	*2.*	*3.*
1	**Тема 1. Основы кибербезопасности**	**Курс от Лаборатории Касперского.** **Введение в курс по основам кибербезопасности.** **Анализ вредоносных программ.** **Безопасность приложений.** **Безопасность сетей.** **Цифровая криминалистика и реагирование на инциденты.**
2	Тема 2. Угрозы информационной безопасности	Угрозы информационной безопасности. Информационные войны. Способы противостояния угрозам информационного воздействия. Защита информационной безопасности. (1 час)
3	Тема 3. Основы кибербезопасности. Обзор угроз в цифровом пространстве.	Понятие «кибербезопаность». История вопроса. Сферы кибербезопасности. Виды киберугроз. Мероприятия по защите информации от вредоносных программ. Вредоносные программы (вирусы) и их классификация (1 час)
4	Тема 4. Методы безопасной работы в ИКС «Интернет».	Основные правила поведения при взаимодействии через интернет. Идентификация, аутентификация пользователей. Классификация методов идентификации пользователей. Уязвимые места информационных систем. Мероприятия по защите информации от несанкционированного доступа. (2 часа)
	Практические занятия (семинары)	Практические задания по блоку от Лаборатории Касперского (4 часа)
		Защита персональных и рабочих устройств. (2 часа)
		Разбор кейсов по кибербезопасности: зарубежный и российский опыт (2 часа)
	Самостоятельная работа	Изучение рекомендованной литературы, самостоятельный анализ кейсов (12 часов)
	Зачет	Собеседование (2 час)

3. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

(формы аттестации, оценочные и методические материалы)

Промежуточная аттестация представляет собой собеседование, которое проводится по результатам практических занятий (семинаров).

1. Для сдачи зачета слушатель должен подготовить ответы на следующие вопросы курса:

1. Актуальность и основные задачи защиты информации. Основные понятия информационной безопасности.
2. Основные угрозы безопасности данных и их классификация.
3. Идентификация, аутентификация пользователей. Классификация методов идентификации пользователе
4. Уязвимые места информационных систем.
5. Основные методы защиты данных и их классификация.
6. Защита информации в системах управления базами данных.
7. Основные средства защиты данных и их классификация.
8. Формальные средства защиты информации.
9. Программно-технический аспект информационной безопасности.
10. Неформальные средства защиты информации.
11. Организационный аспект информационной безопасности.
12. Мероприятия по защите информации от несанкционированного доступа.
13. Управленческий аспект информационной безопасности.
14. Законодательный аспект информационной безопасности.
15. Мероприятия по защите информации от вредоносных программ.
16. Вредоносные программы (вирусы) и их классификация.

№ п/п	Наименование процедуры	Основные показатели оценки	Формы и методы контроля и оценки
1	Промежуточный контроль. Актуальные вопросы информационной безопасности и кибербезопасности	Владеет терминологией и теорией верификации информации, демонстрирует практические навыки проверки сообщений СМИ и социальных медиа	Собеседование

Критерии оценки

№ п/п	Наименование процедуры	Основные показатели оценки		Формы и методы контроля и оценки
	Промежуточный контроль. Актуальные вопросы информационной безопасности и кибербезопасности	Зачтено	В целом хорошая подготовка с заметными ошибками или недочетами. Слушатель дает полный ответ на все теоретические вопросы билета, но имеются неточности в определениях понятий, процессов и т.п. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы экзаменатора. Слушатель работал на практических занятиях.	Собеседование
		Не зачтено	Подготовка недостаточная и требует дополнительного изучения материала. Слушатель дает ошибочные ответы, как на теоретические вопросы билета, так и на наводящие и дополнительные вопросы экзаменатора. Слушатель пропустил большую часть практических занятий.	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МОДУЛЯ

4.1 Учебно-методическое и информационное обеспечение программы:

Для эффективного освоения компетенций, формируемых учебной дисциплиной важно использование в учебном процессе активных и интерактивных форм проведения занятий.

Изучение учебной дисциплины предполагает наличие аудиторной и самостоятельной видов работ слушателей. В ходе практических занятий рассматриваются практические задачи из практики с целью наиболее полного овладения умениями и навыками.

Лекции по учебной дисциплине призваны формировать знания, предусмотренные учебной программой, и включают теоретическую базу статистики, на базе которой строятся прикладные аспекты.

Наряду с проработкой основной литературы (глав базового учебника) предусмотрено самостоятельное чтение дополнительной литературы (статей и других научных публикаций).

Практические занятия в малых группах и самостоятельная внеаудиторная работа направлены на выработку навыков статистического анализа данных.

Для достижения поставленных целей преподавания дисциплины реализуются следующие средства, способы и организационные мероприятия:

- изучение теоретического материала дисциплины на лекции с использованием компьютерных технологий;
- самостоятельное изучение теоретического материала дисциплины с использованием Internet-ресурсов, информационных баз, электронных библиотек, методических разработок, специальной и научной литературы;
- закрепление теоретического материала при проведении практических занятий с использованием учебного и научного оборудования, выполнения проблемно-ориентированных, поисковых, творческих заданий.

Самостоятельная работа слушателей включает:

1. Изучение учебной литературы по курсу.
2. Решение практических ситуаций и задач
3. Изучение источников управленческой информации
4. Работу с ресурсами Интернет
5. Решение практических ситуаций в виде творческих заданий

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

4.2. Содержание комплекта учебно-методических материалов.

- Осавелюк Е. А. Информационная безопасность государства и общества в контексте деятельности СМИ : монография / Осавелюк Е. А. - 3-е изд., стер. - Санкт-Петербург : Лань, 2023.
- - 92 с. - Книга из коллекции Лань - Журналистика и медиабизнес. - ISBN 978-5-507-47137-9., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=883344&idb=0.

- Белоус А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами : монография / Белоус А.И.; Солодуха В.А. - Москва : Инфра-Инженерия, 2020. - 692 с. - ISBN 978- 5-9729-0486-0., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=735678&idb=0.

- Басыня Е. А. Сетевая информационная безопасность : учебник / Басыня Е. А. - Москва : НИЯУ

МИФИ, 2023. - 224 с. - Книга из коллекции НИЯУ МИФИ - Информатика. - ISBN 978-5-7262-2949-2., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=884189&idb=0.

- Чернова Е. В. Информационная безопасность человека : учебное пособие / Е. В. Чернова. - 3-е изд. ; пер. и доп. - Москва : Юрайт, 2023. - 327 с. - (Высшее образование). - ISBN 978-5-534-16772-
- Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=871518&idb=0.
- Джафарли В.Ф. Криминология кибербезопасности. Т. 1. Криминологическая кибербезопасность: теоретические, правовые и технологические основы : монография / ДжафарлиВ.Ф. - Москва : Проспект, 2021. - 288 с. - ISBN 978-5-392-35118-3., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=839152&idb=0.

в) программное обеспечение и Интернет-ресурсы

1. Операционная система Microsoft Windows
2. Пакет прикладных программ Microsoft Office

Лекции и практические занятия проводятся с использованием возможностей мультимедийного класса. Использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций).

4.3. Материально-технические условия реализации программы:

1.

Материально-техническая база

№ п.п.	Наименование модуля (тем, разделов)	Материально-технические условия для реализации программ (наличие лабораторий, производственных участков и т.п. по профилю программы профессиональной переподготовки)
1.	Тема 1. Основы кибербезопасности.	Реализация дисциплины предполагает наличие: - аудиторий для лекционных и практических занятий с необходимым мультимедийным оборудованием; - операционная система MicrosoftWindows, пакет прикладных программ MicrosoftOffice. В ходе проведения занятий рекомендуется использовать компьютерные иллюстрации для поддержки различных видов занятий, подготовленные с использованием MicrosoftOffice или других средств визуализации материала.
2.	Тема 2. Угрозы информационной безопасности	
	Тема 3. Основы кибербезопасности. Обзор угроз в цифровом пространстве.	
	Тема 4. Методы безопасной работы в ИКС «Интернет».	
3.	Практические занятия (семинары)	