

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Институт экономики и предпринимательства

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Рабочая программа дисциплины

Информационная безопасность

Уровень высшего образования

Бакалавриат

Направление подготовки / специальность

38.03.03 - Управление персоналом

Направленность образовательной программы

Управление человеческими ресурсами

Форма обучения

очная, очно-заочная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.03 Информационная безопасность 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
УК-11: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-11.1: Анализирует действующие правовые нормы, способы профилактики, обеспечивающие борьбу с коррупцией и противодействие проявлениям экстремизма, терроризма в различных областях жизнедеятельности УК-11.2: Соблюдает правила взаимодействия на основе нетерпимого отношения к проявлению экстремизма, терроризма, коррупционному поведению в профессиональной деятельности	УК-11.1: Знать: механизмы и причины возникновения коррупционных явлений Уметь: оценивать риски и последствия коррупционной деятельности и применять соответствующие меры противодействия Владеть: навыками анализа нормативно - правовых документов для формулирования аргументации противодействия коррупционному поведению в профессиональной деятельности УК-11.2: Знать: современные средства и возможности систем информационной безопасности для противодействия экстремизму, терроризму, коррупционному поведению Уметь: использовать средства информационных технологий при решении профессиональных задач. Владеть: навыками работы с современными системами	Тест	Зачёт: Контрольные вопросы

		информационной безопасности при принятии управленческих решений		
УК-8: Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности и для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1: Демонстрирует знание основ создания и поддержки в повседневной жизни и в профессиональной деятельности безопасных условий жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов УК-8.2: Демонстрирует умение создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, грамотно вести себя при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1: Знать: современные подходы, принципы, методы и средства защиты для обеспечения безопасности рабочего места, организации и государства в целом. Уметь: применять современные средства защиты для обеспечения безопасности рабочего места, организации и государства в целом. Владеть: современными средствами защиты и методикой их применения для обеспечения безопасности рабочего места, организации и государства в целом. УК-8.2: Знать: основные подходы, принципы, методы и средства защиты, применяемые для предотвращения чрезвычайных ситуаций природного и техногенного характера на рабочем месте, в организации и в государстве в целом. Уметь: организовывать систему безопасности для предотвращения чрезвычайных ситуаций природного и техногенного характера на рабочем месте, в организации и в государстве в целом. Владеть: современными средствами защиты для предотвращения чрезвычайных ситуаций природного и техногенного характера на рабочем месте, в организации и в государстве в целом.	Тест	Зачёт: Контрольные вопросы

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная	очно-заочная
Общая трудоемкость, з.е.	2	2
Часов по учебному плану	72	72
в том числе		
аудиторные занятия (контактная работа):		
- занятия лекционного типа	16	8
- занятия семинарского типа (практические занятия / лабораторные работы)	16	8
- КСР	1	1
самостоятельная работа	39	55
Промежуточная аттестация	0 Зачёт	0 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				
ОФ	ОЗ	ОФ	ОЗ	ОФ	ОЗ	ОФ	ОЗ	ОФ	ОЗ		
Тема 1. Теоретические аспекты информационной безопасности экономических систем	13	12	3	1	2	1	5	2	8	10	
Тема2. Понятие информационных угроз и их виды	13	12	3	1	2	1	5	2	8	10	
Тема 3. Государственное регулирование информационной безопасности	11	12	3	1	2	1	5	2	6	10	
Тема 4.Подходы, принципы, методы и средства обеспечения безопасности	13	12	3	2	3	2	6	4	7	8	
Тема 5. Организация системы защиты информации	12	13	2	2	4	2	6	4	6	9	
Тема 6. Менеджмент и аудит систем информационной безопасности	9	10	2	1	3	1	5	2	4	8	
Аттестация	0	0									
КСР	1	1						1	1		
Итого	72	72	16	8	16	8	33	17	39	55	

Содержание разделов и тем дисциплины

Тема 1. Теоретические аспекты информационной безопасности экономических систем

Тема 2. Понятие информационных угроз и их виды

Тема 3. Государственное регулирование информационной безопасности

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности

Тема 5. Организация системы защиты информации

Тема 6. Менеджмент и аудит систем информационной безопасности

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.

- A. www.gks.ru / Федеральная служба государственной статистики.
- B. Операционная система Microsoft Windows
- C. Прикладное программное обеспечение Microsoft Office
- D. Справочно-правовая система «КонсультантПлюс»

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 - Тест) для оценки сформированности компетенции УК-11:

1. Информационная война - это...

- A. злословие в адрес другого человека;
- B. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;
- B. акт применения информационного оружия.

1. Информационная безопасность - это...

Невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);

- B. предотвращение зла наносимого государственным структурам;
- B. проведение природоохранных мероприятий.

1. К понятию информационной безопасности НЕ относятся:

- A. природоохранные мероприятия;
- B. надежность работы компьютера;

В. сохранность ценных данных.

1. К объектам информационной безопасности на предприятии НЕ относятся:

- А. информационные ресурсы;
- Б. средства вычислительной и организационной техники;
- В. Конституция России.

5. Обеспечение безопасности информации - это...

- А. одноразовое мероприятие;
- Б. комплексное использование всего арсенала имеющихся средств защиты;
- В. разработка каждой службой плановых мер по защите информации.

1. Лингвистическое обеспечение информационной безопасности - это?

- А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;
- Б. нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации;
- В. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

1. Эргономическое обеспечение информационной безопасности - это?

- А. антивирусные программы;
- Б. совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации;
- В. комплекс математических методов, связанных с оценкой опасности технических средств.

1. Информационное обеспечение информационной безопасности — это?

- А. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;
- Б. антивирусные программы;
- В. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы.

1. обеспечение информационной безопасности - это?

- А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;
- Б. совокупность средств;

В. нормативные документы по ИБ, требование которых являются обязательными в рамках сферы действия каждого подразделения.

10. К основным угрозам информационной безопасности НЕ относятся:

- А. раскрытие конфиденциальной информации;
- Б. нарушение принципов экономической безопасности;
- В. отказ от обслуживания.

1. Информационное оружие - это?

- А. комплекс технических средств, методов и технологий, направленных против управленческих систем;
- Б. нормативно-правовая база по информационной безопасности;
- В. комплекс индивидуального и общественного сознания.

1. Правовое обеспечение информационной безопасности - это..?

- А. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
- Б. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
- В. широкое использование технических средств защиты информации.

1. Экономическая информация является товаром?

- А. да;
- Б. нет;
- В. кроме конфиденциальных сведений.

1. К числу особенностей информации как товара НЕ относятся:

- А. сохраняемость;
- Б. несамостоятельность;
- В. самостоятельность.

15. Информация может составлять коммерческую тайну, если:

- А. к ней нет свободного доступа на законном основании;
- Б. содержится в учредительных документах;
- В. содержится в бухгалтерском балансах.

16. Что не являются коммерческой тайной?

А. сведения, содержащиеся в документах, дающие право заниматься предпринимательской деятельностью;

Б. сведения о научных разработках;

В. сведения о персонале предприятия.

17. Конфиденциальность компьютерной информацией - это?

А. предотвращение проникновения компьютерных вирусов в память ПЭВМ;

Б. свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы;

В. безопасное программное обеспечение.

18. Банковская тайна - это..?

А. информация о банковском счете, вкладе, операциях по счету, о клиентах банка;

Б. информация о сотрудниках банка;

В. информация о режиме работы банка.

1. Несанкционированным доступом является:

А. недостаточное знание работниками предприятия правил защиты информации;

Б. слабый контроль за соблюдением правил защиты информации;

В. хищение носителей информации и документальных отходов.

1. Реализации угроз информационной безопасности способствуют:

А. болтливость;

Б. простудные заболевания;

В. Налоговый кодекс.

1. Типовыми путями несанкционированного доступа к информации, являются:

А. дистанционное фотографирование;

Б. выход из строя ПЭВМ;

В. ураганы.

1. Несанкционированным доступом к информации НЕ является:

А. использование программных ловушек;

Б. любительское фотографирование;

В. включение в библиотеки программ специальных блоков типа «троянский конь».

1. К способам воздействия угроз на информационные объекты НЕ относятся:

А. программно-математические;

Б. организационно-правовые;

В. договорные отношения.

1. Хакерская война - это?

А. атака компьютеров и сетей гражданского информационного пространства;

Б. использование информации для влияния на умы союзников и противников;

В. блокирование информации, преследующее цель получить экономическое превосходство.

5.1.2 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции УК-8:

1. Ассоциация вычислительной техники создана в

А. 1947 году;

Б. 1964 году;

В. 2017 году.

1. Консорциум Всемирной Паутины оформлен

А. в 1989 году;

Б. в 1994 году;

В. в 2017 году.

1. Международная организация по стандартизации это

А. ISO;

Б. АСМ;

В. ООН.

1. Проект международных стандартов приобретает статус международного стандарта, если за него проголосовало

А. 100% членов;

Б. 75% членов;

В. 80% членов.

1. Альянс по безопасности сети Интернет создан в

А. 2001 г.

Б. 2016 г.

В. 2017 г.

1. Доктрина Информационной безопасности принята в

А. 2012 году

Б. 2014 году

В. 2016 году

1. В организационную основу системы обеспечения информационной безопасности РФ входит:

А. Совет безопасности РФ;

Б. Министерство образования и науки РФ;

В. ЦРУ США.

1. К актам федерального законодательства по ИБ в РФ входят:

А. Приказы ФСБ;

Б. Международные стандарты;

В. Конституция РФ.

1. Правовое обеспечение ИБ означает:

А. Защиту интересов физических и юридических лиц;

Б. Защиту интересов государства и общества;

В. Все вышеперечисленное.

1. Масштабы компьютерной преступности в РФ

А. Неуклонно снижаются;

Б. Возрастают;

2. Остаются из года в год неизменными.

3. Статья 23 Конституции РФ определяет:

А. Право на получение достоверной информации о состоянии окружающей среды;

Б. Право на неприкосновенность частной жизни, личную и семейную тайну и иные сообщения;

2. Отказ в предоставлении гражданину информации.

3. В Налоговом кодексе РФ имеется:

А. ст. 139 «Служебная и коммерческая тайна»;

Б. ст. 102 «Налоговые тайны»;

В. ст.946 «Тайна страхования».

1. Федеральный закон «Об информации, информационных технологиях и о защите информации»

А. пока не принят;

Б. принят в 2000 году;

В. принят в 2006 году.

1. Федеральный закон «О персональных данных» принят:

А. в 2006 году с изменениями на 1 января 2017 года;

Б. в 2009 году;

В. в 2016 году.

1. В какой статье УК предусматривается наказание за «Неправомерный доступ к компьютерной информации»?

А. в ст.272;

Б. в ст.273;

В. в ст.274.

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
зачтено	Ставится в случае, если студент отвечает четко и последовательно, показывая глубокие знания по теме и уверенное владение основным материалом
не зачтено	Ставится в случае, если студент при ответе на вопросы допускает грубые ошибки, демонстрирует незнание основных терминов и понятий

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатор достижения компетенций)	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
	не зачтено		зачтено				
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту	Уровень знаний ниже минимальных требований. Имели место грубые ошибки	Минимально допустимый уровень знаний. Допущено	Уровень знаний в объеме, соответствующем программе	Уровень знаний в объеме, соответствующем программе	Уровень знаний в объеме, соответствующем программе	Уровень знаний в объеме, превышающем программу подготовки.

	знаний вследствие отказа обучающегося от ответа		много негрубых ошибок	подготовки . Допущено несколько негрубых ошибок	подготовки . Допущено несколько несущественных ошибок	подготовк и. Ошибок нет.	
<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	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы все основные умения. Решены все основные задачи с отдельным и несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы 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 некоторым и недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторым и недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрирован 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 УК-11

Основные тенденции развития информатизации в экономике.

Основные понятия информационной безопасности в экономике.

Информационная безопасность в цифровой экономике.

Экономическая информация как товар и объект безопасности.

Система защиты информации и её структура.

Информационные угрозы, их виды и причины возникновения.

Информационные угрозы для государства.

Информационные угрозы для компании.

Информационные угрозы для личности (физического лица).

Действия и события, нарушающие информационную безопасность.

Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.

Способы воздействия информационных угроз на объекты.

Внешние и внутренние субъекты информационных угроз.

Компьютерные преступления и их классификация.

Исторические аспекты компьютерных преступлений и современность.

Субъекты и причины совершения компьютерных преступлений.

Вредоносные программы, их виды.

История компьютерных вирусов и современность.

Государственное регулирование информационной безопасности.

Деятельность международных организаций в сфере информационной безопасности.

Доктрина информационной безопасности России.

Уголовно-правовой контроль над компьютерной преступностью в России.

Федеральные законы по ИБ в РФ.

Политика безопасности и ее принципы.

Фрагментарный и системный подход к защите информации.

Методы и средства защиты информации.

Организационное обеспечение ИБ.
Организация конфиденциального делопроизводства.

Комплекс организационно-технических мероприятий по обеспечению защиты информации.
Инженерно-техническое обеспечение компьютерной безопасности.
Организационно-правовой статус службы безопасности.
Защита информации в Интернете.
Электронная почта и ее защита.
Защита от компьютерных вирусов.
«Больные» мобильники и их «лечение».
Популярные антивирусные программы и их классификация.
Организация системы защиты информации экономических объектов.
Криптографические методы защиты информации.
Этапы построения системы защиты информации.
Оценка эффективности инвестиций в информационную безопасность.

План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.

Управление информационной безопасностью на государственном уровне.
Аудит ИБ автоматизированных банковских систем.
Электронная коммерция и ее защита.
Менеджмент и аудит информационной безопасности на уровне предприятия.
Информационная безопасность предпринимательской деятельности.
Обеспечение информационной безопасности должностных лиц.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции УК-8

Основные тенденции развития информатизации в экономике.

Основные понятия информационной безопасности в экономике.

Информационная безопасность в цифровой экономике.

Экономическая информация как товар и объект безопасности.

Система защиты информации и её структура.

Информационные угрозы, их виды и причины возникновения.
Информационные угрозы для государства.
Информационные угрозы для компании.
Информационные угрозы для личности (физического лица).
Действия и события, нарушающие информационную безопасность.

Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.

Способы воздействия информационных угроз на объекты.

Внешние и внутренние субъекты информационных угроз.
Компьютерные преступления и их классификация.

Исторические аспекты компьютерных преступлений и современность.
Субъекты и причины совершения компьютерных преступлений.

Вредоносные программы, их виды.

История компьютерных вирусов и современность.

Государственное регулирование информационной безопасности.

Деятельность международных организаций в сфере информационной безопасности.

Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
зачтено	Ставится в случае, если студент отвечает четко и последовательно, показывая глубокие знания по теме и уверенное владение основным материалом
не зачтено	Ставится в случае, если студент при ответе на вопросы допускает грубые ошибки, демонстрирует незнание основных терминов и понятий

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

Основная литература:

1. 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. Баяндин Н. И. Информационно-аналитическое обеспечение безопасности бизнеса. Деловая разведка : учебник для студентов, обучающихся по направлению подготовки «информационная безопасность» / Баяндин Н. И. - Санкт-Петербург : Интермедия, 2017. - 264 с. - Книга из коллекции Интермедия - Информатика. - ISBN 978-5-4383-0122-6., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=880300&idb=0>.
3. Воробьев Е. Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных : учебное пособие для студентов вузов, обучающихся по направлению 090900 «информационная безопасность» / Воробьев Е. Г. - 3-е изд., перераб. - Санкт-Петербург : Интермедия, 2017. - 432 с. - Книга из коллекции Интермедия - Информатика. - ISBN 978-5-4383-0120-2., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=880308&idb=0>.
4. Гилязова Р. Н. Информационная безопасность. Лабораторный практикум / Гилязова Р. Н. - 3-е изд., стер. - Санкт-Петербург : Лань, 2022. - 44 с. - Книга из коллекции Лань - Информатика. - ISBN 978-5-8114-9138-4., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=880909&idb=0>.
5. 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>.

Дополнительная литература:

1. Пугин В. В. Основы информационной безопасности : методические указания к лабораторным работам для студентов очной формы обучения по направлению подготовки 10.05.02 «информационная безопасность телекоммуникационных систем» / Пугин В. В. - Самара : ПГУТИ, 2021. - 39 с. - Книга из коллекции ПГУТИ - Информатика., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=859685&idb=0>.
2. Никулин В. В. Информационная безопасность. Лабораторный практикум : учебно-методическое пособие для студентов направления подготовки 09.03.03 прикладная информатика / Никулин В. В. - Брянск : Брянский ГАУ, 2021. - 84 с. - Книга из коллекции Брянский ГАУ - Информатика., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=860117&idb=0>.
3. Малаховская М. В. Конкурентная разведка : учебное пособие для специальностей «экономическая безопасность», «информационная безопасность» / Малаховская М. В. - Санкт-Петербург : Интермедия, 2018. - 120 с. - Книга из коллекции Интермедия - Информатика. - ISBN 978-5-4383-0132-5., <https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=880302&idb=0>.

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

Консультант плюс

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 38.03.03 - Управление персоналом.

Автор(ы): Дорожкин Артем Владиславович, кандидат экономических наук.

Рецензент(ы): Яснев Вячеслав Николаевич, кандидат экономических наук.

Заведующий кафедрой: Трифонов Юрий Васильевич, доктор экономических наук.

Программа одобрена на заседании методической комиссии от 12.12.2023, протокол № 6.