

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**федеральное государственное автономное
образовательное учреждение высшего образования_
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»**

Институт филологии и журналистики

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Рабочая программа дисциплины

Проблемы безопасности информационной среды

Уровень высшего образования

Магистратура

Направление подготовки / специальность

42.04.02 - Журналистика

Направленность образовательной программы

Международная журналистика

Форма обучения

заочная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.ДВ.02.03 Проблемы безопасности информационной среды относится к части, формируемой участниками образовательных отношений образовательной программы.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции		Наименование оценочного средства	
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	Для текущего контроля успеваемости	Для промежуточной аттестации
ПКР-11: Способен использовать методы разработки и продвижения веб-сайтов, приемы художественно-технического оформления Интернет-ресурсов;	ПКР-11.1: ПКР-11.1. Использует методы разработки веб-сайтов, приемы художественно-технического оформления Интернет-ресурсов ПКР-11.2: ПКР-11.2. Реализует комплекс мер для поднятия позиций сайта в результатах выдачи поисковых систем по определенным запросам пользователей с целью продвижения сайта	ПКР-11.1: Знать методы разработки веб-сайтов, приемы художественно-технического оформления Интернет-ресурсов; Уметь применять в практической деятельности методы разработки веб-сайтов, приемы художественно-технического оформления Интернет-ресурсов; Владеть практическим навыками применения в практической деятельности методов разработки веб-сайтов, приемов художественно-технического оформления Интернет-ресурсов ПКР-11.2: Знать технологии, используемые для поднятия позиций сайта в результатах выдачи поисковых систем по определенным запросам пользователей с целью продвижения сайта; Уметь использовать в практической деятельности технологии поднятия позиций сайта в результатах выдачи поисковых систем по	Кейс-задание	Зачёт: Контрольные вопросы

		<p>определенным запросам пользователей с целью продвижения сайта;</p> <p>Владеть навыками реализации комплекс мер для поднятия позиций сайта в результатах выдачи поисковых систем по определенным запросам пользователей с целью продвижения сайта;</p>		
<p>ПКР-12: Способен использовать в профессиональной деятельности сервисы редакционной аналитики, анализировать и применять их данные для коррекции отдельных публикаций и работы издания/рубрики, оценивать структуру трафика и его основные источники.</p>	<p>ПКР-12.1: ПКР-12.1. Применяет в профессиональной деятельности сервисы редакционной аналитики</p> <p>ПКР-12.2: ПКР-12.2. Владеет методами коррекции отдельных публикаций и работы издания/рубрики, оценивает структуру трафика и его основные источники</p>	<p>ПКР-12.1:</p> <p>Знать основные сервисы редакционной аналитики;</p> <p>Уметь применять в профессиональной деятельности сервисы редакционной аналитики;</p> <p>Владеть практическими навыками применения в профессиональной деятельности сервисы редакционной аналитики;</p> <p>ПКР-12.2:</p> <p>Знать методики коррекции отдельных публикаций и работы издания/рубрики, оценки структуры трафика и его основных источников;</p> <p>Уметь применять в профессиональной деятельности методики коррекции отдельных публикаций и работы издания/рубрики, оценки структуры трафика и его основных источников;</p> <p>Владеть практическими навыками коррекции отдельных публикаций и работы издания/рубрики, оценки структуры трафика и его основных источников;</p>	<p>Кейс-задание</p>	<p>Зачёт:</p> <p>Контрольные вопросы</p>
<p>ПКР-13: Способен устанавливать и поддерживать контакты с внешней средой</p>	<p>ПКР-13.1: ПКР-13.1. Устанавливает и поддерживает обратную связь с аудиторией (прием редакционной почты,</p>	<p>ПКР-13.1:</p> <p>Знать основные технологии взаимодействия с аудиторией;</p>	<p>Кейс-задание</p>	<p>Зачёт:</p> <p>Контрольные вопросы</p>

<p>организации с учетом специфики разных видов СМИ;</p>	<p>ответы на письма, звонки, комментарии на сайте СМИ и страницах в социальных сетях) ПКР-13.2: ПКР-13.2. Использует результаты обработки данных, полученных от аудитории, в целях развития индивидуального и (или) коллективного проекта в сфере журналистики</p>	<p>Уметь устанавливать и поддерживать обратную связь с аудиторией (прием редакционной почты, ответы на письма, звонки, комментарии на сайте СМИ и страницах в социальных сетях);</p> <p>Владеть практическими навыками работы с аудиторией, установления и поддержания обратной связи (прием редакционной почты, ответы на письма, звонки, комментарии на сайте СМИ и страницах в социальных сетях);</p> <p>ПКР-13.2: Знать технологии и методики обработки данных, полученных от аудитории, в целях развития индивидуального и (или) коллективного проекта в сфере журналистики;</p> <p>Уметь использовать в практической деятельности результаты обработки данных, полученных от аудитории, в целях развития индивидуального и (или) коллективного проекта в сфере журналистики;</p> <p>Владеть практическими навыками обработки данных, полученных от аудитории, и их использования в целях развития индивидуального и (или) коллективного проекта в сфере журналистики;</p>		
<p>ПКР-2: Способен анализировать проекты, предлагаемые авторами; выявлять слабые и сильные стороны, соответствие проектов</p>	<p>ПКР-2.1: ПКР-2.1. Оценивает авторские идеи с точки зрения соответствия формату, целевой аудитории и политике СМИ ПКР-2.2: ПКР-2.2. Владеет методами анализа и коррекции концепции</p>	<p>ПКР-2.1: Знать методику оценки соответствия авторских предложений соответствия формату, целевой аудитории и политике СМИ; Уметь применять в практической деятельности</p>	<p>Опрос</p>	<p>Зачёт: Контрольные вопросы</p>

информационной политике СМИ	индивидуального и (или) коллективного проекта в сфере журналистики	<p>методики оценки соответствия авторских предложений соответствия формату, целевой аудитории и политике СМИ;</p> <p>Владеть навыками практической деятельности в оценке соответствия авторских предложений соответствия формату, целевой аудитории и политике СМИ</p> <p>ПКР-2.2:</p> <p>Знать методы анализа и коррекции концепции индивидуального и (или) коллективного проекта в сфере журналистики;</p> <p>Уметь применять в профессиональной деятельности методы анализа и коррекции концепции индивидуального и (или) коллективного проекта в сфере журналистики;</p> <p>Владеть практическими навыками использования методов анализа и коррекции концепции индивидуального и (или) коллективного проекта в сфере журналистики;</p>		
ПКР-7: Способен осуществлять авторскую деятельность любого характера и уровня и сложности с учетом специфики разных типов СМИ	<p>ПКР-7.1: ПКР-7.1. Контролирует достоверность и полноту полученной информации, систематизирует факты и мнения</p> <p>ПКР-7.2: ПКР-7.2. Разрабатывает оригинальные творческие решения</p> <p>ПКР-7.3: ПКР-7.3. Готовит к публикации журналистский текст (или) продукт любого уровня сложности с учетом требований конкретной редакции СМИ или другого медиа</p>	<p>ПКР-7.1:</p> <p>Знать методики проверки достоверности и полноты полученной информации;</p> <p>Уметь контролировать достоверность и полноту полученной информации, систематизирует факты и мнения;</p> <p>Владеть практическими навыками участия в процессе контроля достоверности и полноты полученной информации, систематизации фактов и мнений;</p> <p>ПКР-7.2:</p>	Кейс-задание	Зачёт: Контрольные вопросы

		<p>Знать технологии разработки оригинальных творческих решений в процессе осуществления авторской деятельности;</p> <p>Уметь применять технологии разработки оригинальных творческих решений в процессе осуществления авторской деятельности;</p> <p>Владеть практическими навыками разработки оригинальных творческих решений в процессе осуществления авторской деятельности;</p> <p>ПКР-7.3: Знать методы подготовки к публикации журналистского текста (или) продукта любого уровня сложности с учетом требований конкретной редакции СМИ или другого медиа;</p> <p>Уметь применять в практической деятельности методы подготовки к публикации журналистского текста (или) продукта любого уровня сложности с учетом требований конкретной редакции СМИ или другого медиа;</p> <p>Владеть практическими навыками подготовки журналистского текста (или) продукта любого уровня сложности с учетом требований конкретной редакции СМИ или другого медиа;</p>		
--	--	--	--	--

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	заочная
--	---------

Общая трудоемкость, з.е.	2
Часов по учебному плану	72
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	0
- занятия семинарского типа (практические занятия / лабораторные работы)	6
- КСР	1
самостоятельная работа	61
Промежуточная аттестация	4
	Зачёт

3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	Всего (часы)	в том числе			
		Контактная работа (работа во взаимодействии с преподавателем), часы из них			Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа (практические занятия/лабораторные работы), часы	Всего	
	з Ф о	з Ф о	з Ф о	з Ф о	з Ф о
Тема 1. История вопроса. Термин «информационная безопасность»	11		2	2	9
Тема 2. Информационный ресурс - понятие.	9			0	9
Тема 3. ФЕНОМЕН ИНТЕРНЕТА	8			0	8
Тема 4. Манипулятивные приемы	7			0	7
Тема 5. Угрозы информационной безопасности	7			0	7
Тема 6. Кибербезопасность как инструмент информационной безопасности	9		2	2	7
Тема 7. Информационные войны	9		2	2	7
Тема 8. Способы противостояния угрозам информационного воздействия.	7			0	7
Аттестация	4				
КСР	1				1
Итого	72	0	6	7	61

Содержание разделов и тем дисциплины

Введение. История вопроса. Термин

«информационная безопасность» (впервые введен в 1992 году взамен цензуры). Две

доктрины МИБ (2000 и 2016гг)
Информационный ресурс - понятие.
Информационное
общество - признаки. Структурно- функциональная роль современных СМИ.
Феномен
современного телевидения
(«Декаданс медиа»,
«Ритуал и мифы медиа»)
ФЕНОМЕН
ИНТЕРНЕТА
Манипулятивные
приемы и приемы

актуализации смыслов
Угрозы информационной
безопасности
Информационные войны. Терроризм 21 века. Разновидность информационного оружия как
принципиально
нового класса оружия («гуманное оружие»)
Способы противостояния угрозам
информационного воздействия.
Доктрина МИБ-2016

Практические занятия /лабораторные работы организуются, в том числе, в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

На проведение практических занятий / лабораторных работ в форме практической подготовки отводится: заочная форма обучения - 4 ч.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

В рамках самостоятельной работы студентов предполагается использование УМП
«Психология массовой коммуникации», размещенного в ФЭОР ННГУ
<http://www.unn.ru/books/resources.html>. Дата издания 18.03.2013.

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:

5.1.1 Типовые задания (оценочное средство - Кейс-задание) для оценки сформированности компетенции ПКР-11:

Иванов осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Сбербанка». Рассылка представляла собой электронное письмо с сообщением о переводе 50 000 рублей на личный счет клиента и содержала просьбу зайти в систему Интернет-банкинга «Сбербанк-Online» для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный Ивановым, и очень похожий на стартовый экран «Сбербанк-Online». Десять человек ввели реквизиты кредитной карты и CVV-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, Иванов совершил завладение денежными средствами Петрова и Сидорова, находящимися в Сбербанке, в сумме 15 и 20 тысяч рублей соответственно. Квалифицируйте осуществлённую Ивановым атаку. Дайте рекомендации по поведению в подобных ситуациях.

5.1.2 Типовые задания (оценочное средство - Кейс-задание) для оценки сформированности компетенции ПКР-12:

Некий пользователь ПК читает ленту новостей ВКонтакте. В комментариях он видит сообщение о быстром заработке. Пользователя заинтересовало данное предложение, и он перешёл по этой ссылке. Там появилось окно ввода логина и пароля от ВКонтакте. По неопытности и незнанию пользователь вводит свои данные, после этого его аккаунт из соцсети «крадут» злоумышленники. Какие были совершены ошибки? Как можно было бы избежать этой ситуации?

5.1.3 Типовые задания (оценочное средство - Кейс-задание) для оценки сформированности компетенции ПКР-13:

Иванов осуществлял рассылку подложных электронных писем с целью завладения персональной информацией клиентов «Сбербанка». Рассылка представляла собой электронное письмо с сообщением о переводе 50 000 рублей на личный счет клиента и содержала просьбу зайти в систему Интернет-банкинга «Сбербанк-Online» для подтверждения перевода. В случае следования по указанной ссылке происходило попадание на сайт, созданный Ивановым, и очень похожий на стартовый экран «Сбербанк-Online». Десять человек ввели реквизиты кредитной карты и CVV-код для того, чтобы войти в систему. Воспользовавшись полученной таким образом информацией, Иванов совершил завладение денежными средствами Петрова и Сидорова, находящимися в Сбербанке, в сумме 15 и 20 тысяч рублей соответственно. Квалифицируйте осуществлённую Ивановым атаку. Дайте рекомендации по поведению в подобных ситуациях.

5.1.4 Типовые задания (оценочное средство - Кейс-задание) для оценки сформированности компетенции ПКР-7:

Некий пользователь ПК читает ленту новостей ВКонтакте. В комментариях он видит сообщение о быстром заработке. Пользователя заинтересовало данное предложение, и он перешёл по этой ссылке. Там появилось окно ввода логина и пароля от ВКонтакте. По неопытности и незнанию пользователь вводит свои данные, после этого его аккаунт из соцсети «крадут» злоумышленники. Какие были совершены ошибки? Как можно было бы избежать этой ситуации?

Критерии оценивания (оценочное средство - Кейс-задание)

Оценка	Критерии оценивания
зачтено	Участвует в решении задания, демонстрирует навыки работы в команде
не зачтено	Не участвует в решении задания, демонстрирует навыки работы в команде

5.1.5 Типовые задания (оценочное средство - Опрос) для оценки сформированности компетенции ПКР-2:

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 пользователей.
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.

Критерии оценивания (оценочное средство - Опрос)

Оценка	Критерии оценивания
зачтено	Отвечает на вопросы преподавателя, демонстрирует знания
не зачтено	Не отвечает на вопросы преподавателя, не демонстрирует знания

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации**Шкала оценивания сформированности компетенций**

Уровень сформированности компетенций (индикатора достижения компетенций)	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущено много негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Ошибок нет.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений. Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продemonстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие базовых навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продemonстрирован творческий подход к решению нестандартных задач

Шкала оценивания при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне выше предусмотренного программой

	отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично».
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо».
	удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

5.3.1 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПКР-11

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 пользователей.
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.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПКР-12

Вопрос

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 пользователей.

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.

5.3.3 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПКР-13

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 пользователей.

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.

5.3.4 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПКР-2

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 пользователей.

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.

5.3.5 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПКР-7

Вопрос

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 пользователей.

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.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
зачтено	Отвечает на вопросы преподавателя, демонстрирует знания
не зачтено	Не отвечает на вопросы преподавателя, не демонстрирует знания

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

- 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>.

Дополнительная литература:

- 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>.

2. 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 978-5-534-16772-6. - Текст : электронный // ЭБС "Юрайт"., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=871518&idb=0>.
3. Джафарли В.Ф. Криминология кибербезопасности. Т. 1. Криминологическая кибербезопасность: теоретические, правовые и технологические основы : монография / Джафарли В.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>.

Программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины):

1. Доктрина информационной безопасности Российской Федерации 2001 г. // Российская газета. URL: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>
2. Доктрина информационной безопасности Российской Федерации 2016 г. // URL: <http://publication.pravo.gov.ru/Document/View/0001201612060002>
3. Федеральный закон от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации // Российская газета. URL: <https://rg.ru/2006/07/29/informacia-dok.html>.
4. ГОСТ Р. Защита информации. Основные требования и определения.
Программный комплекс Microsoft Office.

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), техническими средствами обучения, компьютерами.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки/специальности 42.04.02 - Журналистика.

Автор(ы): Макарова Людмила Сергеевна, кандидат филологических наук, доцент
Болдина Ксения Александровна, кандидат политических наук.

Заведующий кафедрой: Савинова Ольга Николаевна, доктор политических наук.

Программа одобрена на заседании методической комиссии от 12.01.2024, протокол № 12.