Приложение № 6 к ОПОП высшего образования, направление подготовки 38.03.01 Экономика, направленность (профиль) программы прикладного бакалавриата «Финансы и кредит»

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
МОСКОВСКИЙ ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ
(АНО ВО МГЭУ)
НИЖЕГОРОДСКИЙ ИНСТИТУТ (ФИЛИАЛ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.10 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки **38.03.01 Экономика**

Направленность (профиль) основной профессиональной образовательной программы прикладного бакалавриата **«Финансы и кредит»**

Формы обучения:	очная, заочная
Виды профессиональной деятельности:	расчетно-финансовая; банковская
Учебный год:	2018/2019

Нижний Новгород 2018

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
МОСКОВСКИЙ ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ
(АНО ВО МГЭУ)
НИЖЕГОРОДСКИЙ ИНСТИТУТ (ФИЛИАЛ)

У Т В Е Р Ж Д А Ю
Директор НИ (ф) АНО ВО МГЭУ
_____ Е.Б. Жбаков
«06» июля 2018г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки **38.03.01 Экономика**

Направленность (профиль) основной профессиональной образовательной программы прикладного бакалавриата **«Финансы и кредит»**

Формы обучения:	очная, заочная
Виды профессиональной деятельности:	расчетно-финансовая; банковская
Учебный год:	2018/2019

Нижний Новгород 2018

Рабочая программа дисциплины разработана в соответствии с:

- Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.03.01 Экономика (уровень бакалавриата) от 12 ноября 2015 г. N1327;
- приказом Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- учебными планами (очной и заочной форм обучения) по направлению подготовки 38.03.01 Экономика.

Рабочая программа дисциплины «Информационная безопасность». – Н.Новгород:НИ(ф) МГЭУ, 2018. – 32 с.

№ 4793

Разработчик:

Преподаватель кафедры общегуманитарных дисциплин НИ(ф) АНО ВО МГЭУ, к.э.н.		П.С. Шалабаев
Должность, ученая степень, ученое звание	*подпись*	*И.О. Фамилия*

Рецензент:

Профессор кафедры прикладной математики НИТПУ, д.т.н, профессор		О.Г. Берестнева
Должность, ученая степень, ученое звание	*подпись*	*И.О. Фамилия*

Рабочая программа дисциплины рассмотрена на заседании кафедры математики и информатики (протокол от 11.03.2019 №8).

Заведующий кафедрой д.т.н., профессор А.М. Сидоренко

СОДЕРЖАНИЕ

1. **Цели и задачи обучения по дисциплине**

Цель обучения по дисциплине «Информационная безопасность» – ознакомление обучающихся с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и, конечно, методов их применения.

Задачи изучения дисциплины «Информационная безопасность»:

- сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

1. **Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы**

Процесс изучения дисциплины «Информационная безопасность» направлен на формирование у обучающихся по программе высшего образования – программе бакалавриата по направлению подготовки 38.03.01 Экономика, направленность (профиль) «Финансы и кредит» компетенций ОК-6 и ОПК-1.

Код и описание компетенции	**Планируемые результаты обучения по дисциплине «Информационная безопасность»**
ОК-6 способность использовать основы правовых знаний в различных сферах жизнедеятельности	Знать: нормативно-правовые документы, применяемые в профессиональной деятельности.
	Уметь: использовать нормативно-правовые документы в практической деятельности.
	Владеть: навыками работы с нормативно-правовыми документами.
ОПК-1 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: систему категорий и методов, направленных на формирование аналитического и логического мышления бухгалтера; основные математические и статистические методы обработки данных, полученных при решении основных профессиональных задач, основы библиографической и информационно-поисковой работы.
	Уметь: анализировать и оценивать профессиональную информацию, обобщать, строить выводы, использовать данные поисковой системы при решении профессиональных задач и оформлении научных статей, отчетов, заключений и пр.
	Владеть: навыками управления информацией, составления и оформления отчетов, заключений и т.д.; навыками решения типовых задач в различных областях профессиональной практики (навыками анализа своей деятельности как профессионального бухгалтера с целью оптимизации собственной деятельности, навыками использования в профессиональной деятельности базовых знаний информатики и современных информационных технологий.

2. **Место дисциплины в структуре образовательной программы**

Дисциплина Б1.Б.10 «Информационная безопасность» реализуется в рамках базовой части Блока I «Дисциплины (модули)» программы бакалавриата.

Дисциплина «Информационная безопасность» является начальным этапом формирования компетенции ОПК-1, в процессе освоения ОПОП, и предшествует изучению дисциплины «Автоматизированные информационные технологии в экономике», а также прохождению учебной и производственной практик, также формирующих данные компетенции.

Дисциплина «Информационная безопасность» является начальным этапом формирования компетенции ОК-6, в процессе освоения ОПОП, основывается на знаниях обучающихся полученных в ходе изучения дисциплины «Правоведение» и предшествует защите выпускной квалификационной работы.

В качестве промежуточной аттестации по дисциплине предусмотрен зачет, который входит в общую трудоемкость дисциплины.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебной работы) и на самостоятельную работу обучающихся

Согласно учебным планам общая трудоемкость дисциплины «Информационная безопасность» составляет 2 зачетные единицы (72 часа).

Очная форма обучения

Вид учебной работы	Всего часов	Семестр
		2
Контактная работа* (аудиторные занятия) всего, в том числе:	**36**	**36**
лекции	18	18
практические занятия	18	18
Самостоятельная работа*	36	36
Промежуточная аттестация - зачёт	**зачет**	**зачет**
Общая трудоемкость	**72**	**72**

Заочная форма обучения

Вид учебной работы	Всего часов	Семестр
		1
Контактная работа* (аудиторные занятия) всего, в том числе:	**8**	**8**
лекции	4	4
практические занятия	4	4
Самостоятельная работа*	**60**	**60**
Промежуточная аттестации - зачёт	**4**	**4**
Общая трудоемкость	**72**	**72**

* для обучающихся по индивидуальному учебному плану количество часов контактной и самостоятельной работы устанавливается индивидуальным учебным планом.[1]

Дисциплина реализуется посредством проведения учебных занятий (включая проведение текущего контроля успеваемости) и промежуточной аттестации обучающихся. В соответствии с рабочей программой и тематическим планом изучение дисциплины проходит в форме контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся. При реализации дисциплины предусмотрена аудиторная контактная работа и внеаудиторная контактная работа посредством электронной информационно-

[1] Примечание: для обучающихся по индивидуальному учебному плану - учебному плану, обеспечивающему освоение соответствующей образовательной программы на основе индивидуализации ее содержания с учетом особенностей и образовательных потребностей конкретного обучающегося (в том числе при ускоренном обучении, для обучающихся с ограниченными возможностями здоровья и инвалидов).

образовательной среды. Учебный процесс в аудитории осуществляется в форме лекций и практических занятий. В лекциях раскрываются основные темы изучаемого курса, которые входят в рабочую программу. На практических занятиях более подробно изучается программный материал в плоскости отработки практических умений и навыков и усвоения тем. Внеаудиторная контактная работа включает в себя проведение текущего контроля успеваемости (тестирование) в электронной информационно-образовательной среде.

4. Содержание дисциплины, структурированное по темам, с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий

Тематический план для очной формы обучения

№	Наименование темы	Количество часов по учебному плану	Количество аудиторных часов	Из них, час		Самостоятельная работа	Формируемые компетенции
				лекции	практические занятия		
1	2	3	4	5	6	7	8
Раздел I. Основы информационной безопасности							
1	Понятие информационной безопасности. Основные составляющие	4	2	2*		2	ОПК-1 ОК-6
2	Объектно-ориентированный подход к рассмотрению защищаемых систем	4	2	2		2	ОПК-1 ОК-6
3	Наиболее распространенные угрозы информационной безопасности и её составляющие	6	4	2	2	2	ОПК-1 ОК-6
Раздел II. Уровни информационной безопасности							
4	Законодательный уровень информационной безопасности	6	4	2*	2	2	ОПК-1 ОК-6
5	Административный уровень информационной безопасности	6	4	2	2	2	ОПК-1 ОК-6
6	Процедурный уровень информационной безопасности	6	4	2	2	2	ОПК-1 ОК-6
Раздел III. Программно-технические меры по обеспечению информационной безопасности							
7	Основные характеристики программно-технических мер	8	4	2	2	4	ОПК-1 ОК-6
8	Идентификация и аутентификация	10	4	2	2*	6	ОПК-1 ОК-6
9	Протоколирование и аудит, шифрование, контроль целостности	10	4	2	2*	6	ОПК-1 ОК-6
10	Экранирование, анализ защищенности	6	2		2	4	ОПК-1
11	Обеспечение высокой доступности	6	2		2	4	ОПК-1
	Зачет	-	-	-	-	-	ОПК-1 ОК-6
	Всего за семестр	**72**	**36**	**18/4***	**18/4***	**36**	

* - темы, изучаемые в интерактивных формах обучения

Формы учебных занятий с использованием активных и интерактивных технологий обучения

№	Наименование разделов (тем), *в которых используются активные и/или интерактивные образовательные технологии*	Образовательные технологии
1.	Лекция Тема 1. Понятие информационной безопасности. Основные составляющие.	*лекция-беседа* (диалог с обучающимися в ходе изложения материала, предполагающий актуализацию прежних знаний обучающихся и побуждающий к самостоятельному размышлению)
2.	Лекция Тема 4. Законодательный уровень информационной безопасности.	*лекция-беседа* (диалог с обучающимися в ходе изложения материала, предполагающий актуализацию прежних знаний обучающихся и побуждающий к самостоятельному размышлению)
3.	Практическое занятие Тема 8. Идентификация и аутентификация.	*работа в малых группах* (выполнение практических заданий в группах 2 – 5 человек позволяет практиковать навыки сотрудничества, межличностного общения, распределения ролей участия)
4.	Практическое занятие Тема 9. Протоколирование и аудит, шифрование, контроль целостности.	*работа в малых группах* (выполнение практических заданий в группах 2 – 5 человек позволяет практиковать навыки сотрудничества, межличностного общения, распределения ролей участия)

Тематический план для заочной формы обучения

№	Наименование темы	Количество часов по учебному плану	Количество аудиторных часов	Из них, час		Самостоятельная работа	Формируемые компетенции
				лекции	практические занятия		
1	2	3	4	5	6	7	8
Раздел I. Основы информационной безопасности							
1	Понятие информационной безопасности. Основные составляющие	6	2	2		4	ОПК-1 ОК-6
2	Объектно-ориентированный подход к рассмотрению защищаемых систем	4				4	ОПК-1 ОК-6
3	Наиболее распространенные угрозы информационной безопасности и её составляющим	4				4	ОПК-1 ОК-6
Раздел II. Уровни информационной безопасности							
4	Законодательный уровень информационной безопасности	8	2	2/2*		6	ОПК-1 ОК-6
5	Административный уровень	6				6	ОПК-1

	информационной безопасности						ОК-6
6	Процедурный уровень информационной безопасности	6				6	ОПК-1 ОК-6
Раздел III. Программно-технические меры по обеспечению информационной безопасности							
7	Основные характеристики программно-технических мер	10	4		4	6	ОПК-1 ОК-6
8	Идентификация и аутентификация	6				6	ОПК-1 ОК-6
9	Протоколирование и аудит, шифрование, контроль целостности	6				6	ОПК-1 ОК-6
10	Экранирование, анализ защищенности	6				6	ОПК-1
11	Обеспечение высокой доступности	6				6	ОПК-1
	Зачет	**4**					ОПК-1 ОК-6
	Всего за семестр	**72**	**8**	**4/2***	**4**	**60**	

* часы занятий, проводимых в активной и интерактивной формах

5.2. Содержание дисциплины, структурированное по темам

РАЗДЕЛ I. Основы информационной безопасности

Тема 1. Понятие информационной безопасности. Основные составляющие (ОПК-1, ОК-6)

Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление*, жизненный цикл информационных систем.

Тема 2. Объектно-ориентированный подход к рассмотрению защищаемых систем (ОПК-1, ОК-6)

Сложные системы. Структурный подход. Объектно-ориентированный подход, класс, объект, метод объекта, инкапсуляция, наследование, полиморфизм, грань объекта, уровень детализации ИС, деление на субъекты и объекты, безопасность повторного использования объектов*, учет семантики*. Операционная система как сервис безопасности*.

Тема 3. Наиболее распространенные угрозы информационной безопасности и её составляющие (ОПК-1, ОК-6)

Основные определения и критерии классификации угроз. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности*.

Раздел II. Уровни информационной безопасности

Тема 4. Законодательный уровень информационной безопасности (ОПК-1, ОК-6)

Российское законодательство в области информационной безопасности. Зарубежное законодательство в области информационной безопасности*. Стандарты и спецификации в области информационной безопасности.

* Для самостоятельного изучения.

Тема 5. Административный уровень информационной безопасности (ОПК-1, ОК-6)

Основные понятия, политика безопасности. Жизненный цикл информационной системы. Синхронизация программы безопасности с жизненным циклом систем*. Управление рисками.

Тема 6. Процедурный уровень информационной безопасности (ОПК-1, ОК-6)

Основные классы мер процедурного уровня. Управление персоналом. Физическая защита*. Поддержание работоспособности. Реагирование на нарушения режима безопасности*. Планирование восстановительных работ.

Раздел III. Программно-технические меры по обеспечению информационной безопасности

Тема 7. Основные характеристики программно-технических мер (ОПК-1, ОК-6)

Основные понятия программно-технического уровня. Архитектурная безопасность. Экранирование. Анализ защищённости. Отказоустойчивость*. Безопасное восстановление.

Тема 8. Идентификация и аутентификация (ОПК-1, ОК-6)

Основные понятия. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos*. Идентификация/аутентификация с помощью биометрических данных*. Управление доступом. Ролевое управление доступом.

Тема 9. Протоколирование и аудит, шифрование, контроль целостности (ОПК-1, ОК-6)

Основные понятия. Активный аудит. Шифрование*. Симметричный метод шифрования. Асимметричный метод шифрования. Секретный и открытый ключ. Криптография. Контроль целостности*. Цифровые сертификаты. Электронная цифровая подпись.

Тема 10. Экранирование, анализ защищенности (ОПК-1)

Основные понятия. Экранирование. Фильтрация. Межсетевые экраны. Классификация межсетевых экранов. Архитектурная безопасность*. Транспортное экранирование. Анализ защищенности. База данных уязвимостей. Сетевой сканер*. Антивирусная защита.

Тема 11. Обеспечение высокой доступности (ОПК-1)

Эффективность услуг. Время недоступности. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Обеспечение обслуживаемости. Туннелирование.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа обучающихся направлена на углубленное изучение разделов и тем рабочей программы и предполагает изучение литературных источников, выполнение домашних заданий и контрольных работ, проведение исследований разного характера.

Работа основывается на анализе литературных источников и материалов, публикуемых в интернете, а также реальных речевых и языковых фактов, личных наблюдений. Также самостоятельная работа включает подготовку и анализ материалов по темам пропущенных занятий.

Самостоятельная работа по дисциплине «Информационная безопасность» включает следующие виды деятельности:

- работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы;
- поиск (подбор) и обзор литературы, электронных источников информации по индивидуально заданной проблеме курса, написание доклада и подготовка презентации, исследовательской работы по заданной проблеме;
- выполнение задания по пропущенной или плохо усвоенной теме;
- выполнение домашней контрольной работы (решение заданий, выполнение упражнений);
- изучение материала, вынесенного на самостоятельную проработку (отдельные темы, параграфы);
- подготовка к практическим занятиям;
- подготовка к зачёту.

№ п/п	Вид учебно-методического обеспечения
1	Общие методические рекомендации по изучению дисциплины «Информационная безопасность» для обучающихся
2	Методические рекомендации по самостоятельной работе и выполнению контрольных работ по дисциплине «Информационная безопасность» для обучающихся
3	Комплекс заданий для текущего контроля успеваемости и критерии оценки выполнения заданий.
4	Задания для промежуточной аттестации по дисциплине и критерии оценки уровня сформированности компетенции.

7. Оценочные материалы для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Порядок, определяющий процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированности компетенций, определен в Положении о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в АНО ВО МГЭУ и институтах (филиалах).

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Этапы формирования компетенций в процессе освоения ОПОП прямо связаны с местом дисциплин в образовательной программе. Каждый этап формирования компетенции характеризуется определенными знаниями, умениями и навыками и (или) опытом профессиональной деятельности, которые оцениваются в процессе текущего контроля успеваемости, промежуточной аттестации по дисциплине (практике) и в процессе государственной итоговой аттестации.

Дисциплина «Информационная безопасность» является начальным этапом формирования компетенции ОПК-1 в процессе освоения ОПОП и предшествует изучению

дисциплины «Автоматизированные информационные технологии в экономике» и прохождению учебной и производственной практик, также формирующих данные компетенции, а также является продолжающим этапом формирования компетенции ОК-6.

В процессе изучения дисциплины компетенции также формируются поэтапно.

Основными этапами формирования компетенций при изучении дисциплины «Информационная безопасность» является последовательное изучение содержательно связанных между собой тем учебных занятий. Изучение каждой темы предполагает овладение обучающимися необходимыми дескрипторами (составляющими) компетенций. Для оценки уровня сформированности компетенций в процессе изучения дисциплины «Информационная безопасность» предусмотрено проведение текущего контроля успеваемости по темам (разделам) дисциплины и промежуточной аттестации по дисциплине – зачёт.

Итоговая оценка уровня сформированности компетенций ОК-6, ОПК-1 определяется в период государственной итоговой аттестации.

7.2. Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

На этапе текущего контроля успеваемости обучающихся по дисциплине «Информационная безопасность» показателями оценивания уровня сформированности компетенций являются результаты тестирования и выполнения практических заданий по темам.

Критерии оценки результатов тестирования и выполнения практических заданий по темам по дисциплине «Информационная безопасность»

% верных решений (ответов)	Шкала оценивания
80-100	5 – «Отлично»
61-89	4 – «Хорошо»
40-60	3 – «Удовлетворительно»
0-39	2 – «Неудовлетворительно»

На этапе промежуточной аттестации по дисциплине **«Информационная безопасность»** показателями оценивания компетенций являются результаты обучения по дисциплине (знает, умеет, владеет).

Показатели оценивания компетенций (ОК-6, ОПК-1)
ОК-6
Знает: • основные правовые понятия, правовые акты Российской Федерации в области защиты информации; • правовые нормы и стандарты по лицензированию в области обеспечения защиты коммерческой и государственной тайны и сертификации средств защиты информации; • руководящие документы по оценке защищенности компьютерных систем; • основные руководящие документы по обеспечению режима и секретности (конфиденциальности)
Умеет: • применять нормативные документы в сфере информационной безопасности и защиты информации при определении категории доступа к информации организации, а также для ее защиты

• выявлять уязвимости активов организации • оценивать состояние организационной защиты информации
Владеет: • навыками определения перечня и режима доступа к сведениям, являющимся коммерческой тайной организации • определения угроз активам организации
ОПК-1
Знает: • основные термины и понятия информационной безопасности • направления обеспечения информационной безопасности • действия, приводящие к незаконному овладению информацией • виды тайн как объекта защиты • компоненты и уровни системы информационной безопасности • порядок защиты информационных активов • основные положения политики информационной безопасности
Умеет: • определять виды активов организации • определять ценность каждого актива организации • формулировать требования к обеспечению сотрудниками защиты информации
Владеет: • навыками определения и ранжирования активов организации • разработками политики информационной безопасности организации

Шкала оценивания, в зависимости от уровня сформированности компетенций

Уровень сформированности компетенций			
«недостаточный» Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы	**«пороговый»** Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	**«продвинутый»** Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	**«высокий»** Компетенции сформированы. Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
Описание критериев оценивания			
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе,	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. -способность устанавливать	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений,

билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «не зачтено»	**Оценка «зачтено»**	**Оценка «зачтено»**	**Оценка «зачтено»**

Оценочный лист результатов обучения по дисциплине

Код компетенции	Уровень сформированности компетенции на данном этапе / оценка
ОК-6	
ОПК-1	
Оценка по дисциплине	

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной.

«Зачтено» выставляется, если все компетенции сформированы на уровне не ниже «порогового».

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций[2]

Тестовые задания к разделу 1 (ОК-6; ОПК-1)

1. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

[2] Оценочные материалы в полном объеме разработаны и утверждены кафедрой, реализующей данную дисциплину, являются составной частью ОПОП.

1. актуальностью информации
2. доступностью
3. качеством информации
4. целостностью

2. Согласно «Оранжевой книге» минимальную защиту имеет группа критериев
1. C
2. A
3. B
4. D

3. Организационные требования к системе защиты
1. управленческие и идентификационные
2. административные и аппаратурные
3. административные и процедурные
4. аппаратурные и физические

4. Основу политики безопасности составляет
1. программное обеспечение
2. управление риском
3. способ управления доступом
4. выбор каналов связи

5. Соответствие средств безопасности решаемым задачам характеризует
1. эффективность
2. корректность
3. адекватность
4. унификация

6. С точки зрения ФСТЭК основной задачей средств безопасности является обеспечение сохранности информации
1. защиты от НСД
2. простоты реализации
3. надежности функционирования

7. Согласно «Европейским критериям» формальное описание функций безопасности требуется на уровне
1. E5
2. E7
3. E4
4. E6

8. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

1. аудит
2. аутентификация
3. авторизация
4. идентификация

9. Согласно «Оранжевой книге» уникальные идентификаторы должны иметь
1. наиболее важные субъекты
2. наиболее важные объекты

3. все субъекты
4. все объекты

10. Соответствие средств безопасности решаемым задачам характеризует
1. эффективность
2. корректность
3. адекватность
4. унификация

11. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется
1. системой защиты
2. стандартом безопасности
3. профилем безопасности
4. профилем защиты

12. Для решения проблемы правильности выбора и надежности функционирования средств защиты в «европейских критериях» вводится понятие
1. унификации средств защиты
2. надежности защиты информации
3. адекватности средств защиты
4. оптимизации средств защиты

Тестовые задания к разделу 2 (ОК-6; ОПК-1)

1. Организационные требования к системе защиты
    1. управленческие и идентификационные
    2. административные и аппаратурные
    3. административные и процедурные
    4. аппаратурные и физические

2. Основу политики безопасности составляет
    1. программное обеспечение
    2. управление риском
    3. способ управления доступом
    4. выбор каналов связи

3. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности
    1. Лендвера
    2. С полным перекрытием
    3. Белла-ЛаПадула
    4. На основе анализа угроз

4. Из перечисленного услуга защиты целостности доступна на уровнях: 1) сетевом; 2) транспортном; 3) сеансовом; 4) канальном; 5) прикладном; 6) физическом
1. 1, 2, 5
2. 1, 3, 5
3. 1, 2, 3
4. 4, 5, 6

5. Присвоение субъектам и объектам доступа уникального номера, шифра, ключа и т.п. с целью получения доступа к информации — это

1. идентификация
2. аудит
3. авторизация
4. аутентификация

6. Из перечисленного типами услуг аутентификации являются: 1) идентификация; 2) достоверность происхождения данных; 3) достоверность объектов коммуникации; 4) причастность;
1. 3, 4
2. 1, 4
3. 2, 3
4. 1, 2

7. Как предотвращением неавторизованного использования ресурсов определена услуга защиты
1. аутентификация
2. причастность
3. контроль доступа
8. целостность

9. Пользовательское управление данными реализуется на уровне модели взаимодействия открытых систем
1. представления данных
2. канальном
3. сеансовом
4. прикладном

Тестовые задания к разделу 3 (ОК-6; ОПК-1)

1. Наукой, изучающей математические методы защиты информации путем ее преобразования, является
1. криптоанализ
2. криптология
3. стеганография
4. криптография

2. Конечное множество используемых для кодирования информации знаков называется
1. шифром
2. кодом
3. алфавитом
4. ключом

3. Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей объединяет
1. криптология
2. стеганография
3. криптоанализ
4. криптография

4. Обеспечением скрытности информации в информационных массивах занимается
1. криптография
2. криптоанализ

3. криптология
4. стеганография

5. Два ключа используются в криптосистемах
1. с открытым ключом
2. с закрытым ключом
3. двойного шифрования
4. симметричных

6. Главным параметром криптосистемы является показатель
1. безошибочности шифрования
2. скорости шифрования
3. криптостойкости
4. надежности функционирования

7. Длина исходного ключа в ГОСТ 28147-89 (бит)
1. 128
2. 256
3. 64

8. Основной целью системы брандмауэра является управление доступом
1. к архивам
2. внутри защищаемой сети
3. к секретной информации
4. к защищаемой сети

9. Маршрутизаторы с фильтрацией пакетов осуществляют управление доступом методом проверки
1. адресов отправителя и получателя
2. содержания сообщений
3. электронной подписи
4. структуры данных

10. Из перечисленного система брандмауэра может быть: 1) репитором; 2) маршрутизатором; 3) ПК; 4) хостом; 5) ресивером
1. 3, 4, 5
2. 2, 3, 4
3. 1, 4, 5
4. 1, 2, 3

Типовые практические задания **(ОК-6; ОПК-1)**

Задание 1

1. Придумайте компанию, для которой вы будете разрабатывать нормативное и административно-организационное обеспечение информационной безопасности. Это может быть:

- вымышленная компания;
- компания, где вы работаете;
- компания, по которой планируете выполнять дипломный проект;
- компания, где вы проходили практику;
- компания, описание и данные по которой вы использовали в рамках другого курса;

2. Приведите краткое описание компании:

- название, организационно-правовая форма, учредители
- краткая история компании (год основания, основные этапы развития)
- сфера деятельности
- миссия
- количество сотрудников
- организационная структура (представить в виде рисунка)
- способы ведения бизнеса
- основные конкуренты и конкурентная стратегия
- основные поставщики и потребители (клиенты)
- цели компании на ближайшие год (не менее 5 целей), три года (не менее 5 целей), пять лет (не менее 5 целей).

Задание 2

Определить основные активы компании, занести данные в соответствующую таблицу. Количество активов каждого вида определяется особенностями компании и должно соответствовать информационным потокам компании, а также используемым программным и техническим средствам для их обработки.

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная оценка	Качественная
Информационные активы						
Активы программного обеспечения						
Физические активы						

Задание 3

Провести ранжирование активов по пятибалльной шкале по степени их значимости для компании, выявить наиболее ценные активы. Данные представить в виде таблицы.

Наименование актива	Ценность актива (ранг)

Задание 4

Разработка политики информационной безопасности

1. Ознакомьтесь с прилагаемыми нормативными документами для разработки политики информационной безопасности (ИБ), а также учебным фрагментом политики ИБ компании «Ин Техно» (в фрагменте представлена общая политика ИБ без указания конкретных деталей, сроков, ответственных лиц и так далее).
2. Разработайте проект политики ИБ для вашей организации. При этом следует акцентировать внимание на следующих аспектах:

- цели политики ИБ;

- основные принципы;
- на кого будет распространяться эта политика;
- выделение групп пользователей;
- выделение основных видов информационных ресурсов;
- определение уровней доступа (атрибутов безопасности) к информации:
- открыто (О)
- конфиденциально (К)
- секретно (С),
- совершенно секретно (СС)
- особая важность (ОВ)
- определение политики в отношении паролей, в честности:
- повторяемость / неповторяемость паролей
- количество паролей, хранимое системой
- максимальный срок действия пароля
- минимальный срок действия пароля
- минимальная длина пароля
- соответствие требованиям сложности
- параметры блокировки учетных записей (пороговое значение блокировки, время блокировки, сброс счетчика блокировки)
- определение политики в отношении доступа к ресурсам сети Internet, в частности:
- использование доступа к сети Internet в личных целях
- ведение «белого» или «черного» списка сайтов
- временной интервал доступа сети Internet
- объем скачиваемой и загружаемой информации
- возможности использования ресурсов сети Internet различными группами пользователей
- использование почтовых и иных сервисов
- контроль за использованием ресурсов сети Internet
- что разрешено, а что запрещено различным группам пользователей
- рекомендации для пользователей.

Политика ИБ должна отвечать на следующие вопросы

1. Насколько возможно использование интернета в личных целях?
2. Ограничивать ли работу в интернете в нерабочее время?
3. Как решаются вопросы конфиденциальности корпоративной информации?
4. Какое место занимают вопросы безопасности в политике ИБ?
5. На кого распространяется эта политика?
6. Какие права оставляет за собой организация?
7. Какие юридические аспекты необходимо учитывать?
8. Прочие вопросы.

Задание 5.

Обменяйтесь выполненным заданием с вашим одногруппником. Проведите условный анализ выполнения основных задач по обеспечению безопасности на основе полученных данных. Результаты представьте в виде таблицы: **Анализ выполнения основных задач по обеспечению информационной безопасности.**

Основные задачи по обеспечению информационной безопасности	Степень выполнения

Дополнительно опишите ваши замечания по полученным данным, в частности, по оценке информационных активов, рисков, угроз, политики ИБ и так далее.

Критерии оценки результатов выполнения практических заданий по дисциплине «Информационная безопасность»:

% верных решений (ответов)	Шкала оценивания
85-100	5 – «Отлично»
71-84	4 – «Хорошо»
50-70	3 – «Удовлетворительно»
0-49	2 – «Неудовлетворительно»

Вопросы к зачету (ОК-6; ОПК-1)

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
3. Сложные системы. Структурный подход.
4. Основные определения и критерии классификации угроз.
5. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
6. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
7. Российское законодательство в области информационной безопасности.
8. Зарубежное законодательство в области информационной безопасности.
9. Стандарты и спецификации в области информационной безопасности.
10. Основные понятия, политика безопасности.
11. Жизненный цикл информационной системы.
12. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
13. Основные классы мер процедурного уровня.
14. Управление персоналом. Физическая защита.
15. Поддержание работоспособности.
16. Реагирование на нарушения режима безопасности.
17. Планирование восстановительных работ.
18. Основные понятия программно-технического уровня. Архитектурная безопасность.
19. Экранирование. Анализ защищённости.
20. Отказоустойчивость. Безопасное восстановление.
21. Основные понятия криптографии.
22. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации
23. Kerberos.
24. Идентификация/аутентификация с помощью биометрических данных.
25. Управление доступом. Ролевое управление доступом.
26. Активный аудит. Шифрование.
27. Симметричный метод шифрования.
28. Асимметричный метод шифрования.
29. Секретный и открытый ключ.

30. Криптография. Контроль целостности
31. Цифровые сертификаты.
32. Электронная цифровая подпись.
33. Экранирование. Фильтрация. Межсетевые экраны.
34. Классификация межсетевых экранов.
35. Архитектурная безопасность.
36. Транспортное экранирование. Анализ защищенности.
37. Сетевой сканер. Антивирусная защита.

Примерный вариант билета

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2. Архитектурная безопасность.
3. Практическое задание: Провести ранжирование активов по пятибалльной шкале по степени их значимости для компании, выявить наиболее ценные активы. Данные представить в виде таблицы.

Наименование актива	Ценность актива (ранг)

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Информационная безопасность: учебник и практикум для академического бакалавриата / С.А. Нестеров.- М.: Издательство Юрайт, 2018.- 321 с.
2. Мельников В.П. Информационная безопасность : учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева ; под ред. В.П. Мельникова. — М. : РУСАЙНС, 2016. — 354 с. — (Бакалавриат). /ЭБС Book.ru [Электронный ресурс]. - URL: https://www.book.ru/book/920736/view2/1

Дополнительная литература:

1. ВОРОНЦОВА С.В. Информационная безопасность в финансовой сфере : научно-практическое пособие / С.В. Воронцова . – М. : МГЭУ , 2015. - 160 с.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

а) электронные образовательные ресурсы (ЭОР):

1. Министерство образования и науки Российской Федерации [Электронный ресурс] – Режим доступа: https://минобрнауки.рф/
2. Российская государственная библиотека [Электронный ресурс] – Режим доступа: http://www.rsl.ru
3. Образовательные ресурсы сети Интернет: http://book.kbsu.ru; http://koob.ru, http://ihtik.lib.ru, https://elibrary.ru/defaultx.asp
4. Федеральный портал «Российское образование» http://www.edu.ru/
5. Специализированный сайт по тематике информационной безопасности http://all-ib.ru/
6. Официальный сайт Institute of Electrical and Electronics Engineers (IEEE) http://www.ieee.org/index.html
7. Официальный сайт Лаборатории Касперского http://www.kaspersky.ru/

8. Официальный сайт компании Symantec http://www.symantec.com/ru/ru/
9. Официальный сайт сетевой академии Cisco http://cisco.netacad.net
10. Электронная информационно-образовательная среда МГЭУ (лицензия № 978ДО16АР от 28 октября 2016 г. на использование программного обеспечения «ЭИОС»; поставщиком программного обеспечения является ООО «УНИАР»; договор № МГЭИ-У/1-2016 от 01 марта 2016 г.).

б) электронно-библиотечные системы (ЭБС):

№ п/п	Дисциплина	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность/срок действия договора
1.	Информационная безопасность	www.book.ru	Электронно-библиотечная система (ЭБС)	Индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет/ Договор 18491246 срок действия с 14.03.2018-13.03.2019 Договор №18495243 срок действия с 08.02.2019 – 08.02.2020
2.	Информационная безопасность	www.biblioclub.ru	Электронно-библиотечная система (ЭБС) «Университетская библиотека онлайн»	Индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет/ Договор №042-03/2018 срок действия с 15.03.2018-18.03.2019 Договор №12-01/2019 срок действия с 15.01.2019 – 18.03.2020

Обучающимся обеспечен доступ к современным профессиональным базам данных и информационным справочным системам:

Polpred.com - Обзор СМИ https://www.polpred.com/	База данных с рубрикатором: 53 отрасли / 600 источников / 8 федеральных округов РФ / 235 стран и территорий / главные материалы / статьи и интервью 13000 первых лиц. Ежедневно тысяча новостей, полный текст на русском языке. Миллионы сюжетов информагентств и деловой прессы за 15 лет. Интернет-сервисы по отраслям и странам.
Бюро ванДайк (BvD) https://www.bvdinfo.com/ru-ru/home?utm_campaign=search&utm_medium=cpc&u	Бюро ванДайк (BvD) публикует исчерпывающую информацию о компаниях России, Украины, Казахстана и всего мира, а также бизнес-аналитику.

tm_source=google	
Университетская информационная система РОССИЯ https://uisrussia.msu.ru/	Тематическая электронная библиотека и база для прикладных исследований в области экономики, управления, социологии, лингвистики, философии, филологии, международных отношений, права.
Федеральная служба государственной статистики http://www.gks.ru/	Удовлетворение потребностей органов власти и управления, средств массовой информации, населения, научной общественности, коммерческих организаций и предпринимателей, международных организаций в разнообразной, объективной и полной статистической информации – главная задача Федеральной службы государственной статистики. Международная экспертиза признала статистические данные Федеральной службы государственной статистики надежными.
научная электронная библиотека Elibrary http://elibrary.ru/	Научная электронная библиотека eLIBRARY.RU - это крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 26 млн научных статей и публикаций, в том числе электронные версии более 5600 российских научно-технических журналов, из которых более 4800 журналов в открытом доступе
портал Электронная библиотека: диссертации http://diss.rsl.ru/?menu=dissscatalog/	Российская государственная библиотека предоставляет возможность доступа к полным текстам диссертаций и авторефератов, находящимся в электронной форме, что дает уникальную возможность многим читателям получить интересующую информацию, не покидая своего города. Для доступа к ресурсам ЭБД РГБ создаются Виртуальные читальные залы в библиотеках организаций, в которых и происходит просмотр электронных диссертаций и авторефератов пользователями. Каталог Электронной библиотеки диссертаций РГБ находится в свободном доступе для любого пользователя сети Интернет.
сайт Института научной информации по общественным наукам РАН. http://www.inion.ru	Библиографические базы данных ИНИОН РАН по социальным и гуманитарным наукам ведутся с начала 1980-х годов. Общий объём массивов составляет **более 3 млн. 500 тыс. записей** (данные на 1 января 2012 г.). **Ежегодный прирост — около 100 тыс. записей.** В базы данных включаются аннотированные описания книг и статей из журналов и сборников на 140 языках, поступивших в Фундаментальную библиотеку ИНИОН РАН. Описания статей и книг в базах данных снабжены шифром хранения и ссылками на полные тексты источников из

	Научной электронной библиотеки.
Федеральный портал «Российское образование» [Электронный ресурс] – http://www.edu.ru	**Федеральный портал «Российское образование» – уникальный интернет-ресурс в сфере образования и науки.** Ежедневно публикует самые актуальные новости, анонсы событий, информационные материалы для широкого круга читателей. Еженедельно на портале размещаются эксклюзивные материалы, интервью с ведущими специалистами – педагогами, психологами, учеными, репортажи и аналитические статьи. Читатели получают доступ к нормативно-правовой базе сферы образования, они могут пользоваться самыми различными полезными сервисами – такими, как онлайн-тестирование, опросы по актуальным темам и т.д.

10. Методические рекомендации для обучающихся по освоению дисциплины

10.1. Общие методические рекомендации по освоению дисциплины «Информационная безопасность» для обучающихся

В соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.01 Экономика реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий с целью формирования профессиональных навыков обучающихся.

Основными видами учебной работы являются лекционные, практические занятия. Групповое обсуждение и индивидуальные консультации обучающихся в процессе решения учебных задач, в т.ч. посредством телекоммуникационных технологий. Обсуждение конкретных ситуаций. Просмотр и анализ учебных фильмов.

Успешное изучение дисциплины «Информационная безопасность» предполагает целенаправленную работу обучающихся над освоением ее теоретического содержания, предусмотренного учебной программой дисциплины, активное участие в подготовке и проведении активных форм учебных занятий. В связи с этим обучающиеся должны руководствоваться рядом методических указаний.

Во-первых, при изучении дисциплины следует опираться и уметь конспектировать лекции, так как в учебниках, как правило, излагаются общепринятые, устоявшиеся научные взгляды.

Во-вторых, обучающийся обязан целенаправленно готовиться к практическим занятиям.

В-третьих, обучающемуся следует внимательно изучить целевую установку по изучаемой дисциплине и квалификационные требования, предъявляемые к подготовке выпускников, рабочую программу и тематический план. Это позволит четко представлять круг изучаемых дисциплиной проблем, ее место и роль в подготовке бакалавра.

В-четвертых, качественное и в полном объеме изучение дисциплины возможно при активной работе в часы самостоятельной подготовки. Обучающийся должен использовать нормативные документы, научную литературу и другие источники, раскрывающие в полном объеме содержание дисциплины. Список основной и дополнительной литературы, сайтов интернета предлагается в рабочей программе. При этом следует иметь в виду, что для глубокого изучения дисциплины необходима литература различных видов:

а) учебники, учебные и учебно-методические пособия, в том числе и электронные;

б) справочная литература – энциклопедии, словари, тематические, терминологические

справочники, раскрывающие категориально-понятийный аппарат дисциплины.

Изучая учебную литературу, следует уяснить основное содержание той или иной проблемы.

Для того, чтобы успешно овладеть содержанием дисциплины «Информационная безопасность» обучающиеся должны выполнить нижеследующие указания:

Методические указания для обучающихся по освоению дисциплины для подготовки к занятиям **лекционного типа**:

В ходе лекционных занятий вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

Методические указания для обучающихся по освоению дисциплины для подготовки к занятиям**:**

Подготовка к занятиям включает 2 этапа: 1-й – организационный;

2-й – закрепление и углубление теоретических знаний. На первом этапе студент планирует свою самостоятельную работу, которая включает: уяснение задания на самостоятельную работу; подбор рекомендованной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку обучающегося к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы обучающийся должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. Каждый участник практических занятий должен быть готовым к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении. Выступление должно строиться свободно, убедительно и аргументированно. Преподаватель следит, чтобы выступление не сводилось к репродуктивному уровню (простому воспроизведению текста), не допускается и простое чтение конспекта. Необходимо, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного. При этом студент может обращаться к записям конспекта и лекций, непосредственно к первоисточникам, факты и наблюдения современной жизни и т. д.

10.2. Методические рекомендации по самостоятельной работе по дисциплине «Информационная безопасность» для обучающихся

Самостоятельная работа обучающихся (СРО) по дисциплине играет важную роль в ходе всего учебного процесса. Методические материалы и рекомендации для обеспечения СРО содержатся в приложении, а также готовятся преподавателем по отдельным темам и выдаются обучающемуся. Для успешного усвоения курса необходимо не только посещать аудиторные занятия, но и вести активную самостоятельную работу. При самостоятельной проработке курса обучающиеся должны:

просматривать основные определения и факты;
повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
изучить рекомендованную основную и дополнительную литературу;
самостоятельно выполнять задания для самостоятельной подготовки;
использовать для самопроверки материалы фонда оценочных средств;
Домашнее задание оценивается по следующим критериям:
степень и уровень выполнения задания;
аккуратность в оформлении работы;
использование специальной литературы;
сдача домашнего задания в срок.
Оценивание домашних заданий входит в накопленную оценку.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационно-справочных систем

В процессе реализации образовательной программы при осуществлении образовательного процесса по дисциплине «Информационная безопасность» применяются **следующие информационные технологии:**

1) презентационные материалы (слайды по всем темам лекционных и практических занятий);
2) доступ в режиме online в Электронную библиотечную систему (ЭБС) www.book.ru;
3) доступ в режиме online в Электронную библиотечную систему (ЭБС) www.biblioclub.ru;
4) доступ в электронную информационно-образовательной среду университета.

Обучающимся МГЭУ обеспечена возможность свободного доступа в электронную информационную образовательную среду (ЭИОС).

Электронная информационно-образовательная среда − это совокупность электронных информационных и образовательных ресурсов, информационных и телекоммуникационных технологий и средств, обеспечивающих освоение обучающемуся образовательных программ.

ЭИОС МГЭУ обеспечивает:

а) доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочей программе;

б) фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы бакалавриата;

в) проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

г) формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;

д) взаимодействие между участниками образовательного процесса, в том числе синхронное и/или асинхронное взаимодействие посредством сети «Интернет»;

е) демонстрацию дидактических материалов дисциплины через LCD-проектор;

ж) доступ к программам текущего контроля успеваемости и промежуточной аттестации: «Тестер знаний» и Интернет-тренажеры в сфере образования (http://www.i-exam.ru).

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих.

Программное обеспечение:

1. Ежегодно обновляемое лицензионное ПО

MS Windows 7 Professional; MS Windows XP.
Microsoft Office 2007.
Dr. Web (версия 11.00).

2. Свободно распространяемое ПО

7-Zip
K-Lite Codec Pack
Adobe Reader

Информационно-справочные системы:

Информационно-справочная система «Консультант Плюс» – www.consultant.ru

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия, текущий контроль успеваемости и промежуточная аттестация по данной дисциплине проводятся в учебных аудиториях для занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Данные учебные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Типовая комплектация таких аудиторий состоит из комплекта мебели для обучающихся и преподавателя, доски маркерной/для мела, инструкции пожарной безопасности, огнетушителя. Занятия лекционного типа проводятся в аудиториях, оснащённых стационарным или переносным мультимедийным оборудованием.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий (презентации по темам интерактивных лекций и практических занятий), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей персональный компьютер (с техническими характеристиками не ниже Intel Core i5-2100), блок управления оборудованием. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в

удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения отдельных корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение:

MS Windows 7 Professional; MS Windows XP.
Microsoft Office 2007.
7-Zip Свободно распространяемое ПО.
K-Lite Codec Pack Свободно распространяемое ПО.
Dr. Web (версия 11.00).
Adobe Reader XI Свободно распространяемое ПО.

Типовая комплектация аудитории, оснащённой переносным мультимедийным оборудованием состоит из: комплекта мебели для обучающихся и преподавателя, доски маркерной/для мела, инструкции пожарной безопасности, огнетушителя, переносного мультимедийного (компьютерного) оборудования (ноутбука, проектора, колонок). Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение:

MS Windows 7 Professional; MS Windows XP.
Microsoft Office 2007.
7-Zip Свободно распространяемое ПО.
K-Lite Codec Pack Свободно распространяемое ПО.
Dr. Web (версия 11.00).
Adobe Reader XI Свободно распространяемое ПО.

Качественный и количественный состав оборудования определяется спецификой данной дисциплины и имеет своё отражение в справке о материально-техническом обеспечении основной образовательной программы высшего образования – программы бакалавриата (Приложение 12)

Также предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.

Для организации **самостоятельной работы** обучающихся используется:

- библиотечный фонд вуза, расположенный по адресу: шоссе Сормовское, 20 (каб. №522);
- читальный зал, учебная аудитория для самостоятельной работы, для курсового проектирования №520.
  Доска 3-х элем. меловая (1 шт.). Стол уч. м/к (3 шт.). Стол письм. дер. (8 шт.). Стол компьют. 90х72 (18 шт.). Стул «Сатурн» сер. (36 шт.). Трибуна метал.(1 шт.). Стеллаж м/к корич. 900х320х1900 (1 шт.).

Компьютеры для обучающихся ПК Dual-Core E5300 2.6GHZ (19 шт.) с выходом в Интернет и ЭИОС; монитор Samsung SyncMaster E1920NR (19 шт.); мышь компьютерная (19 шт.); клавиатура (19 шт.); колонки компьютерные (1 шт.); проектор Epson EB-X14G (1 шт.); экран настенный 180х180 (1 шт.).

Программное обеспечение: MS Windows XP, MS Office 2007 лицензия №48131620. Дата выдачи лицензии: 22.02.2011. Срок действия лицензии: бессрочно. Dr.Web (версия 11.00) лицензия №G6SS-D3BK-7TA2-XS96. Дата выдачи лицензии: 11.05.2018. Срок действия лицензии: 1 год.

Информационно-справочная система:
«КонсультантПлюс».

13. Средства адаптации образовательного процесса по дисциплине к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ)

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ОВЗ:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества;
- создание возможности для обучающихся воспринимать одну и ту же информацию из разных источников – например, так, чтобы лица с нарушением слуха получали информацию визуально, с нарушением зрения – аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счет альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, выступлений с докладами и защитой выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ОВЗ форм промежуточной аттестации по отношению к установленной продолжительности их сдачи: зачет и экзамен, проводимые в письменной форме, - не более чем на 90 мин., проводимые в устной форме – не более чем на 20 мин.,
- продолжительность выступления обучающегося при защите курсовой работы – не более чем на 15 мин.

Университет устанавливает конкретное содержание рабочих программ дисциплин и условия организации и проведения конкретных видов учебных занятий, составляющих контактную работу обучающихся с преподавателем и самостоятельную работу обучающихся с ограниченными возможностями здоровья, инвалидов (при наличии факта зачисления таких обучающихся с учетом конкретных нозологий).

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ
рабочей программы дисциплины
«Информационная безопасность»

Рабочая программа дисциплины рассмотрена на заседании кафедры общегуманитарных дисциплин, математики и информатики (протокол от 11.03.2019 №8) и одобрена на заседании Совета Института (протокол от 11.03.2019 №8) для исполнения в 2018-2019 учебном году

Внесены дополнения (изменения):в Перечень договоров ЭБС (за период, соответствующий сроку получения образования по ООП) за 2018-2019 уч. г.:

1. Договор №18495243 на оказание услуг по предоставлению доступа к Электронно-библиотечной системе «book.ru». «КноРус медиа», г. Москва. Срок действия с «08» февраля 2019г. по «08» февраля 2020г.

2. Договор №012-01/2019 об оказании информационных услуг. Электронно-библиотечная система (ЭБС) «Университетская библиотека онлайн». ООО «Современные цифровые технологии», г. Москва. Срок действия с «15» января 2019г. по «18» марта 2020г

Заведующий кафедрой

А.М. Сидоренко
(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от_____ №___) и одобрена на заседании Ученого совета (протокол от _____ №____) для исполнения в 20__-20__ учебном году

Внесены дополнения (изменения): _____
_____
_____
_____

Заведующий кафедрой

_____
(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от_____ №___) и одобрена на заседании Ученого совета (протокол от _____ №____) для исполнения в 20__-20__ учебном году

Внесены дополнения (изменения): _____
_____
_____
_____

Заведующий кафедрой

_____
(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от_____ №___) и одобрена на заседании Ученого совета (протокол от _____ №____) для исполнения в 20__-20__ учебном году

Внесены дополнения (изменения): _____
_____

Заведующий кафедрой

_____
(подпись, инициалы и фамилия)

ШАЛАБАЕВ ПАВЕЛ СЕРГЕЕВИЧ

Р А Б О Ч А Я П Р О Г Р А М М А
Д И С Ц И П Л И Н Ы

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки
38.03.01 Экономика

Направленность (профиль) основной профессиональной образовательной программы прикладного бакалавриата «Финансы и кредит»

Печатается в авторской редакции
Корректор Афиногенова Е.В,

НИ(ф) МГЭУ, Нижний Новгород, 603074, шоссе Сормовское., д. 20