Приложение 4

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
38.03.06 - Торговое дело

Направленность образовательной программы
Управление торговой и логистической деятельностью

Форма обучения
очная, очно-заочная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.О.14 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-2: Способен осуществлять сбор, обработку и анализ данных, необходимых для решения оперативных и тактических задач в сфере профессиональной деятельности	*ИД-1: Осваивает статистические методы формирования данных и применяет направления и методы анализа информации в контексте конкретных управленческих задач* *ИД-2: Применяет знания об основных методах, способах и средствах получения, хранения и переработки информации в целях реализации функций профессиональной деятельности, владеет навыками работы с компьютером как средством управления информацией, работает с информацией в глобальных компьютерных сетях*	*ИД-1:* *Знать методы сбора, обработки и анализа данных, необходимых для решения оперативных и тактических задач в сфере профессиональной деятельности* *Уметь применять сбор, обработку и анализ данных, необходимых для решения оперативных и тактических задач в сфере профессиональной деятельности* *Владеть Способами сбора, обработки анализа данных, необходимых для решения оперативных и тактических задач в сфере профессиональной деятельности* *ИД-2:* *Знать: современные средства и возможности систем информационной безопасности при обработке отчетности в целях принятия управленческих решений* *Уметь: использовать средства информационных технологий при решении профессиональных задач.* *Владеть: навыками работы с современными системами*	*Доклад* *Задания* *Тест*	*Зачёт:* *Контрольные вопросы* *Практическое задание*

		информационной безопасности при принятии управленческих решений		
ОПК-6: Способен понимать принципы работы современных информационных технологий и использовать их для *решения задач профессиональной деятельности.*	*ИД-1: Понимает принципы работы современных информационных технологий и использует их в профессиональной деятельности* *ИД-2: Обрабатывает полученную информацию и использует ее для решения задач профессиональной деятельности*	*ИД-1:* *Знать: основные методы, способы и средства преобразования информации* *Уметь: работать с компьютером как средством управления информацией* *Владеть: основными способами обнаружения информационных угроз и использования с антивирусных программ* *ИД-2:* *Знать: функции и задачи менеджмента и аудита систем информационной безопасности* *Уметь: выявлять информационные угрозы, выбирать методы и средства управления и аудита систем информационной безопасности* *Владеть: принципами менеджмента и аудита систем информационной безопасности*	*Дискуссия* *Задания* *Тест*	*Зачёт:* *Контрольные вопросы* *Практическое задание*

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			
	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно	очно	очно-заочно
Тема 1. Теоретические аспекты информационной безопасности экономических систем	35	33	8	4	8	4	16	8	19	25
Тема2. Понятие информационных угроз и их виды	36	38	8	4	8	4	16	8	20	30
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

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 "https://e-learning.unn.ru/course/view.php?id=1809" (https://e-learning.unn.ru/course/view.php?id=1809).

Иные учебно-методические материалы: 1. Определить место и роль информационной безопасности при использовании личного компьютера и мобильных устройств. Охарактеризовать последствия взлома ваших личных аккаунтов в соц. сетях, электронной почты.

2. Вы работаете бухгалтером-экономистом. Под Вашим логином и паролем со счета предприятия ушли большие суммы денег неизвестным контрагентам. Последствия, Ваша ответственность.

3. Вы работаете клиентским менеджером. С Вашего компьютера похищена клиентская база. Конкуренты предложили Вашим клиентам более привлекательные условия и цены. Последствия. Ваша ответственность.

4. Приведите примеры нарушения информационной безопасности из собственной

практики. Охарактеризуйте последствия. Какие действия предпринимало руководство Вашей организации? Как в дальнейшем складывалась карьера виновных сотрудников?
Типовые задания для оценки сформированности компетенции _ПК-3___
1.Защита информации от сбоев оборудования и случайной потери
1. Ответьте на вопрос: «Что подразумевается под сбоем оборудования?», «Что означает случайная потеря информации?»
2. Определите методы защиты
1 периодическое архивирование программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);
2 автоматическое резервирование файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.
3 периодическая проверка исправности оборудования (в частности - поверхности жесткого диска) при помощи специальных программ. Например: Disk Doctor, ScanDisk . Подобные программы позволяют обнаружить дефектные участки на поверхности диска и соответствующим образом их пометить, чтобы при записи информации эти участки были обойдены.
4 периодическая оптимизация (дефрагментация) диска для рационального размещения файлов на нем, ускорения работы и уменьшения его износа.

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 - Доклад) для оценки сформированности компетенции ОПК-2:

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Что понимается под средствами защиты государственной тайны?
4. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
5. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
6. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
7. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
8. Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?

9. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".
10. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
11. Показатели защищенности межсетевых экранов.

Критерии оценивания (оценочное средство - Доклад)

Оценка	Критерии оценивания
зачтено	отлично - Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично» очень хорошо Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо» хорошо- Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «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», ни одна из компетенций не сформирована на уровне «плохо» плохо Хотя бы одна компетенция сформирована на уровне «плохо»

5.1.2 Типовые задания (оценочное средство - Дискуссия) для оценки сформированности компетенции ОПК-6:

1. **Темы для проведения дискуссий (ОПК-6, ПК-3)**

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Что понимается под средствами защиты государственной тайны?
4. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
5. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
6. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
7. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
8. Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?

9. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".
10. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
11. Показатели защищенности межсетевых экранов.

Классы защищенности межсетевых экранов

Критерии оценивания (оценочное средство - Дискуссия)

Оценка	Критерии оценивания
зачтено	отлично - Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично» очень хорошо Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо» хорошо- Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «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», ни одна из компетенций не сформирована на уровне «плохо» плохо Хотя бы одна компетенция сформирована на уровне «плохо» льно Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»

5.1.3 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-2:

1. **Задания для оценки компетенции «ОПК-2»**

Задание 1

1. Определить место и роль информационной безопасности при использовании личного компьютера и мобильных устройств. Охарактеризовать последствия взлома ваших личных аккаунтов в соц. сетях, электронной почты.
2. Вы работаете бухгалтером-экономистом. Под Вашим логином и паролем со счета предприятия ушли большие суммы денег неизвестным контрагентам. Последствия, Ваша ответственность.
3. Вы работаете клиентским менеджером. С Вашего компьютера похищена клиентская база. Конкуренты предложили Вашим клиентам более привлекательные условия и цены. Последствия. Ваша ответственность.

4. Приведите примеры нарушения информационной безопасности из собственной практики. Охарактеризуйте последствия. Какие действия предпринимало руководство Вашей организации? Как в дальнейшем складывалась карьера виновных сотрудников?

Задание 2

Защита информации от сбоев оборудования и случайной потери

1. Ответьте на вопрос: «Что подразумевается под сбоем оборудования?», «Что означает случайная потеря информации?»
2. Определите методы защиты
3. периодическое архивирование программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);
4. автоматическое резервирование файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.
5. периодическая проверка исправности оборудования (в частности - поверхности жесткого диска) при помощи специальных программ. Например: Disk Doctor, ScanDisk . Подобные программы позволяют обнаружить дефектные участки на поверхности диска и соответствующим образом их пометить, чтобы при записи информации эти участки были обойдены.
6. периодическая оптимизация (дефрагментация) диска для рационального размещения файлов на нем, ускорения работы и уменьшения его износа.

Определите методы защиты от случайной потери или искажения информации, *хранящейся в компьютере:*

1 автоматический запрос на подтверждение команды, приводящей к изменению содержимого какого-либо файла. Если вы хотите удалить файл или разместить новый файл под редакторы позволяют сделать документ доступным только для чтения или скрыть файл, сделав недоступным его имя в программах работы с файлами;

1. возможность отменить последние действия. Если вы редактируете документ, то можете пользоваться функцией отмены последнего действия или группы действий, имеющейся во всех современных редакторах. Если вы ошибочно удалили нужный файл, то специальные программы позволяют его восстановить, правда, только в том случае, когда вы ничего не успели записать поверх удаленного файла;
2. разграничение доступа пользователей к ресурсам файловой системы, строгому разделению системного и пользовательского режимов работы вычислительной системы.

Ответьте на вопрос: «Что означает защита информации от кражи?»

Определите методы защиты информации.

5.1.4 Типовые задания (оценочное средство - Задания) для оценки сформированности компетенции ОПК-6:

Типовые практические задания для оценки сформированности компетенции ОПК-6

1. Как по отношению к информации Вашей организации ведут себя конкурирующие фирмы?

Пытаются ли они заполучить важную информацию? Каким образом это происходит?

1. Сайт фирмы. Что допустимо на нем размещать? Уместно ли размещать образцы договоров?

Выскажите Ваше мнение. Как сейчас в условиях кризиса размещать прайсы? С минимальной ценой от какой то суммы? Поясните Вашу позицию.

1. Некая фирма решила торговать тем же ассортиментом что и ваша фирма. Запрашивает прайс у поставщика, программисты полностью копируют ваш интернет-магазин, меняют только главную страницу сайта. Как это предупредить заранее? Опишите Ваши действия.
2. У Вас небольшая фирма. Вид деятельности придумайте сами. Как угрозы информационной безопасности вашей деятельности вы предполагаете? Как вы будете защищать информацию?
3. ИТ-специалист вашей фирмы. Как вы будете работать с ним? По договору? Возьмете его в штат? Какие обязанности вы для него предусмотрите с учетом требований информационной безопасности? Бюджет ограничен. На что вы планируете потратить деньги в первую очередь при сотрудничестве с ИТ-специалистом?
4. На какой платформе вы бы поручили разработать сайт компании? Обоснуйте решение.

Ответьте на вопрос: «Что такое компьютерный вирус?».
Назовите разновидности вирусов
Определите методы защиты от вирусов.

Задание 2

Установить антивирусное программное обеспечение на мобильное устройство и выполнить сканирование на вирусы

Разобрать практические ситуации

1. Связь основных понятий информационной безопасности

В издательство "Тезис" поступил звонок от провайдера. Предприятию отключили доступ к сети, потому что была зарегистрирована рассылка спама. Пришли большие счета, при сравнительно малом использовании ресурсов сети. В результате отключения Интернета были просрочены заказы, нарушена связь с несколькими клиентами, Оказалось, что менеджеры имеет несложный пароль, в основном даты рождения. У некоторых на мониторе приклеен стикер с паролем. Какие ошибки в информационном поведении сотрудников. Как действовать в данной ситуации. Как избежать подобных ситуаций позднее?

1. Основные уязвимости

Иногда изменяются содержательные данные, порой — служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) возбудила судебный иск против президента корпорации, обвиняя его в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее боссом президенту.

Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что он (босс) в указанное время разговаривал по мобильному телефону, находясь за рулем автомобиля вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарь знала пароль своего босса, поскольку ей было поручено его регулярное изменение), и иск был отвергнут... Участники обсуждения делятся на защитников секретаря и защитников босса компании Oracle и доказывают правоту защищаемой стороны и возможность фальсификации доказательств противника.

1. История вирусов

Александр Квасов, начальник управления информационных технологий Нижегородского регионального центра-филиала ОАО АКБ «СОЮЗ»: — В конце 90-х много вирусов было настроено на остановку работоспособности компьютера — уничтожение информации в BIOS, и на жестких дисках. На себе я испытал поражение жесткого диска вирусом W95.CIH «Чернобыль». На офисных компьютерах стояла операционная система Windows 95, доступ в Интернет имел один компьютер, остальные были связаны с ним в локальной сети. 26 апреля 1999 года не загрузились все офисные компьютеры, информация на дисках стала недоступной. Данные, к счастью, удалось восстановить, однако это было не так просто. Фирма понесла большие убытки.

Критерии оценивания (оценочное средство - Задания)

Оценка	Критерии оценивания
зачтено	отлично - Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично» очень хорошо Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо» хорошо- Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «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», ни одна из компетенций не сформирована на уровне «плохо» плохо Хотя бы одна компетенция сформирована на уровне «плохо» льно Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»

5.1.5 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-2:

Тест 1

1. Информационная война - это...
2. злословие в адрес другого человека;

Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;

2. акт применения информационного оружия.
3. Информационная безопасность - это...

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

Б. предотвращение зла наносимого государственным структурам;

В. проведение природоохранных мероприятий.

1. К понятию информационной безопасности НЕ относятся:

А. природоохранные мероприятия;

Б. 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.

1. Обеспечение безопасности информации - это...
2. одноразовое мероприятие;

+Б. комплексное использование всего арсенала имеющихся средств защиты;

2. разработка каждой службой плановых мер по защите информации.
3. 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. Организационное 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.

1. 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.

5.1.6 Типовые задания (оценочное средство - Тест) для оценки сформированности компетенции ОПК-6:

Тест 1

1. Минимизация утечки информации через персонал это

А. организационно-технические средства защиты информации;
Б. организационно-экономические меры;
В. организационно-административные меры.

1. К организации конфиденциального делопроизводства относится:

А. организация документооборота;
Б. использование сертифицированных технических и программных средств;
В. проверка надежности сотрудников.

1. Организационное обеспечение информационной безопасности - это..?

А. реализация защиты информации, осуществляемая службами безопасности режима, защита информации техническими средствами и др.;
Б. совокупность средств, обеспечивающих удобства работы пользователей;
В. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения.

1. С увольняющимися сотрудниками

А. подписывается договор о не распространении конфиденциальности;
Б. обмениваются рукопожатием;
В. предлагают вернуться.

1. Организация документооборота предполагает:

А. исключение доступа к бумажной «стружке»;
Б. предупреждение не обоснованного ознакомления с документами;
В. исключение не обоснованной рассылки.

1. Проведение организационно-экономических мероприятий предполагает:

А. страхование информационных рисков;
Б. организацию пассивного противодействия техническими средствами;
В. обеспечения электронного документооборота.

Тест 2

1. Адрес электронной почты включает:

А. Логин.
Б. Символический адрес сервера и имя зоны.
В. Все вышеперечисленное.

1. Электронная почта НЕ служит для:
2. Передачи текстовых сообщений в пределах Интернет.

Б. Системы телеконференций.

В. Оповещения пользователей о наступлении определенных событий.

С. Информационными угрозами в Интернете НЕ является:

А. Несанкционированный доступ к сети организации.
Б. Сбор и мониторинг сетевой информации в интересах третьих лиц.
В. Использование брандмауэра.

1. Для защиты электронной почты в Интернете используются:

А. Антивирусные программы.
Б. Специальные протоколы (REM, CryptoAPi и др.)

В. Наиболее простое обозначение электронной почты (фамилия, паспортные данные и т.п.).

1. Основные сервисы системы Интернет:

А. WorldWideWeb (WWW).
Б. Программы-браузеры и системы телеконференций.
В. Все вышеперечисленное.

1. К серверам системы Интернет НЕ относятся:

А. Программа печати учетных документов.
Б. Программа пересылки файлов.
В. Система информационного поиска сети Интернет.

1. Адрес электронной почты имеет вид:

А. логин@символический адрес сервера.имя зоны;
Б. логин.имя зоны;
В.логин.

1. Межсетевой экран - это

А. Брандмауэр (Firewalls);
Б. Фильтр;

1. Антивирусная программа.
2. Чтобы избавиться от мобильного вируса:

А. Нужно пользоваться клавишным мобильником.
Б. Приобрести самый дорогостоящий мобильник.
В. Познакомиться с хакером.

1. Недостатком информирования с симметричным ключом:
2. Легко реализовать аппаратно;

Б. Быстрота;

B. Оба ключа одинаковы.
C. Преимущества шифрования с открытым (ассиметричным) ключом
D. Работает медленно;

Б. Требует больших вычислительных мощностей;
В. используется два разных ключа.

Критерии оценивания (оценочное средство - Тест)

Оценка	Критерии оценивания
зачтено	отлично - Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично» очень хорошо Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо» хорошо- Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо» удовлетворительно Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне

Оценка	Критерии оценивания
	не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
не зачтено	неудовлетворительно Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо» плохо Хотя бы одна компетенция сформирована на уровне «плохо» льно Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»

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**				
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	При решении стандартных	Имеется минимальн	Продемонстрированы	Продемонстрированы	Продемонстрированы	Продемонстрирован

	навыков. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	задач не продемонстрированы базовые навыки. Имели место грубые ошибки	ый набор навыков для решения стандартных задач с некоторыми недочетами	базовые навыки при решении стандартных задач с некоторыми недочетами	базовые навыки при решении стандартных задач без ошибок и недочетов	навыки при решении нестандартных задач без ошибок и недочетов	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 ОПК-2

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 безопасности на государственном уровне

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ОПК-6

1. Основные тенденции развития информатизации в экономике.
2. Основные понятия информационной безопасности в экономике.
3. Информационная безопасность в цифровой экономике.
4. Экономическая информация как товар и объект безопасности.
5. Система защиты информации и её структура.
1. 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.
2. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
Способы воздействия информационных угроз на объекты.
3. Внешние и внутренние субъекты информационных угроз.
Компьютерные преступления и их классификация.
Исторические аспекты компьютерных преступлений и современность.
Субъекты и причины совершения компьютерных преступлений.
4. Вредоносные программы, их виды.
5. История компьютерных вирусов и современность.
6. Государственное регулирование информационной безопасности.
Деятельность международных организаций в сфере информационной безопасности.
Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
Доктрина информационной безопасности России.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
зачтено	отлично - Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично» очень хорошо Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо» хорошо- Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «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»

Оценка	Критерии оценивания
не зачтено	неудовлетворительно Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо» плохо Хотя бы одна компетенция сформирована на уровне «плохо»

5.3.3 Типовые задания (оценочное средство - Практическое задание) для оценки сформированности компетенции ОПК-2

Разобрать практические ситуации.

1. Компьютерная неграмотность персонала

В понедельник утром в фирму "Омега" поступил звонок от провайдера. Фирме отключили доступ к сети, потому что в период с 3.00 до 5.00 с адреса компьютера секретаря была совершена рассылка 1500 писем. Секретарь фирмы - Яна, имеет несложный пароль, состоящий из цифр, по совету системного администратора часто меняет его, но не придумывая новый, а переставляю цифры в старом, для запоминания клеит стикеры с паролем на монитор. Какие ошибки в информационном поведении сотрудницы. Как действовать в данной ситуации. Как избежать подобных ситуаций позднее?

1. Вы купили готовый бизнес - автомойка + шиномонтаж. Выполните аудит информационной безопасности предприятия. Проверьте наличие защиты компьютеров, хранение клиентской базы, доступ к АСУ, уровни доступа пользователей. Проверьте отключен ли доступ к АСУ у уволившихся сотрудников. Продолжите дальше список ваших действий.
2. Вы поступили на должность директора кафе. Проведите аудит информационной безопасности. Дайте рекомендации собственнику бизнеса.
3. Ответьте на вопрос «Что такое несанкционированный доступ?». Определите методы защиты.
4. Есть множество программ, помогающих защитить информацию на вашем компьютере. Ознакомьтесь и установите их.

Программный продукт SysUtils Device Manager Enterprise Edition обеспечивает разграничение доступа к устройствам хранения данных, использующим съемные носители информации, таким как дискетные дисководы, компакт-дисководы и накопители на флэш-памяти.
CD-DVD Lock - программа дает возможность запретить доступ на чтение или на запись съемных дисков - CD, DVD,USB, дискет, а также на определенные разделы жестких дисков. Можно ограничить доступ двумя путями: скрыть ваши устройства от возможности просмотра или закрыть к ним доступ.
TimeBoss - программа предназначена для управления временем работы пользователей, зарегистрированных в системе Windows. Позволяет ограничивать время, запрещать запуск отдельных указанных программ или программ, расположенных в определенных папках или дисках. Ведет журнал учета работы пользователей.

Lock 2.0 - предназначена для блокирования запуска приложений, графических и текстовых файлов. Lock не позволяет также перемещать, копировать и прикреплять к

отправляемым по e- mail письмам указанные файлы. Что может существенно ограничить доступ к Вашей информации посторонним лицам.

5.3.4 Типовые задания (оценочное средство - Практическое задание) для оценки сформированности компетенции ОПК-6

1. **Задания для оценки компетенции «ОПК-6»**

1. Задачи информационной безопасности состоят в…
2. Перечислите основополагающие документы по информационной безопасности.
3. Понятие государственной тайны.
4. Что понимается под средствами защиты государственной тайны?
5. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
6. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
7. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
8. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?

Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?

1. **Задания для оценки компетенции ОПК-2**

Рассмотрите вопросы на примере конкретного предприятия.
Что может предпринять руководство
Управление эффективной системой обеспечения безопасности и ее координация -задача, которую следует решать на уровне правления компании. Слабое знание этого вопроса не может стать поводом для уклонения от его обсуждения.
Как добиться того, чтобы рассмотрение вопросов поддержания безопасности отражало потребности предприятия, а не было реакцией на нашумевшие статьи в прессе?
Задавайте правильные вопросы, критически анализируйте ответы и оценивайте результаты. Перечисленные ниже вопросы помогут вам в этом.

1. Понимает ли правление вашего предприятия, что задачу обеспечения информационной безопасности следует решать на уровне правления и нельзя передавать исключительно под ответственность отдела ИТ? Согласована ли стратегия обеспечения ИБ предприятия с его общей стратегией?
2. Существует ли в вашей организации четкое распределение обязанностей по под держанию ИБ?

3) Могут ли руководители определить риски и опасные зоны деятельности предприятия? С какой периодичностью эти данные пересматриваются?
4) Знаете ли вы, сколько средств тратится на ИБ, и на что именно? В состоянии ли вы оценить отдачу от этих вложений?

5) Какие последствия для предприятия будет иметь серьезное нарушение безопасности (для репутации и доходов, юридические последствия, для результатов операционной деятельности и доверия инвесторов)?

1. Считается ли в вашей компании, что система ИБ может быть инструментом, стимулирующим новые виды деятельности (например, если вы внедрите эффективную систему ИБ, удастся ли организации увеличить объем операций в Internet)?
2. Насколько вам грозит риск приобрести репутацию компании, небрежно относящейся к вопросам ИБ?
3. Какие меры вы приняли, чтобы действующие из лучших побуждений (или наоборот) третьи лица не смогли нанести ущерб информационной безопасности вашей компании?
4. Каким образом вы проводите независимую проверку с целью убедиться в том, что управление ИБ организовано в компании должным образом?

10)Как вы оцениваете эффективность предпринимаемых вами мер по обеспечению ИБ?

Что можно сделать

Если вы считаете, что у вашего предприятия есть стратегия обеспечения информационной безопасности, убедитесь в том, что (1) в ней учтены все риски, с которыми компания сталкивается, а не только используемые вашей компанией информационные технологии, (2) эта стратегия правильно понята и (3) выполняется. Удостоверьтесь, что вы получаете объективное подтверждение эффективности своей стратегии. Если у предприятия стратегии нет, то действовать нужно уже сейчас:

1) Вне зависимости от того, тестируете ли вы существующую стратегию ИБ или разрабатываете новую с нуля, удостоверьтесь в том, что окончательный вариант стратегии будет давать положительные ответы на приведенные ниже вопросы:

учитывает ли данная стратегия общую стратегию деятельности вашего предприятия, его опыт и культуру;

соответствует ли она общей стратегии в области ИТ и обеспечения безопасности коммерческой деятельности предприятия;

служит ли она основой для программ информирования о целях информационной безопасности, стратегии выбора поставщиков, привлечения финансирования, определения приоритетов, поиска ресурсов, внедрения технологий и оборудования;

дает ли она рекомендации для принятия решений по основным партнерам-поставщикам услуг, клиентам и продавцам;

существует ли ясно сформулированный и согласованный список расположенных в порядке значимости слабых сторон предприятия и угрожающих ему рисков? Регулярно ли производится пересмотр этого списка?

Критерии оценивания (оценочное средство - Практическое задание)

Оценка	Критерии оценивания
зачтено	отлично - Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично» очень хорошо Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо» хорошо- Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна

Оценка	Критерии оценивания
	компетенция сформирована на уровне «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», ни одна из компетенций не сформирована на уровне «плохо» плохо Хотя бы одна компетенция сформирована на уровне «плохо»

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

Основная литература:

1. Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев ; ННГУ им. Н. И. Лобачевского. - Нижний Новгород : Изд-во ННГУ, 2017. - 198 с. - Текст : электронный., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=823079&idb=0.
2. Баранова Елена Константиновна. Информационная безопасность и защита информации : Учебное пособие / Национальный исследовательский университет "Высшая школа экономики". - 4. - Москва : Издательский Центр РИОР, 2022. - 336 с. - ВО - Бакалавриат. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=832410&idb=0.

Дополнительная литература:

1. Баранова Елена Константиновна. Информационная безопасность и защита информации : Учебное пособие / Национальный исследовательский университет "Высшая школа экономики". - 4. - Москва : Издательский Центр РИОР, 2022. - 336 с. - ВО - Бакалавриат. - ISBN 978-5-369-01761-6. - ISBN 978-5-16-106532-7. - ISBN 978-5-16-013849-7., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=832410&idb=0.

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

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

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

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 38.03.06 - Торговое дело.

Автор(ы): Ясенев Вячеслав Николаевич, кандидат экономических наук, профессор.

Заведующий кафедрой: Трифонов Юрий Васильевич, доктор экономических наук.

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