

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Исторический факультет
Кафедра международных отношений и внешней политики



УТВЕРЖДАЮ
проректор

П.А. Машаров

«29» марта 2024 г.

МП

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»**

У крупненная группа направлений
подготовки
Программа высшего образования
Направление подготовки

41.00.00 Политические науки и
регионоведение
Программа бакалавриата
41.03.05 Международные отношения

Профиль подготовки

Международные отношения

Квалификация
Форма обучения

Бакалавр
Очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «**Основы информационной безопасности в профессиональной деятельности**» для обучающихся по направлению подготовки 41.03.05 Международные отношения (Профиль: Международные отношения), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 41.03.05 Международные отношения, утвержденного приказом Министерства образования и науки Российской Федерации от 15 июня 2017 г. № 555 (с изм. и доп.); Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:

доцент кафедры международных отношений и
внешней политики,
канд. истор. наук, доцент



Л.Ю. Медовкина

Рабочая программа одобрена на заседании кафедры международных отношений и
внешней политики.

Протокол от 26.03.2024 г. № 10

Заведующий кафедрой



А.И. Минаев

СОГЛАСОВАНО:

Декан исторического факультета



А.И. Минаев

28.03.2024 г.

Учебно-методическая комиссия исторического факультета

Протокол от 27.03.2024 г. № 7

Председатель



Е.В. Кузнецова

Руководитель основной профессиональной
образовательной программы,

д-р ист. наук, проф.

26.03.2024 г.



А.И. Минаев

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

дисциплины программы бакалавриата: Правоведение, Информационно-аналитическая деятельность в международных отношениях, Государственное право России и зарубежных стран;

дисциплины программы бакалавриата: Информационные войны в современном мире, Международная информация.

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

дисциплины программы бакалавриата: Геополитика, Современные международные отношения, Ведение переговоров, Производственная практика: научно-исследовательская работа по теме выпускной квалификационной работы.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1.Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	41.03.05 Международные отношения (Профиль: Международные отношения)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.3.2 Основы информационной безопасности в профессиональной деятельности
Часть образовательной программы	Вариативная часть: выбор обучающегося
Количество зачетных единиц / всего часов	2 / 72

2.2.Распределение часов по периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	2	3	17	17	–	38	72	зачет

3. ЦЕЛИ ДИСЦИПЛИНЫ

Формирование у обучающихся понимания основ информационной безопасности, практических навыков организации работ по обеспечению информационной безопасности на предприятиях и организациях

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1. Компетенции

ПК-3. Способен работать с материалами средств массовой информации.

4.2. Индикаторы компетенций

ПК-3.1. Составляет обзоры прессы по заданным международным темам, находит, собирает и первично обобщает фактический материал, делая обоснованные выводы.

ПК-3.3. Владеет навыками публичных выступлений, как перед отечественной, так и зарубежной аудиторией

4.3. Результаты обучения

ПК-3.1.1. Знает особенности освящения информационных войн СМИ.

ПК-3.1.2. Умеет самостоятельно оценивать и анализировать различные точки зрения в процессе изучения информационного общества.

ПК-3.1.3. Умеет собирать и обрабатывать данные об информационных потоках и информационных войнах.

ПК-3.3.1. Способен публично выступать об информационной безопасности, выявляя специфику информационных войн на современном этапе и их влияния на политический процесс.

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Актуальность проблемы информационной безопасности.	1.1. Понятие информационной безопасности. 1.2. Проблема информационной безопасности общества. 1.3. Основные положения государственной политики РФ в информационной сфере. 1.4. Этапы развития информационных технологий, методов и средств обеспечения информационной безопасности. 1.5. Проблемы и актуальность обеспечения информационной безопасности.
2. Основные термины и определения категории «безопасность», виды безопасности.	2.1. Понятие, источники, формы, виды, свойства информации. 2.2. Национальная безопасность, информационная безопасность, цель и решаемые задачи. 2.3. Жизненно важные интересы личности, общества, государства в сфере информационной безопасности. 2.4. Объекты защиты. 4.5. Опасность, ущерб, источники угроз, угроза информационной безопасности.
3. Национальная безопасность Российской Федерации. Место информационной безопасности в системе национальной безопасности Российской Федерации.	3.1. Задачи информационной безопасности общества. 3.2. Комплексное обеспечение информационной безопасности РФ. 3.3. Ценности и модели развития глобальной конкуренции. 3.4. Глобальное информационное противоборство. 3.5. Значение информационной безопасности в обеспечении национальной безопасности Российской Федерации.

	3.6. Положения основных нормативных документов Российской Федерации в области национальной, и информационной безопасности.
4. Государственная система обеспечения информационной безопасности Российской Федерации.	4.1. Основные элементы системы государственной информационной безопасности Российской Федерации. 4.2. Законодательные органы Российской Федерации. 4.3. Значение и роль судебных органов Российской Федерации в обеспечении информационной безопасности и защиты информации. 4.4. Органы исполнительной власти Российской Федерации в проведении единой технической политики в области информационной безопасности и защиты информации.
5. Законодательные акты Российской Федерации в области информационной безопасности, государственная тайна, конфиденциальная информация.	5.1. Основные нормативные акты Российской Федерации, назначение и основные положения. 5.2. Классификация информации по своей доступности и распространенности в соответствии с Российским законодательством, правовой институт тайн в Российской Федерации. 5.3. Государственная тайна, содержание, основные понятия. 5.4. Конфиденциальная информация, основные понятия, виды конфиденциальной информации. 5.5. Нормативно-правовые и руководящие документы органов исполнительной власти РФ, назначение и основные положения в сфере информационной безопасности и защиты информации.
6. Информация, как объект защиты, источники угроз, угрозы информационной безопасности.	6.1. Понимание информации как объекта защиты, юридические свойства информации. 6.2. Информационное право как юридическая отрасль права, цели, задачи, принципы информационного права. 6.3. Правовое регулирование субъектов по отношению к объектам интеллектуальной собственности. 6.4. Каналы утечки, методы и способы несанкционированного доступа к защищаемой информации, объектам защиты. 6.5. Источники угроз воздействия на объект защиты. 6.6. Угрозы, влияющие на состояние информационной безопасности, методы и способы реализации угроз.
7. Правовой уровень обеспечения информационной безопасности.	7.1. Назначение, цели и задачи правового уровня обеспечения информационной безопасности. 7.2. Международные и российские стандарты в области информационной безопасности. 7.3. Нормативно-правовые и руководящие документы ФСТЭК РФ по защите информации от несанкционированного доступа (НСД) к информационным системам.
8. Административный уровень, политика информационной безопасности предприятия.	8.1. Политика информационной безопасности, как концептуальный документ по обеспечению информационной безопасности на предприятии состав и содержание политики информационной безопасности. 8.2. Состав и содержание программы информационной

	безопасности. 8.3. Анализ и оценка рисков, управление рисками по исключению реализации угроз информационной безопасности. 8.4. Цели, задачи и основные мероприятия по построению системы обеспечения информационной безопасности на предприятии.
9. Процедурный уровень информационной безопасности.	9.1. Основные классы мер процедурного уровня информационной безопасности. 9.2. Управление персоналом, назначение, основные положения. 9.3. Физическая защита, назначение, основные положения. 9.4. Поддержание работоспособности информационных систем. 9.5. Реагирование на нарушения режима безопасности. 9.6. Планирование восстановительных работ системы обработки и защиты информации.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 2, семестр – 3

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
1. Актуальность проблемы информационной безопасности.	1	1	—	6	8
2. Основные термины и определения категории «безопасность», виды безопасности.	2	2	—	4	8
3. Национальная безопасность Российской Федерации. Место информационной безопасности в системе национальной безопасности Российской Федерации.	2	2	—	4	8
4. Государственная система обеспечения информационной безопасности Российской Федерации.	2	2	—	4	8
5. Законодательные акты Российской Федерации в области информационной безопасности, государственная тайна, конфиденциальная информация.	2	2	—	4	8
6. Информация, как объект защиты, источники угроз, угрозы информационной безопасности.	2	2	—	4	8
7. Правовой уровень обеспечения информационной безопасности.	2	2	—	4	8
8. Административный уровень, политика информационной безопасности предприятия.	2	2	—	4	8
9. Процедурный уровень информационной безопасности.	2	2	—	4	8
ИТОГО ЗА КУРС	17	17	—	38	72

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

Раздел 1

1. Перечислите этапы развития информационных технологий и методов обеспечения безопасности информации.
2. Назовите проблемы обеспечения информационной безопасности на современном этапе развития общества.
3. Определите значение информационной безопасности в развитии общества. 4. Назовите основные положения по обеспечению информационной безопасности на современном этапе.
4. Назовите источники, формы, виды, свойства информации.
5. Перечислите цели и решаемые задачи в обеспечении национальной безопасности.
6. Дайте определение информационной безопасности, цель и решаемые задачи.
7. Назовите жизненно важные интересы личности, общества, государства в сфере информационной безопасности.
8. Объекты защиты в области информационной безопасности.
9. Виды источников угроз информационной безопасности.
10. Виды угроз информационной безопасности.
11. Назовите ценности и модели развития глобальной конкуренции. Дайте определение глобальное информационное противоборство на международной арене.
12. Информационная безопасность в обеспечении национальной безопасности Российской Федерации.
13. Перечислите базовые нормативно-правовые документы Российской Федерации в области национальной, информационной безопасности.
14. Назовите органы власти которые входят в государственную систему обеспечения информационной безопасности Российской Федерации.
15. Назовите законодательные органы Российской Федерации.
16. Назначение и роль судебных органов Российской Федерации в обеспечении информационной безопасности и защиты информации.
17. Перечислите органы исполнительной власти Российской Федерации, которые проводят единую техническую политику в области информационной безопасности и защиты информации,
18. Назовите министерства, ведомства, федеральные службы, которые разрабатывают нормативные и руководящие документы в области информационной безопасности и защиты информации.
19. Перечислите основные нормативные акты РФ в области информационной безопасности, назначение и основные положения.
20. Перечислите нормативно-правовые и руководящие документы органов исполнительной власти РФ , назначение и основные положения в сфере информационной безопасности.
21. Охарактеризуйте основные виды тайн.
22. Информация, как объект защиты.
23. Информационного право в обеспечении информационной безопасности, цели, задачи, принципы информационного права.
24. Значение и роль правового регулирования субъектов к объектам интеллектуальной собственности.
25. Приведите классификацию источников угроз информационной безопасности.

26. Приведите классификацию угроз информационной безопасности, методы и способы реализации угроз.
27. Назовите возможные каналы утечки, методы и способы несанкционированного доступа к защищаемой информации.
28. Назовите назначение, цели и задачи правового уровня обеспечения информационной безопасности.
29. Перечислите основные международные и российские стандарты в области информационной безопасности.
30. Основные положения по защите информации от несанкционированного доступа к объектам защиты.
31. Назовите назначение политики информационной безопасности в производственной деятельности предприятия.
32. Политика информационной безопасности, назначение, состав и содержание документа.
33. Назовите назначение и содержание программы информационной безопасности, состав и содержание документа.
34. Перечислите методики анализа и оценки рисков, влияющих на состояние информационных безопасности.
35. Перечислите меры процедурного уровня информационной безопасности, основные классы мер процедурного уровня.
36. Методы и принципы управления персоналом.
37. Основные меры обеспечения физической защиты, направления обеспечения физической защиты, цель, решаемые задачи.
38. Основные меры поддержания работоспособности, реагирование на нарушения режима безопасности: назначение, цель, решаемые задачи.
39. Основные меры планирования восстановительных работ: цель, решаемые задачи, методы по обеспечению работоспособностью информационных систем.
40. Принципы архитектурной безопасности и сервисы информационной безопасности.
41. Методы управления доступом к информационным ресурсам, определение, назначение, решаемые задачи.

7.2. Темы докладов (рефератов)

1. Проблемы кодификации информационного законодательства.
2. Правовое обеспечение информационной безопасности в сфере бизнеса
3. Право и СПАМ: возможности и перспективы правового регулирования почтовой рассылки в сети Интернет.
4. Всевозможные методы шифрования информации и их применение в различных сферах деятельности.
5. Защита программных данных от несанкционированного копирования.
6. Нормативно-правовое обеспечение информационной безопасности.
7. Стандарты информационной безопасности
8. Классификация информации. Виды данных и носителей.
9. Ценность информации. Цена информации.
10. Количество и качество информации.
11. Виды защищаемой информации.
12. Демаскирующие признаки объектов защиты.
13. Классификация источников и носителей информации.
14. Методы защиты информации от преднамеренного доступа.
15. Криптографическая защита информации (основные понятия).

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

8.1. Семестр 3

Номера разделов	Виды работ	Максимальное количество баллов
1	Организационно-учебная работа в аудитории	40
	Самостоятельная работа + контроль	20
	Индивидуально-творческое задание	10
ИТОГО		70
Зачет		30
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся во 2-м учебном корпусе (г. Донецк, ул. Университетская, д. 22). Для проведения лабораторных занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, материально-техническая база учебной лаборатории кафедры международных отношений и внешней политики (ауд. 25 и 52).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Внуков А. А. Основы информационной безопасности: защита информации: учебное пособие для СПО /Внуков А. А.. – 3-е изд., пер. и доп. – Москва : Юрайт, 2020 – 161 с. – Текст: электронный.
2. Гульяева Т. А. Основы информационной безопасности / Т. А. Гульяева. – Новосибирск : Новосибирский государственный технический университет, 2018 – 79 с. – Текст : электронный.

3. Казарин О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2021 — 342 с. — Текст : электронный

4. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва :

Издательство Юрайт, 2021 — 312 с. — Текст: электронный

5. Щербак А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2022 — 259 с. — Текст : электронный

11.2. Дополнительная литература

1. Вострецова Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. — Екатеринбург : Изд-во Урал. ун-та, 2019 — 204 с. — Текст : электронный

2. Гафнер В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с. — Текст : электронный

3. Груздева Л. М. Основы информационной безопасности : учеб. пособие в двух частях. — Ч. 1 / Л. М. Груздева. — М. : Юридический институт МИИТа, 2017 — 101 с. — Текст : электронный

4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с. — Текст : электронный

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. — Москва, 2019- . — URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). — Режим доступа: свободный, подписка. Необходима установка программного обеспечения. — Текст: электронный.

2. **eLIBRARY.RU:** научная электронная библиотека: сайт. — Москва, 2000- . — URL: <https://elibrary.ru> (дата обращения: 01.09.2023). — Режим доступа: для авторизов. пользователей. — Текст: электронный.

3. Научная электронная библиотека **«КиберЛенинка»:** сайт / Ассоциация «Открытая наука». — Москва, 2014- . — URL: <https://cyberleninka.ru/>. — Режим доступа: свободный. — Текст: электронный.

4. Электронно-библиотечная система **«Лань»:** [сайт]. — URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). — Режим доступа: для авторизов. пользователей. — Текст: электронный.

5. **ЭБС Юрайт:** электронная библиотечная система: сайт. — Москва, 2013. — URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). — Режим доступа: для авторизов. пользователей. — Текст: электронный.

6. **Электронно-библиотечная система ДонГУ:** сайт / ФГБОУ ВО «ДонГУ». — Донецк, 2016- . — URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). — Режим доступа: свободный. — Текст: электронный.

7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. — Текст: электронный // ЭБС ДонГУ: сайт. — URL: <http://library.donnu.ru/catalog/> (дата обращения: 01.09.2023). — Режим доступа: поиск свободный, электронные документы — для пользователей ДонГУ.

8. **Электронный архив ДонГУ**: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).