

Частное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ
УПРАВЛЕНИЯ И ЭКОНОМИКИ»

РАССМОТРЕНО И ОДОБРЕНО

На заседании кафедры информацион-
ных технологий и математики
Протокол № 9 от 25.05.2023

УТВЕРЖДАЮ

Первый проректор
Авдашкевич С.В.
28.06.2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина:	Б1.В.ДВ.04.02 Информационная безопасность и защита информации
Направление подготовки:	38.03.01 Экономика
Направленность (профиль):	«Международные финансы»
Уровень высшего образования:	бакалавриат
Программа:	академического бакалавриата
Форма обучения:	очная
Разработчики:	Кандидат экономических наук, доцент Удахина С.В

1. Цели и задачи дисциплины:

Цель дисциплины: формирование студентами методически правильных основ знаний и практических навыков по основам информационной безопасности (ИБ), необходимых выпускникам университета, занимающимся эксплуатацией корпоративных информационных систем.

Задачи дисциплины:

- получение студентами необходимых для их работы теоретических знаний о современных средствах, методах и технологиях обеспечения информационной безопасности корпоративных информационных систем;
- формирование студентами практических навыков организации работ по обеспечению основ информационной безопасности и защиты информации на предприятиях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы высшего образования

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Содержание компетенции
ПК-4	способностью на основе описания экономических процессов и явлений строить стандартные теоретические и эконометрические модели, анализировать и содержательно интерпретировать полученные результаты
ПК-7	способностью, используя отечественные и зарубежные источники информации, собрать необходимые данные проанализировать их и подготовить информационный обзор и/или аналитический отчет
ПК-8	способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии
ПК-10	способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии

Планируемые результаты обучения:

Код компетенции	Основные признаки освоения		
	Знать	Уметь	Владеть
ПК-4	- закономерности и принципы функционирования социально-экономических систем; - взаимосвязь безопасности и экономических интересов общества и государства; - современные информационные технологии и закономерности и принципы, используемые для создания систем безопасности.	- применять понятия и методы экономической науки при изучении проблем экономической информационной безопасности; - использовать закономерности и принципы функционирования социально-экономических систем в решении задач управления организацией; - при анализе деятельности хозяйствующих субъектов определять возможные источники угроз его внешней и внутренней безопасности.	- навыками использования понятий и методов экономической теории при исследовании проблем информационной безопасности; - навыками применения законов и принципов управления организацией; - навыками построения аналитических моделей учетной информации и финансовой отчетности для принятия обоснованных решений и предупреждения, локализации и нейтрализации угроз информационной безопасности.
ПК-7	- принципы и методы сбора данных из различных источников экономической информации; - современные методы анализа данных, полученных из	- использовать адекватные методы сбора данных из различных источников экономической информации;	- навыками использования современных методов и средств получения данных из различных источников; - современными средствами анализа и отбора данных,

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

	<p>отечественных и зарубежных источников информации; - приёмы формирования информационных обзоров и аналитических расчетов на основе отечественных и зарубежных источников информации в сфере обеспечения безопасности данных.</p>	<p>- использовать современные методы анализа данных, полученных из отечественных и зарубежных источников информации; - использовать средства и приёмы формирования информационных обзоров и аналитических расчетов на основе отечественных и зарубежных источников информации.</p>	<p>полученных из различных источников информации; - навыками анализа и подготовки информационных обзоров и проведения аналитических расчетов в области защиты информации.</p>
ПК-8	<p>- основные современные технические средства и информационные технологии для решения аналитических и исследовательских задач в экономической области; - основы функционирования безопасности информационных систем; - методы и средства защиты информационной безопасности.</p>	<p>- использовать основные современные технические средства и информационные технологии для решения аналитических и исследовательских задач в экономической области; - оценивать и выбирать необходимые средства защиты информации; - использовать современные вычислительные и коммуникационные средства и информационные технологии для решения аналитических и исследовательских задач в экономической области; - осваивать перспективные информационные технологии.</p>	<p>- навыками использования современных технических средств и информационных технологий для решения аналитических и исследовательских задач в экономической области; - навыками определения классов защищенных систем по совокупности мер защиты; - теоретическими знаниями и практическими навыками, позволяющих ориентироваться в области информационных технологий.</p>
ПК-10	<p>- основные современные технические средства и информационные технологии для решения коммуникативных задач; - задачи программно-технического обеспечения информационной безопасности; - виды угроз ИС и методы обеспечения информационной безопасности.</p>	<p>- использовать основные современные технические средства и информационные технологии для решения коммуникативных задач; - проводить анализ предметной области, выявлять информационные потребности и разрабатывать требования к ИС; - осуществлять выбор и использовать современные технические средства, информационные технологии для решения коммуникативных задач; - осваивать перспективные информационные технологии в области телекоммуникации.</p>	<p>- навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах; - навыками использования современных технических средств и информационных технологий для решения коммуникативных задач; - прикладными и инструментальными средствами создания систем информационной безопасности.</p>

3. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» входит в Блок 1 «Дисциплины (модуля)» (Вариативная часть) образовательной программы высшего образования по направлению 38.03.01 Экономика направленность (профиль) «Международные финансы».

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые формируются в процессе изучения следующих дисциплин (практик):

Стратегический менеджмент

Знания, умения и навыки, приобретенные в процессе изучения данной дисциплины, будут использованы обучающимся при изучении дисциплин (практик):

Методы принятия управленческих решений, Английский язык международных документов и дипломатической переписки, Методы научных исследований, Учебная практика: практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности, Деньги, кредит, банки, Иностраный язык (второй), Финансовое планирование и бюджетирование, Актуальные вопросы экономики, управления и финансов, Логистика, Управление проектами, Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности, Международный менеджмент, Международные валютно-кредитные и финансовые отношения, Международные финансы, Экономическая психология, Экономика персонала, Банковский маркетинг, Управление продажами, Лидерство, Управление человеческими ресурсами, Производственная практика: научно-исследовательская работа, Производственная практика: преддипломная практика

4. Объем дисциплины

Очная форма обучения:

Вид учебной работы	Всего часов	Семестр
		3
Аудиторные занятия (АЗ):	54	54
В том числе:		
Лекционные занятия (Лек)	18	18
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	36	36
Самостоятельная работа студента (СР)	57	57
В том числе:		
Курсовая работа	0	0
Другие виды самостоятельной работы*	57	57
Контроль самостоятельной работы (КСР)	6	6
Контактная работа (КоР)	60	60
Форма промежуточной аттестации		Экзамен
Подготовка к экзамену и сдача экзамена (СР, КоР)	27	27
Общая трудоемкость дисциплины, часы/ЗЕТ	144/4	144/4

* - подготовка к аудиторным занятиям, подготовка к зачету (при наличии).

5. Содержание дисциплины

Очная форма обучения:

№ п/п	Наименование темы дисциплины	Се- местр/ Курс	Количество учебных часов			СР	Практическая подготовка*
			В том числе по видам аудиторных занятий				
			Лек	Пр	Лаб		

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

1	Основные направления формирования информационной безопасности современного предприятия.	3	4	8	0	14	8
2	Защищенная информационная система. Уровни и структура информационной безопасности.	3	4	8	0	14	8
3	Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.	3	4	10	0	14	10
4	Технологии и методы обеспечения информационной безопасности. Комплексная защита информационных систем.	3	6	10	0	15	10
Итого:			18	36	0	57	36

* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия обучающихся, курсовая работа	Компетенции	Оценочное средство текущего контроля
1	2	3	4
Тема 1: Основные направления формирования информационной безопасности современного предприятия.	Предпосылки становления предметной области информационной безопасности. Ключевые вопросы информационной безопасности. Концепция информационной безопасности Российской Федерации. Разработка корпоративной концепции информационной безопасности Правовые аспекты информационной безопасности. Международное и российское законодательство в сфере информационной безопасности Практические занятия/ Самостоятельная работа: Основные вопросы информационной безопасности. Международное законодательство в сфере информационной безопасности. Корпоративная концепция информационной безопасности. Лабораторная работа: -	ПК-4, ПК-7; ПК-8; ПК-10	Тестирование №1
Тема 2: Защищенная информационная система. Уровни и структура информационной безопасности.	Виды защищаемой информации. Модель угроз и модель информационной безопасности Понятие защищенной информационной системы. Программа информационной безопасности. Организационно-распорядительные документы в сфере информационной безопасности. Политика информационной безопасности. Практические занятия/ Самостоятельная работа: Модели угроз и информационной безопасности. Программа и политика информационной безопасности на международном рынке. Лабораторная работа: -	ПК-4, ПК-7; ПК-8; ПК-10	Тестирование №2; Доклады №1
Тема 3: Модели и стандарты в сфере информационной безопасности и	Управление информационными рисками. Стандартизация в сфере информационной безопасности. Практические занятия/ Самостоятельная работа: Управление информационными рисками в области международных финансов	ПК-4, ПК-7; ПК-8; ПК-10	Коллоквиум №1

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

управления рисками информационной безопасности.	Лабораторная работа: -		
Тема 4: Технологии и методы обеспечения информационной безопасности. Комплексная защита информационных систем.	Защита информационной инфраструктуры от атак. Антивирусные средства защиты. Оценка эффективности средств защиты информации. Практические занятия/ Самостоятельная работа: Антивирусные средства защиты информационной безопасности. Комплексная защита информационной инфраструктуры и ресурсов в сфере международных финансов. Лабораторная работа: -	ПК-4, ПК-7; ПК-8; ПК-10	Коллоквиум №2
Курсовая работа	Не предусмотрено учебным планом		

6. Формы проведения занятий

При реализации дисциплины применяются инновационные формы учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, принятия решений, лидерские качества.

Очная форма обучения:

№ п/п	Наименование темы/ лекционного (практического) занятия	Тип занятия	Кол-во часов	Форма проведения занятий
1	Основные направления формирования информационной безопасности современного предприятия.: Основные вопросы информационной безопасности. Международное законодательство в сфере информационной безопасности. Корпоративная концепция информационной безопасности.	Пр	8	Конференция
2	Модели и стандарты в сфере информационной безопасности и управления рисками информационной безопасности.: Управление информационными рисками в области международных финансов.	Пр	10	Дискуссия

7. Способ реализации дисциплины

Без использования онлайн-курса.

8. Учебно-методическое обеспечение дисциплины:

Основная литература:

Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2023. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519780>

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/495922>

38.03.01 Экономика, направленность «Международные финансы»
Программа академического бакалавриата
Рабочая программа дисциплины
Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
Форма обучения: очная
Разработана для приема 2019/2020, 2020/2021 учебного года
Обновлена на 2023/2024 учебный год

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511998>

Дополнительная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490277>

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844>

3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2023. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/520063>

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения

1. Операционная система
2. Пакет прикладных офисных программ
3. Антивирусное программное обеспечение
4. Oracle VM Virtualbox

Дополнительно при применении электронного обучения, дистанционных образовательных технологий используются:

1. LMS Moodle
2. Вебинарная платформа

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», информационных справочных систем и профессиональных баз данных, необходимых для освоения дисциплины

1. ibooks.ru : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: <https://ibooks.ru>. - Текст: электронный

2. Электронно-библиотечная система СПбУТУиЭ : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: <http://libume.ru>. - Текст: электронный

3. Юрайт : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: <https://urait.ru>. - Текст: электронный

4. [eLibrary.ru](http://elibrary.ru) : научная электронная библиотека [Электронный ресурс] : профессиональная база данных. - Режим доступа: <http://elibrary.ru>. - Текст: электронный

5. Архив научных журналов НЭИКОН [Электронный ресурс] : профессиональная база данных. - Режим доступа: agch.neicon.ru. - Текст: электронный

6. КиберЛенинка : научная электронная библиотека [Электронный ресурс] : информационная справочная система. - Режим доступа: <http://cyberleninka.ru>. - Текст: электронный

38.03.01 Экономика, направленность «Международные финансы»
Программа академического бакалавриата
Рабочая программа дисциплины
Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
Форма обучения: очная
Разработана для приема 2019/2020, 2020/2021 учебного года
Обновлена на 2023/2024 учебный год

7. Лань : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: <https://e.lanbook.com>. - Текст: электронный

8. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] : профессиональная база данных. - Режим доступа: <https://rkn.gov.ru/>. - Текст: электронный

9. it-world.ru [Электронный ресурс] : информационная справочная система. - Режим доступа: <https://www.it-world.ru/>. - Текст: электронный

10. Бизнес-информатика [Электронный ресурс] : информационная справочная система. - Режим доступа: <https://bijournal.hse.ru/>. - Текст: электронный

11. Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа - практических занятий, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованные: рабочими местами для обучающихся, оснащенными специальной мебелью; рабочим местом преподавателя, оснащенного специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской.

Учебная аудитория для проведения занятий семинарского типа - практических занятий – компьютерный класс, оборудованный рабочими местами для обучающихся, оснащенными специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; рабочим местом преподавателя, оснащенного специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской.

Помещение для самостоятельной работы, оборудованное специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, программным обеспечением.

При применении электронного обучения, дистанционных образовательных технологий используются: виртуальные аналоги учебных аудиторий - вебинарные комнаты на вебинарных платформах, рабочее место преподавателя, оснащенное персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному portalу Университета imeos.ru, веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройства), программным обеспечением; рабочее место обучающегося оснащено персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному portalу Университета imeos.ru, веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройства), программным обеспечением. Авторизация на информационно-образовательном portalе Университета imeos.ru и начало работы осуществляются с использованием персональной учетной записи (логина и пароля).

12. Оценочные материалы по дисциплине

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

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

Очная форма обучения:

Код компетенции	Название дисциплины	Форма промежуточной аттестации	Семестр/курс	Этап формирования компетенции
ПК-4	Стратегический менеджмент	зачет	3	1
ПК-4	Информационное общество и международные отношения	экзамен	3	1
ПК-4	Информационная безопасность и защита информации	экзамен	3	1
ПК-4	Методы научных исследований	зачет	4	2
ПК-4	Учебная практика: практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности	зачет с оценкой	4	2
ПК-4	Деньги, кредит, банки	экзамен	5	3
ПК-4	Финансовое планирование и бюджетирование	экзамен	6	4
ПК-4	Актуальные вопросы экономики, управления и финансов	зачет	6	4
ПК-4	Логистика	экзамен	6	4
ПК-4	Управление проектами	экзамен	6	4
ПК-4	Международный менеджмент	зачет	7	5
ПК-4	Международные валютно-кредитные и финансовые отношения	зачет	7	5
ПК-4	Международные финансы	экзамен	7	5
ПК-4	Банковский маркетинг	экзамен	8	6

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

ПК-4	Управление продажами	экзамен	8	6
ПК-4	Производственная практика: научно-исследовательская работа	зачет с оценкой	8	6
ПК-4	Производственная практика: преддипломная практика	зачет с оценкой	8	6
ПК-7	Информационное общество и международные отношения	экзамен	3	1
ПК-7	Информационная безопасность и защита информации	экзамен	3	1
ПК-7	Методы принятия управленческих решений	экзамен	4	2
ПК-7	Английский язык международных документов и дипломатической переписки	экзамен	4	2
ПК-7	Методы научных исследований	зачет	4	2
ПК-7	Учебная практика: практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности	зачет с оценкой	4	2
ПК-7	Иностранный язык (второй)	экзамен	5	3
ПК-7	Производственная практика: научно-исследовательская работа	зачет с оценкой	8	4
ПК-7	Производственная практика: преддипломная практика	зачет с оценкой	8	4
ПК-8	Информационное общество и международные отношения	экзамен	3	1

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

ПК-8	Информационная безопасность и защита информации	экзамен	3	1
ПК-8	Методы научных исследований	зачет	4	2
ПК-8	Учебная практика: практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности	зачет с оценкой	4	2
ПК-8	Производственная практика: научно-исследовательская работа	зачет с оценкой	8	3
ПК-8	Производственная практика: преддипломная практика	зачет с оценкой	8	3
ПК-10	Информационное общество и международные отношения	экзамен	3	1
ПК-10	Информационная безопасность и защита информации	экзамен	3	1
ПК-10	Английский язык международных документов и дипломатической переписки	экзамен	4	2
ПК-10	Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности	зачет с оценкой	6	3
ПК-10	Экономическая психология	экзамен	7	4
ПК-10	Экономика персонала	экзамен	7	4
ПК-10	Лидерство	экзамен	8	7
ПК-10	Управление человеческими ресурсами	экзамен	8	7

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

ПК-10	Производственная практика: преддипломная практика	зачет с оценкой	8	7
-------	---	-----------------	---	---

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования в процессе изучения дисциплины, описание шкал оценивания

2.1 Текущий контроль

Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.

Выполнение теста оценивается по следующим показателям:

- Правильность выполнения заданий теста за отведенный промежуток времени.

Критерии и шкала оценивания теста

Выполнение заданий теста оценивается по единой схеме, основанной на вычислении коэффициента результативности (КР) учебных достижений. Для этого подсчитывается количество правильных ответов к заданиям теста (А), при этом каждое тестовое задание оценивается в бинарной шкале «правильно – не правильно». Далее фиксируется максимальное количество заданий данного теста (А_{max}).

Величина коэффициента результативности учебных достижений студентов в рамках тестирования вычисляется по следующей формуле: $KP = A / A_{max}$ (значения КР изменяются в пределах от 0 до 1).

Коэффициент результативности (КР)	$KP < 0,4$	$0,4 \leq KP < 0,6$	$0,6 \leq KP \leq 0,8$	$0,8 < KP \leq 1$
Баллы в БРС университета	0	6	8	10
Уровень сформированности компетенций	Не сформирована	Пороговый	Высокий	Повышенный

ДОКЛАД, СООБЩЕНИЕ

Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Показатели и критерии оценивания доклада, сообщения

№ п/п	Показатели оценки	Критерии оценивания
1	Структура (количество слайдов соответствует содержанию и продолжительности выступления, например: для 7-минутного выступления рекомендуется использовать не более 10 слайдов, включая титульный слайд и слайд с выводами)	Каждый из предложенных показателей оценивается по критерию « выполнен - частично выполнен - не выполнен », что соответствует следу-
2	Наглядность (иллюстрации хорошего качества, с четким изображением, текст легко читается, например: используются средства наглядности информации в виде таблиц, схем, графиков и т. д.)	
3	Дизайн и настройка (оформление слайдов соответствует теме, не препятствует восприятию содержания, для всех слайдов презентации используется один и тот же шаблон оформления)	

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

4	Содержание (презентация отражает основные этапы исследования – проблему, цель, гипотезу, ход выполнения работы, выводы, т.е. содержит полную, понятную информацию по теме доклада при наличии орфографической и пунктуационной грамотности)	по общему распределению баллов « 2 балла - 1 балл - 0 баллов »
5	Требования к выступлению (выступающий свободно владеет содержанием, ясно и грамотно излагает материал, выступающий свободно и корректно отвечает на вопросы и замечания аудитории, выступающий точно укладывается в рамки регламента).	

Шкала оценивания доклада

Баллы в БРС Университета	10-9	8-7	6-5	Менее 5
Уровень сформированности компетенции	Повышенный	Высокий	Пороговый	Не сформированы

КОЛЛОКВИУМ

Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.

Коллоквиум оценивается по следующим показателям:

1. Глубокое и прочное усвоение программного материала;
2. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания;
3. Владение разносторонними навыками и приемами выполнения практических работ;
4. Владение профессиональной терминологией;
5. Полный конспект лекционных материалов.

Критерии оценивания коллоквиума

Студент полностью раскрыл содержание материала в объеме, предусмотренном программой, изложил материал грамотным языком в определенной логической последовательности, точно используя терминологию и символику; продемонстрировал сформированность и устойчивость полученных знаний. Возможны одна-две неточности при ответе на дополнительные вопросы, которые студент легко исправил по замечанию преподавателя.	20 баллов
Ответ студента имеет один из недостатков: в изложении вопроса допущены небольшие пробелы, не исказившие содержание ответа; допущены один-два недочета при освещении основного содержания ответа, не исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении дополнительных вопросов, легко исправленные по замечанию преподавателя.	15 баллов
Студент неполно раскрыл содержание вопроса, но показал общее понимание материала и продемонстрировал умения, достаточные для дальнейшего усвоения программного материала; имеет затруднения или допустил ошибки в определении понятий, использовании терминологии и исправил их после нескольких наводящих вопросов преподавателя.	10 баллов
Студент обнаружил полное незнание и непонимание изучаемого учебного материала по дисциплине или не смог ответить ни на один из дополнительных вопросов по изучаемому материалу.	0 баллов

Шкала оценивания коллоквиума

Баллы в БРС Университета	20	15	10	0
Уровень сформированности компетенции	Повышенный	Высокий	Пороговый	Не сформированы

2.2. Курсовая работа

Не предусмотрено учебным планом

2.3. Промежуточная аттестация в форме зачёта

Не предусмотрено учебным планом

2.4. Промежуточная аттестация в форме экзамена

Экзамен проводится в форме группового бланкового тестирования (письменный экзамен). Процедура проведения экзамена изложена в «Положении о текущем контроле успеваемости, промежуточной аттестации и балльно-рейтинговой системе оценки учебных достижений студентов».

Выполнение теста оценивается по следующим показателям:

- Правильность выполнения заданий теста за отведенный промежуток времени.

Критерии и шкала оценивания теста

Выполнение заданий теста оценивается по единой схеме, основанной на вычислении коэффициента результативности (КР) учебных достижений. Для этого подсчитывается количество правильных ответов к заданиям теста (А), при этом каждое тестовое задание оценивается в бинарной шкале «правильно – не правильно». Далее фиксируется максимальное количество заданий данного теста (А_{max}).

Величина коэффициента результативности учебных достижений студентов в рамках тестирования вычисляется по следующей формуле: $KP = A / A_{max}$ (значения КР изменяются в пределах от 0 до 1).

Коэффициент результативности (КР)	КР < 0,4	0,4 ≤ КР < 0,6	0,6 ≤ КР ≤ 0,8	0,8 < КР ≤ 1
Баллы в БРС университета	0	18	24	30
Уровень сформированности компетенций	Не сформирована	Пороговый	Высокий	Повышенный

Баллы по дисциплине*	60 и менее		61-73		74-90		91-100
Итоговая оценка по дисциплине*	Неудовлетворительно		Удовлетворительно		Хорошо		Отлично
Баллы в международной шкале ECTS с буквенным обозначением уровня	<50	51-60	61-67	68-73	74-83	84-90	91-100
	F	Fx	E	D	C	B	A
Уровень сформированности компетенций	Не сформированы		Пороговый		Высокий		Повышенный

*Оценка, полученная студентом за промежуточную аттестацию, выставляется с учетом баллов, полученных за текущий контроль (сумма баллов за экзамен и текущий контроль).

2.5 Описание показателей и критериев оценивания компетенций, сформированных дисциплиной

После выполнения студентом всех видов оценочных средств, указанных в рабочей программе дисциплины, производится оценка уровня сформированности компетенций по дисциплине:

		Основные признаки освоения компетенций
--	--	---

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

		Знать	Уметь	Владеть
ПК-4	Пороговый	- закономерности и принципы функционирования социально-экономических систем.	- применять понятия и методы экономической науки при изучении проблем экономической информационной безопасности.	- навыками использования понятий и методов экономической теории при исследовании проблем информационной безопасности.
	Высокий	- закономерности и принципы функционирования социально-экономических систем; - взаимосвязь безопасности и экономических интересов общества и государства.	- применять понятия и методы экономической науки при изучении проблем экономической информационной безопасности; - использовать закономерности и принципы функционирования социально-экономических систем в решении задач управления организацией.	- навыками использования понятий и методов экономической теории при исследовании проблем информационной безопасности; - навыками применения законов и принципов управления организацией.
	Повышенный	- закономерности и принципы функционирования социально-экономических систем; - взаимосвязь безопасности и экономических интересов общества и государства; - современные информационные технологии и закономерности и принципы, используемые для создания систем безопасности.	- применять понятия и методы экономической науки при изучении проблем экономической информационной безопасности; - использовать закономерности и принципы функционирования социально-экономических систем в решении задач управления организацией; - при анализе деятельности хозяйствующих субъектов определять возможные источники угроз его внешней и внутренней безопасности.	- навыками использования понятий и методов экономической теории при исследовании проблем информационной безопасности; - навыками применения законов и принципов управления организацией; - навыками построения аналитических моделей учетной информации и финансовой отчетности для принятия обоснованных решений и предупреждения, локализации и нейтрализации угроз информационной безопасности.
ПК-7	Пороговый	- основные приёмы сбора данных из отечественных и зарубежных источников информации; - основы анализа данных, полученных из отечественных и зарубежных источников информации; - приёмы формирования информационных обзоров на основе отечественных и зарубежных источников информации.	- проводить сбор данных из отечественных и зарубежных источников информации; - анализировать данные, полученные из различных источников информации; - формировать информационные обзоры на основе отечественных и зарубежных источников информации.	- приемами сбора данных из различных источников экономической информации; - навыками анализа данных, полученных из различных источников экономической информации; - навыками составления информационных обзоров на основе полученной информации.

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

	Высокий	<ul style="list-style-type: none"> - принципы и методы сбора данных из различных источников экономической информации; - методы анализа данных, полученных из отечественных и зарубежных источников информации; - приёмы формирования информационных обзоров и аналитических расчетов на основе отечественных и зарубежных источников информации. 	<ul style="list-style-type: none"> - использовать принципы и методы сбора данных из различных источников экономической информации; - анализировать и выбирать данные, полученные из различных источников информации; - анализировать и готовить информационные обзоры и аналитические расчеты на основе отечественных и зарубежных источников информации. 	<ul style="list-style-type: none"> - навыками сбора данных из различных источников экономической информации; - приёмами анализа и отбора данных, полученных из различных источников информации; - навыками анализа и подготовки информационных обзоров и проведения аналитических расчетов на основе полученных данных.
	Повышенный	<ul style="list-style-type: none"> - принципы и методы сбора данных из различных источников экономической информации; - современные методы анализа данных, полученных из отечественных и зарубежных источников информации; - приёмы формирования информационных обзоров и аналитических расчетов на основе отечественных и зарубежных источников информации в сфере обеспечения безопасности данных. 	<ul style="list-style-type: none"> - использовать адекватные методы сбора данных из различных источников экономической информации; - использовать современные методы анализа данных, полученных из отечественных и зарубежных источников информации; - использовать средства и приёмы формирования информационных обзоров и аналитических расчетов на основе отечественных и зарубежных источников информации. 	<ul style="list-style-type: none"> - навыками использования современных методов и средств получения данных из различных источников; - современными средствами анализа и отбора данных, полученных из различных источников информации; - навыками анализа и подготовки информационных обзоров и проведения аналитических расчетов в области защиты информации.
ПК-8	Пороговый	<ul style="list-style-type: none"> - основные современные технические средства и информационные технологии для решения аналитических и исследовательских задач в экономической области. 	<ul style="list-style-type: none"> - использовать основные современные технические средства и информационные технологии для решения аналитических и исследовательских задач в экономической области. 	<ul style="list-style-type: none"> - навыками использования современных технических средств и информационных технологий для решения аналитических и исследовательских задач в экономической области.
	Высокий	<ul style="list-style-type: none"> - основные современные технические средства и информационные технологии для решения аналитических и исследовательских задач в экономической области; - основы функционирования безопасности информационных систем. 	<ul style="list-style-type: none"> - использовать основные современные технические средства и информационные технологии для решения аналитических и исследовательских задач в экономической области; - оценивать и выбирать необходимые средства защиты информации. 	<ul style="list-style-type: none"> - навыками использования современных технических средств и информационных технологий для решения аналитических и исследовательских задач в экономической области; - навыками определения классов защищенных систем по совокупности мер защиты.
	Повышенный	<ul style="list-style-type: none"> - основные современные технические средства и информационные технологии для решения аналитических и исследовательских задач в экономической области; - основы функционирования безопасности информационных систем; 	<ul style="list-style-type: none"> - использовать основные современные технические средства и информационные технологии для решения аналитических и исследовательских задач в экономической области; 	<ul style="list-style-type: none"> - навыками использования современных технических средств и информационных технологий для решения аналитических и исследовательских задач в экономической области; - навыками определения классов защищенных систем

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

		- методы и средства защиты информационной безопасности.	- оценивать и выбирать необходимые средства защиты информации; - использовать современные вычислительные и коммуникационные средства и информационные технологии для решения аналитических и исследовательских задач в экономической области; - осваивать перспективные информационные технологии.	по совокупности мер защиты; - теоретическими знаниями и практическими навыками, позволяющих ориентироваться в области информационных технологий.
ПК-10	Пороговый	- основные современные технические средства и информационные технологии для решения коммуникативных задач.	- использовать основные современные технические средства и информационные технологии для решения коммуникативных задач.	- навыками использования современных технических средств и информационных технологий для решения коммуникативных задач.
	Высокий	- основные современные технические средства и информационные технологии для решения коммуникативных задач; - задачи программно-технического обеспечения информационной безопасности.	- использовать основные современные технические средства и информационные технологии для решения коммуникативных задач; - проводить анализ предметной области, выявлять информационные потребности и разрабатывать требования к ИС.	- навыками использования современных технических средств и информационных технологий для решения коммуникативных задач; - прикладными и инструментальными средствами создания систем информационной безопасности.
	Повышенный	- основные современные технические средства и информационные технологии для решения коммуникативных задач; - задачи программно-технического обеспечения информационной безопасности; - виды угроз ИС и методы обеспечения информационной безопасности.	- использовать основные современные технические средства и информационные технологии для решения коммуникативных задач; - проводить анализ предметной области, выявлять информационные потребности и разрабатывать требования к ИС; - осуществлять выбор и использовать современные технические средства, информационные технологии для решения коммуникативных задач; - осваивать перспективные информационные технологии в области телекоммуникации.	- навыками работы с программными и аппаратными средствами обеспечивающие защиту информации в компьютерных системах; - навыками использования современных технических средств и информационных технологий для решения коммуникативных задач; - прикладными и инструментальными средствами создания систем информационной безопасности.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Методика формирования оценки по дисциплине. Успеваемость студента оценивается в баллах и состоит из:

- суммы баллов за выполнение заданий текущего контроля (обучающийся может получить в сумме не более 70 баллов);
- баллов за посещаемость (не более 10 баллов);
- баллов за активность на занятиях (занятия в интерактивной форме – п. 6. Формы проведения занятий), выполнение дополнительных заданий и пр. по усмотрению преподавателя, ведущего дисциплину – премиальные баллы (не более 20 баллов).

Полученные итоговые баллы по дисциплине переводятся в оценку по традиционной пяти-балльной шкале оценивания и по 100-балльной шкале оценок Европейской системы перевода и накопления баллов (ECTS) в соответствии с таблицами, представленными в п. Таблицами. 1, 2. Оценки в пятибалльной шкале выставляются в ведомости и зачетные книжки, в 100-балльной – в ведомости.

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности приводятся в соответствующих методических материалах и локальных нормативных актах Университета (Положение «О текущем контроле успеваемости, промежуточной аттестации и балльно-рейтинговой системе оценки учебных достижений студентов», Положение «Об оценочных средствах», Положение «О контроле самостоятельности выполнения письменных работ обучающимися университета с использованием системы «Антиплагиат ВУЗ» и др.).

Уровень сформированности компетенции № 1 (№ N) определяется перечнем оценочных средств:

Оценочное средство (в том числе экзамен, зачет с оценкой при наличии)	Уровень сформированности компетенции*			Средний уровень сформированности компетенций по каждому оценочному средству
	Студент №1	...	Студент № N	
.....			
Итоговый уровень:			

* пороговый, высокий или повышенный

Итоговый (общий/средний) уровень рассчитывается как среднее арифметическое с округлением в сторону более высокого уровня.

Далее делается вывод об общем уровне освоения компетенций студентами в ходе изучения дисциплины:

Оценочный лист по дисциплине

ФИО студента	Уровень сформированности компетенций								
	Общекультурные компетенции			Общепрофессиональные компетенции			Компетенции по видам деятельности		
	№ 1	№ N	Уровень сформированности общекультурных компетенций	№ 1	№ N	Уровень сформированности общепрофессиональных компетенций	№ 1	№ N	Уровень сформированности компетенций по виду деятельности №1
Студент № 1									
Студент № 2									
.....									

4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Темы докладов №1

1. Основные направления и способы защиты информации.
2. Понятия идентификации и аутентификации.
3. Требования к парольной защите.
4. Основные направления технической защиты информации.
5. Понятие технического канала утечки информации.
6. Классификация угроз информационной безопасности по базовым признакам.
7. Угрозы нарушения конфиденциальности.
8. Угрозы нарушения целостности данных.
9. Угрозы отказа служб (угрозы отказа в доступе).
10. Понятие политики безопасности информационных систем. Назначение политики безопасности.
11. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
12. Законодательный уровень обеспечения информационной безопасности.
13. Основные законодательные акты РФ в области защиты информации.
14. Естественные и искусственные угрозы безопасности информации. Уязвимости информационных систем.

Вопросы к коллоквиуму № 1

1. Основные понятия и определения информационной безопасности. Виды информации ограниченного доступа.
2. Цели и задачи защиты информации.
3. Естественные и искусственные угрозы безопасности информации. Уязвимости информационных систем.
4. Основные направления и способы защиты информации.
5. Понятия идентификации и аутентификации.
6. Требования к парольной защите.
7. Основные направления технической защиты информации.
8. Понятие технического канала утечки информации.
9. Угрозы утечки информации по техническим каналам.
10. Характеристики объектов информатизации.
11. Побочные электромагнитные излучения и наводки.
12. Классификация технических каналов утечки информации.
13. Понятие политики безопасности организации.
14. Сертификация средств защиты информации.
15. Категорирование информационных объектов по степени важности и конфиденциальности защищаемой информации.

Дополнительные вопросы на коллоквиуме

1. Программы внутренней защиты. Программы ядра системы безопасности.
2. Интегральная безопасность информационных систем.
3. Комплексная защита объектов.
4. Механические системы защиты.
5. Системы оповещения.

Вопросы к коллоквиуму № 2

1. Аттестация объектов по выполнению требований обеспечения безопасности информации.
2. Основные разделы документов, характеризующих политику безопасности организации.
3. Задачи технических средств защиты информации.
4. Пассивные и активные средства и способы защиты информации.
5. Методы выявления закладочных устройств.
6. Устройства защиты телефонных переговоров. Генераторы пространственного зашумления.
7. Генераторы акустического и виброакустического зашумления.
8. Сетевые фильтры.
9. Подавители диктофонов.

Дополнительные вопросы на коллоквиуме

1. Системы опознавания.
2. Основы физической защиты объектов.
3. Интегральный комплекс физической защиты объектов.

Тестирование №1

- 1) Что входит в понятие “безопасность информации”
 - a) исключение ознакомления с информацией сотрудников АСОИ
 - b) предотвращение ознакомления с информацией лиц к ней не допущенных
 - c) исключение изменений информации
 - d) исключение утечки информации за счет излучений и наводок
- 2) Конфиденциальность информации обеспечивается путем
 - a) содержания критической информации в секрете
 - b) ограничения доступа в специальные помещения
 - c) организации мониторинга сети
- 3) Информационная безопасность информации достигается обеспечением
 - a) конфиденциальности
 - b) доступности
 - c) комплексирования средств ЗИ
 - d) целостности информации
- 4) Защита целостности потоков данных осуществляется с использованием
 - a) дополнительных форм нумерации
 - b) меток времени
 - c) повтором сообщений
 - d) включением дополнительных признаков к сообщению
- 5) Для обеспечения защиты от анализа трафика могут быть использованы

- a) механизм заполнения текста
- b) генерация фиктивных сообщений
- c) ограничение доступа в выделенные помещения
- 6) Если сеть централизованная, то защита должна
 - a) централизованной
 - b) распределенной
- 7) При схеме управления защитой информации "*длинные руки*" полномочия пользователей на каждом компьютере устанавливаются
 - a) администратором удаленно со своего рабочего места
 - b) самим пользователем системы
 - c) пользователем системы после действий администратора безопасности
- 8) Схема отложенного централизованного управления доступом требует, чтобы компьютеры пользователей на момент изменения полномочий были
 - a) включены
 - b) выключены
 - c) безразлично
- 9) Для облегчения работы администратора безопасности по контролю за состоянием безопасности АС необходимо предусмотреть следующие возможности
 - a) селекцию определенных событий из системных журналов
 - b) ограничение перечня событий, регистрируемых СЗИ
 - c) семантическое сжатие данных в журналах регистрации
 - d) автоматическую подготовку отчетных документов
- 10) Реальные возможности нарушителя определяются
 - a) психологическим состоянием нарушителя
 - b) состоянием объекта защиты,
 - c) наличием потенциальных каналов утечки информации,
 - d) качеством средств защиты информации
- 11) В качестве показателя эффективности системы защиты информации может быть использованы
 - a) вероятность обнаружения нарушения
 - b) своевременность реакции на каждый вид нарушения
 - c) доказуемость нарушения
- 12) Для осуществления несанкционированного доступа в информационную систему требуется провести подготовительные действия
 - a) собрать сведения о системе
 - b) выполнить пробные попытки вхождения в систему
 - c) выявить организационную структуру предприятия
- 13) Программы ЦП характеризуются следующими параметрами
 - a) криптостойкостью
 - b) количеством операторов
 - c) временем работы
 - d) функциональными возможностями
- 14) Время работы алгоритма ЦП складывается из времени
 - a) набора текста
 - b) генерации ключей
 - c) проверки подписи
 - d) постановки подписи

- 15) С увеличением криптостойкости системы ЦП временные характеристики
- a) падают
 - b) увеличиваются

Тестирование №2

- 1) Конечная цель защиты информации
 - a) уменьшение возможных точек атак
 - b) сведение к минимуму потерь в управлении
 - c) формирование системы информационной безопасности
 - d) минимизация риска
- 2) Основные принципы построения системы защиты информации
 - a) принцип совместимости средств защиты информации
 - b) принцип непрерывного совершенствования СЗИ
 - c) принцип открытости
 - d) принцип комплексного использования средств защиты
- 3) Принцип непрерывности совершенствования СЗИ заключается в
 - a) постоянном контроле функционирования СЗИ
 - b) выявлении слабых мест в СЗИ
 - c) анализе рынка услуг в области защиты информации
 - d) обновлении и дополнении механизма защиты
- 4) Вероятные угрозы техническому обеспечению
 - a) изменение конфигурации
 - b) изменение маршрутизации
 - c) физический съём информации с каналов
 - d) искажение входных данных
- 5) Вероятные угрозы информационному обеспечению
 - a) Съём и использование выходной информации
 - b) Подмена протоколов
 - c) Изменение топологии
 - d) Перегрузка канала или устройства
- 6) Вероятные угрозы прикладным программам
 - a) ознакомление и изменение программ решения
 - b) изменение прав и полномочий на доступ к ресурсам
 - c) искажение входных данных
- 7) Администратор безопасности
 - a) осуществляет эксплуатацию средств защиты информации
 - b) обеспечивает непрерывность процесса обработки информации
 - c) восстанавливает работоспособность компьютерной системы
 - d) осуществляет допуск в специальные помещения
- 8) В случае возникновения нарушения в компьютерной системе администратор безопасности
 - a) изменяет пароли пользователей
 - b) локализует нарушение
 - c) определяет причину возникновения нарушения
 - d) вызывает представителей МВД
- 9) Источники получения информации для администратора безопасности
 - a) от пользователей

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

- b) из системного журнала
- c) кадровых органов
- 10) Нарушитель это лицо, предпринявшее попытку выполнения запрещенных операций
 - a) по ошибке
 - b) незнанию
 - c) осознанно
 - d) с использованием служебного положения
- 11) Облик нарушителя по совершению противоправных действий определяется
 - a) мотивацией и намерениями,
 - b) совокупностью знаний, умений и навыков (способов) совершения нарушений
 - c) возможностями технических средств снятия информации
 - d) умением пользоваться средствами технической разведки
- 12) Реальные возможности нарушителя определяются
 - a) психологическим состоянием нарушителя
 - b) состоянием объекта защиты,
 - c) наличием потенциальных каналов утечки информации,
 - d) качеством средств защиты информации
- 13) Цифровая подпись это
 - a) полученная хэш-функция
 - b) хэш-функция, прошедшая математическую обработку
 - c) электронная версия фактической подписи
- 14) Цифровая подпись может храниться
 - a) вместе с документом
 - b) в отдельном файле
 - c) в закрытой области памяти
- 15) Проверка ЦП включает в себя проверку соотношения, связывающего
 - a) хэш-функцию и подпись под документом
 - b) подпись под документом и открытый ключ
 - c) хэш-функцию и открытый ключ
 - d) хэш-функцию, подпись и открытый ключ

Перечень вопросов для подготовки к экзамену

<p>ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ И ЭКОНО- МИКИ»</p> <p>Институт экономики менеджмента и информационных технологий Кафедра информационных технологий и математики</p>		
<p>Направление: 38.03.01 Экономика Направленность: «Международные финансы» Дисциплина «Информационная безопасность и защита информации»</p>		<p style="text-align: center;">УТВЕРЖДАЮ</p> <p style="text-align: center;">Заведующий кафедрой _____ И.О. Фамилия «___» _____ 201__ г.</p>

ВАРИАНТ № 1

	Задание	Варианты ответа	К ол-во баллов																								
.	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее, это ...	А. Уязвимость проектирования В. Атака С. Угроза безопасности информации D. Тревога																									
.	Не относится к уровням обеспечения информационной безопасности:	А. нормативно-правовой В. организационный С. социальный D. технический																									
	Принцип, состоящий в том, что ни один сотрудник организации не должен иметь полномочий, позволяющих ему единолично выполнять критичные операции, называется ...	А. Непрерывность защиты В. Разделение функций С. Разумная достаточность D. Персональная ответственность																									
	Не является сервисом безопасности:	А. экранирование В. управление доступом С. туннелирование D. кодирование																									
	Комплекс предупредительных мер по обеспечению ИБ организации, включающий руководящие принципы, правила и процедуры в области безопасности, это ...	А. Программа безопасности В. Политика безопасности С. Кодекс безопасности D. Защита информации																									
	Зашифровать слово БЕЗОПАСНОСТЬ перестановкой согласно таблице. <table border="1" style="margin-left: 20px;"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td> </tr> <tr> <td>5</td><td>8</td><td>6</td><td>11</td><td>1</td><td>10</td><td>9</td><td>4</td><td>3</td><td>12</td><td>2</td><td>7</td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	5	8	6	11	1	10	9	4	3	12	2	7	А. ПНАТЪСООЗЪЕС В. ПНАСБТООЗЪЕС С. ПОАТЪСНОЗЪЕС D. ПНАТЪСООЗЕС	
1	2	3	4	5	6	7	8	9	10	11	12																
5	8	6	11	1	10	9	4	3	12	2	7																
	При моноалфавитной замене получен шифрокод ЗЖРЦ. Расшифровать слово, если известно, что смещение к является нечетным числом.	А. ФЛЭШ В. БАЙТ С. ЛОГИН D. СТЭК																									
	Зашифровать слово НАИФ способом простой замены, используя таблицу. <table border="1" style="margin-left: 20px;"> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> <tr> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td> </tr> </table>																									А. FOID В. AFDX С. FOAD D. AFDU	
	Зашифровать сообщение (2,3) методом RSA, если открытый ключ	А. (27,4) В. (29,9)																									

38.03.01 Экономика, направленность «Международные финансы»
 Программа академического бакалавриата
 Рабочая программа дисциплины
 Дисциплина: Б1.В.ДВ.04.02 Информационная безопасность и защита информации
 Форма обучения: очная
 Разработана для приема 2019/2020, 2020/2021 учебного года
 Обновлено на 2023/2024 учебный год

	$(K_0, N) \rightarrow (7, 33)$.	С. (29,4) D. (29,2)																			
0	Расшифровать криптограмму (3,1) методом RSA, если секретный ключ $(K_c, N) \rightarrow (3, 22)$.	A. (5, 1) B. (7, 5) C. (7, 1) D. (9, 11)																			
1	Зашифровать методом Виженера сообщение ШИФРЫ ЗАМЕНЫ. Ключ – ХАКЕР (Таблицу см. в приложении).	A. МИЮФЛЫАЦКЭР B. МИЮФЛЫАЦЛЭР C. МИЭХЛЫАШКЭР D. МИОХЛЫАЦКЭР																			
2	Определить ключ слова ТЕХНОЛОГИЯ, шифрокод которого по методу Виженера: ФКЯПУХРИТА.	A. ТПК B. ВОЛЬТ C. ВЕК D. СТО E.																			
3	Зашифровать сообщение ИНТЕР- NET способом Гронсфельда. <table border="1" style="margin-left: 20px;"> <tr> <td>№ позиции</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>6</td> <td>7</td> <td>8</td> </tr> <tr> <td>Ключ</td> <td>5</td> <td>2</td> <td>4</td> <td>8</td> <td>1</td> <td>3</td> <td>6</td> <td>7</td> </tr> </table>	№ позиции	1	2	3	4	5	6	7	8	Ключ	5	2	4	8	1	3	6	7	A. МОХЛРПЙШ B. МОЧЛРСЙШ C. НПЦМСРКЦ D. НПЦМКРКЦ	
№ позиции	1	2	3	4	5	6	7	8													
Ключ	5	2	4	8	1	3	6	7													
4	Получить шифрокод слова УНИВЕРСИТЕТ методом гаммирования, если гаммой шифра является ХЕШИРОВАНИЕ.	A. БЗПЙЭЦРЗЬОФ B. БЗСЙЦЭРЗЬОФ C. БЗПЙЦЭРЗЬОФ D. БЗСЙЦЭРТЬОФ																			
5	Определить гамму, если шифрокоду ТЕСТ соответствует информация КРАХ.	A. ХЦТД B. ЧЦТД C. ЧФТД D. ЧЦРД																			