Приложение 4

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION

Federal State Autonomous Educational Institution of Higher Education
«National Research Lobachevsky State University of Nizhny Novgorod»

Институт экономики и предпринимательства

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Working programme of the discipline

Information Security

Higher education level

Bachelor degree

Area of study / speciality

38.03.01 - Economics

Focus /specialization of the study programme

World Economy

Mode of study

full-time

Nizhny Novgorod

Year of commencement of studies 2024

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.15 Информационная безопасность относится к обязательной части 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**
ОПК-6: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	*ОПК-6.1: Понимает принципы работы современных информационных технологий* *ОПК-6.2: Использует принципы работы современных информационных технологий для решения задач профессиональной деятельности*	*ОПК-6.1:* *- знать принципы работы современных информационных технологий,* *- уметь понимать принципы работы современных информационных технологий,* *- владеть принципами работы современных информационных технологий* *ОПК-6.2:* *- знать использование принципов работы современных информационных технологий для решения задач профессиональной деятельности,* *- уметь использовать принципы работы современных информационных технологий для решения задач профессиональной деятельности,* *- владеть использованием принципов работы современных информационных технологий для решения задач профессиональной деятельности*	*Доклад-презентация*	*Зачёт:* *Доклад-презентация*
ПК-3: Способен анализировать и интерпретировать данные отечественной и	*ПК-3.1: Формирует, анализирует и интерпретирует финансово-экономическую информацию*	*ПК-3.1:* *- знать формирование, анализ и интерпретацию финансово-экономической информации,* *- уметь формировать,*	*Доклад-презентация*	*Зачёт:* *Доклад-презентация*

зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений	*ПК-3.2: Выявляет тенденции и использует результаты анализа информации для принятия управленческих решений*	*анализировать и интерпретировать финансово-экономическую информацию,* *- владеть формированием, анализом и интерпретацией финансово-экономической информации* *ПК-3.2:* *- знать выявление тенденций и использование результатов анализа информации для принятия управленческих решений,* *- уметь выявлять тенденции и использовать результаты анализа информации для принятия управленческих решений,* *- владеть выявлением тенденций и использованием результатов анализа информации для принятия управленческих решений*		

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	**2**
Часов по учебному плану	**72**
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	**16**
- занятия семинарского типа (практические занятия / лабораторные работы)	**16**
- КСР	**1**
самостоятельная работа	**39**
Промежуточная аттестация	**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	
	очно	очно	очно	очно	очно
Классификация угроз информационной безопасности	18	4	4	8	10
Построение защиты информации	53	12	12	24	29
Аттестация	0				
КСР	1			1	
Итого	72	16	16	33	39

Contents of sections and topics of the discipline

Раздел 1. Угроза — это фактор, стремящийся нарушить работу системы. В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности, насчитывающий сотни пунктов. Для информационных систем было предложено рассматривать три основных вида угроз:
1. Угроза нарушения конфиденциальности реализуется в том случае, если информация становится известной лицу, не располагающему полномочиями доступа к ней. Угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в информационной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой нарушения конфиденциальности используется термин «утечка».
2. Угроза нарушения целостности реализуется при несанкционированном изменении информации, хранящейся в информационной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).
3. Угроза нарушения доступности (отказа служб) реализуется, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Блокирование может быть постоянным — запрашиваемый ресурс никогда не будет получен, или может вызывать только задержку запрашиваемого ресурса. 4. Угроза раскрытия параметров системы, включающей в себя систему защиты. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которой определяются основные параметры системы, ее характеристики и т. п.
Результатом разведки является уточнение поставленной задачи, а также выбор наиболее оптимального технического средства.
Раздел 2. Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:
- организационные (в т. ч. административные);
- технологические (или инженерно-технические);
- правовые;
- финансовые;

- морально-этические (или социально-психологические).
К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников.
Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например, систем идентификации и аутентификации или охранной сигнализации.
Третья категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации.
Финансовые методы защиты предполагают введение специальных доплат при работе с защищаемой информацией, а также систему вычетов и штрафов за нарушение режимных требований. Морально-этические методы не носят обязательного характера, однако являются достаточно эффективными при борьбе с внутренними нарушителями. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации)
способов защиты.

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.

Для обеспечения самостоятельной работы обучающихся используются:
- электронный курс "Информационная безопасность".

5. Assessment tools for ongoing monitoring of learning progress and interim certification in the discipline (module)

5.1 Model assignments required for assessment of learning outcomes during the ongoing monitoring of learning progress with the criteria for their assessment:

5.1.1 Model assignments (assessment tool - Report-presentation) to assess the development of the competency ОПК-6:

В чем уязвимость информационных ресурсов?

5.1.2 Model assignments (assessment tool - Report-presentation) to assess the development of the competency ПК-3:

Назовите тенденции в защите информации.

Assessment criteria (assessment tool — Report-presentation)

Grade	Assessment criteria
pass	Вопрос изучен, излагаемый материал полностью раскрывает вопрос
fail	Излагаемый материал не полностью раскрывает вопрос

Grade	Assessment criteria

5.2. Description of scales for assessing learning outcomes in the discipline during interim certification

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	**плохо**	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	не зачтено		**зачтено**				
Знания	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.
Умения	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 отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	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	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми 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

Scale of assessment for interim certification

Grade		Assessment criteria
pass	**outstanding**	All the competencies (parts of competencies) to be developed within the discipline have been developed at a level no lower than "outstanding", the knowledge and skills for the relevant competencies have been demonstrated at a level higher than the one set out in the programme.
	excellent	All the competencies (parts of competencies) to be developed within the discipline have been developed at a level no lower than "excellent",
	very good	All the competencies (parts of competencies) to be developed within the discipline have been developed at a level no lower than "very good",
	good	All the competencies (parts of competencies) to be developed within the discipline have been developed at a level no lower than "good",
	satisfactory	All the competencies (parts of competencies) to be developed within the discipline have been developed at a level no lower than "satisfactory", with at least one competency developed at the "satisfactory" level.
fail	**unsatisfactory**	At least one competency has been developed at the "unsatisfactory" level.
	poor	At least one competency has been developed at the "poor" level.

5.3 Model control assignments or other materials required to assess learning outcomes during the interim certification with the criteria for their assessment:

5.3.1 Model assignments (assessment tool - Report-presentation) to assess the development of the competency ОПК-6

Каковы основные цели защиты информации?

5.3.2 Model assignments (assessment tool - Report-presentation) to assess the development of the competency ПК-3

Каковы особенности стандартов информационной безопасности в разных странах?

Assessment criteria (assessment tool — Report-presentation)

Grade	Assessment criteria
pass	Вопрос изучен, излагаемый материал полностью раскрывает вопрос
fail	Излагаемый материал не полностью раскрывает вопрос

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

Основная литература:

1. Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, В. А. Матвеев [и др], под общей ред. В. Н. Ясенева ; ННГУ им. Н. И. Лобачевского. - Нижний Новгород : Изд-во ННГУ, 2018. - 182 с. - Текст : электронный., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=796253&idb=0.

Дополнительная литература:

1. Щербак А. В. Информационная безопасность : учебник / А. В. Щербак. - Москва : Юрайт, 2023. - 259 с. - (Профессиональное образование). - ISBN 978-5-534-15345-3. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=845835&idb=0.
2. Суворова Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. - Москва : Юрайт, 2023. - 253 с. - (Высшее образование). - ISBN 978-5-534-13960-0. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=839715&idb=0.
3. Нестеров С. А. Информационная безопасность : учебник и практикум / С. А. Нестеров. - Москва : Юрайт, 2018. - 321 с. - (Профессиональное образование). - ISBN 978-5-534-07979-1. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=840366&idb=0.

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

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

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 38.03.01 - Economics.

Author(s): Носаков Игорь Владимирович, кандидат технических наук.
Заведующий кафедрой: Горбунова Мария Лавровна, доктор экономических наук.

Программа одобрена на заседании методической комиссии от 12.12.23, протокол № 6.