Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
Кафедра Информационных технологий и систем безопасности

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Основная профессиональная образовательная программа
высшего образования по специальности

38.03.05 **«Бизнес-информатика»**

Профиль:
Бизнес-аналитика
Уровень:
Бакалавр

Форма обучения
Очная/ очно-заочная/ заочная

Согласовано
Руководитель ОПОП

_____ Степанов С.Ю.

Председатель УМС
_____ И.И. Палкин
Рекомендовано решением
Ученого совета РГГМУ
19 05 2021 г., протокол
№ 8

Рассмотрена и утверждена на заседании
кафедры Информационных технологий и
систем безопасности
___ июня 2021 г., протокол № ____
И.о. зав. кафедрой Татарникова Т.М.

Автор-разработчик:
Богданов П.Ю./_____
_____/_____

Санкт-Петербург 2021

1. Цель и задачи освоения дисциплины

Цель освоения дисциплины – формирование у студентов комплекса знаний, навыков и компетенций в области информационной безопасности и применения их на практике при организации процессов, хранения, обработки и передачи информации.

Задачи:

- Изучение общих принципов организации защиты информации;
- Освоение принципов оценки защищенности информационных технологий;
- Приобретение знаний в области стандартов и нормативных документов по защите информации;
- Формирование навыков применения типовых средств обеспечения информационной безопасности.

2. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Информационная безопасность» относится к базовой части дисциплин, формируемой участниками образовательных отношений, и является обязательной для изучения дисциплиной при освоении ОПОП по направлению 38.03.05 – «Бизнес-информатика», профиль подготовки – «Бизнес-аналитика»

Дисциплина «Электронная среда и цифровые технологии» изучается на очной форме обучения в 7 семестре, очно–заочной форме обучения в 8 семестре, и заочной форме обучения на 5 году. Для освоения дисциплины «Информационная безопасность», необходимо освоить материал предшествующих дисциплин:

«Информатика»;
«IT-инфраструктура предприятия»;
«Операционные системы»;
«Системное администрирование».

3. Перечень планируемых результатов обучения

Процесс изучения дисциплины направлен на формирование компетенций:
ПК-4

Таблица 1.

Профессиональные компетенции

Код и наименование профессиональной компетенции	**Код и наименование индикатора достижения профессиональной компетенции**	**Результаты обучения**
ПК-4 Способен использовать информационные системы и технологии для автоматизации задач организационного управления и бизнес-процессов.	ПК-4.2 Использует методы и технологии защиты данных.	**Знать:** Требования законодательства в области защиты информации, базовые процессы обеспечения информационной безопасности **Уметь:** Применять технологии обеспечения конфиденциальности, целостности, доступности **Владеть:** методикой построения модели угроз и защиты

Рассмотрено и рекомендовано к использованию в учебном процессе на 2022/2023 учебный год без изменений*

Протокол № 2 заседания кафедры Прикладной информатики от 17.03.2022г.

4. Структура и содержание дисциплины

4.1. Объем дисциплины

Объем дисциплины составляет 3 зачетные единицы, 108 академических часов.

Таблица 2.

Объем дисциплины по видам учебных занятий в академических часах

Объём дисциплины	**Всего часов**		
	Очная форма обучения	**Очно-заочная форма обучения**	**Заочная форма обучения**
Объем дисциплины	**108**	**108**	**108**
Контактная работа обучающихся с преподавателем (по видам аудиторных учебных занятий) – всего:	**42**	**28**	**12**
в том числе:	**-**	**-**	**-**
лекции	**14**	**8**	**4**
занятия семинарского типа:			
практические занятия			
лабораторные занятия	**28**	**20**	**8**
Самостоятельная работа (далее – СРС) – **всего:**	**66**	**80**	**96**
в том числе:	**-**	**-**	**-**
курсовая работа			
контрольная работа			**14**
Вид промежуточной аттестации	**зачет**	**зачет**	**зачет**

4.2. Структура дисциплины

Таблица 3.

Структура дисциплины для очной формы обучения

№	Раздел / тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Формируемые компетенции	Индикаторы достижения компетенций
			Лекции	Практические занятия	СРС			
1	Информационная безопасность	7	2	6	12	Устный опрос, Отчеты по лабораторным работам	ПК-4	ПК-4.2
2	Криптографические методы защиты информации	7	4	10	20	Устный опрос, Отчеты по лабораторным работам	ПК-4	ПК-4.2
3	Правовые аспекты информационной безопасности	7	4	4	18	Устный опрос, Отчеты по лабораторным работам	ПК-4	ПК-4.2
4	Технические методы защиты информации	7	4	8	16	Устный опрос, Отчеты по лабораторным работам	ПК-4	ПК-4.2
	ИТОГО	**-**	**14**	**28**	**66**	**-**	**-**	**-**

Таблица 4.

Структура дисциплины для очно-заочной формы обучения

№	Раздел / тема дисциплины	Семестр	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Формируемые компетенции	Индикаторы достижения компетенций
			Лекции	Практические занятия	СРС			
1	Информационная безопасность	8	2	4	12	Устный опрос, Отчеты по лабораторным работам	ПК-4	ПК-4.2
2	Криптографические методы защиты информации	8	2	6	28	Устный опрос, Отчеты по лабораторным работам	ПК-4	ПК-4.2
3	Правовые аспекты информационной безопасности	8	2	4	18	Устный опрос, Отчеты по лабораторным работам	ПК-4	ПК-4.2
4	Технические методы защиты информации	8	2	6	22	Устный опрос, Отчеты по лабораторным работам	ПК-4	ПК-4.2
	ИТОГО	**-**	**8**	**20**	**80**	**-**	**-**	**-**

Таблица 5.

Структура дисциплины для заочной формы обучения

№	Раздел / тема дисциплины	Год	Виды учебной работы, в т.ч. самостоятельная работа студентов, час.			Формы текущего контроля успеваемости	Формируемые компетенции	Индикаторы достижения компетенций
			Лекции	Практические занятия	СРС			
1	Информационная безопасность	5	1	2	24	Устный опрос, Отчеты по лабораторным работам, контрольная работа	ПК-4	ПК-4.2
2	Криптографические методы защиты информации	5	1	2	24	Устный опрос, Отчеты по лабораторным работам, контрольная работа	ПК-4	ПК-4.2
3	Правовые аспекты информационной безопасности	5	1	2	24	Устный опрос, Отчеты по лабораторным работам, контрольная работа	ПК-4	ПК-4.2
4	Технические методы защиты информации	5	1	2	24	Устный опрос, Отчеты по лабораторным работам. Контрольная работа	ПК-4	ПК-4.2
	ИТОГО	**-**	**4**	**8**	**96**	**-**	**-**	**-**

4.3. Содержание *разделов/тем* дисциплины

1 Информационная безопасность

Информация. Её виды и свойства. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность. Государственная тайна. Коммерческая тайна. Персональные данные. Служебная тайна. Профессиональная тайна. Угрозы информационной безопасности. Каналы утечки информации. Модель нарушителя информационной безопасности

2 Криптографические методы защиты информации

Исторические шифры. Симметричные алгоритмы шифрования. Криптографические алгоритмы с открытым ключом. Электронно-цифровая подпись. Перспективы развития криптографических методов защиты информации.

3 Правовые аспекты информационной безопасности

Доктрина информационной безопасности. Преступления в сфере компьютерной. Информации. Международные стандарты информационной безопасности. Политика информационной безопасности. Аудит информационной безопасности.

4. Технические методы защиты информации

Межсетевое экранирование. Разграничение доступа. Монитор обращений. Системы обнаружения вторжений. Система обнаружения утечек. Анализатор сетевого трафика

4.4. Содержание занятий семинарского типа

Таблица 6.

Содержание лабораторных занятий для очной формы обучения

№ темы дисциплины	Тематика лабораторных занятий	Всего часов	В том числе часов практической подготовки
1	Криптоконтейнеры VeraCrypt	6	
2	Шифр простой замены	4	
2	Основы шифрования данных	4	
2	Исследование шифра гаммирования	2	
2	Исследование пакета Gpg4win для передачи сообщений по сети с использованием ассиметричной криптографией	2	
3	Разработка политики информационной безопасности	4	
4	Управление доступом к файлам на NTFS	2	
4	Работа с анализатором трафика	4	

Таблица 7.

Содержание лабораторных занятий для очно-заочной формы обучения

№ темы дисциплины	Тематика лабораторных занятий	Всего часов	В том числе часов практической подготовки
1	Криптоконтейнеры VeraCrypt	4	
2	Основы шифрования данных	4	
2	Исследование пакета Gpg4win для передачи сообщений по сети с использованием ассиметричной криптографией	2	
3	Разработка политики информационной безопасности	4	
4	Управление доступом к файлам на NTFS	2	
4	Работа с анализатором трафика	4	

Таблица 8.

Содержание лабораторных занятий для заочной формы обучения

№ темы дисциплины	Тематика лабораторных занятий	Всего часов	В том числе часов практической подготовки
1	Криптоконтейнеры VeraCrypt	2	
2	Исследование пакета Gpg4win для передачи сообщений по сети с использованием ассиметричной криптографией	2	
3	Разработка политики информационной безопасности	2	
4	Управление доступом к файлам на NTFS	2	

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1 Конспект лекций

2 Методические указания к лабораторным работам

6. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Учет успеваемости обучающегося по дисциплине осуществляется по 100-балльной шкале. Максимальное количество баллов по дисциплине за один семестр – 100:

- максимальное количество баллов за выполнение всех видов текущего контроля - 55;
- максимальное количество баллов за посещение лекционных занятий – 10;
- максимальное количество баллов за прохождение промежуточной аттестации - 20;
- максимальное количество дополнительных баллов 15

6.1. Текущий контроль

Типовые задания, методика выполнения и критерии оценивания текущего контроля по разделам дисциплины представлены в Фонде оценочных средств по данной дисциплине.

6.2. Промежуточная аттестация

Форма промежуточной аттестации по дисциплине – **зачет**

Форма проведения **зачета**: устно по билетам

Перечень вопросов для подготовки к зачету

ПК-4 (ПК-4.2)

1. Проблема информационной безопасности
2. Свойства информационной безопасности
3. Методы обеспечения информационной безопасности
4. Угрозы информационной безопасности
5. Структура системы защиты от угроз нарушения конфиденциальности информации
6. Организационные меры и меры обеспечения физической безопасности
7. Идентификация и аутентификация
8. Модели разграничения доступа
9. Симметричные криптосистемы
10. Асимметричные криптосистемы
11. Электронная подпись
12. Межсетевое экранирование
13. Модели OSI/ISO
14. Системы обнаружения вторжений
15. Протоколирование и аудит
16. Криптографические хэш-функции
17. Структура системы защиты от угроз нарушения доступности
18. Резервное копирование информации
19. Критерии оценки доверенных компьютерных систем
20. Классификация Автоматизированных систем
21. Защита Государственной тайны
22. Коммерческая тайна
23. Персональные данные
24. Служебная тайна
25. Профессиональная тайна
26. Средства анонимности в интернете

6.3. Балльно-рейтинговая система оценивания

Таблица 9.

Распределение баллов по видам учебной работы

Вид учебной работы, за которую ставятся баллы	**Баллы**
Посещение лекционных занятий	0-10
Опрос	0-15
Контроль выполнения лабораторных работ	0-40
Дополнительные баллы	0-15
Промежуточная аттестация	0-20
ИТОГО	**0-100**

Таблица 10.

Распределение дополнительных баллов

Дополнительные баллы (баллы, которые могут быть добавлены до 100)	**Баллы**
Участие в CTF*	0-15
ИТОГО	**0-15**

*Участие в соревнованиях по информационной безопасности в формате CTF

Минимальное количество баллов для допуска до промежуточной аттестации составляет 40 баллов при условии выполнения всех видов текущего контроля.

Таблица 11.

Балльная шкала итоговой оценки на зачете

Оценка	**Баллы**
Зачтено	65-100
Незачтено	0-64

7. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации ко всем видам аудиторных занятий, а также методические рекомендации по организации самостоятельной работы, в том числе по подготовке к текущему контролю и промежуточной аттестации представлены в Методических рекомендации для обучающихся по освоению дисциплины «Информационная безопасность».

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1) Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/475890 (дата обращения: 23.06.2021).

2) Организационно-правовое обеспечение информационной безопасности:

Учебное пособие./ П.Ю. Богданов, Н.В. Яготинцева. СПБ.: ООО «Андреев-ский издательский дом», 2015 г. -169 стр.

Дополнительная литература

1) Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467370 (дата обращения: 23.06.2021).

2) Рыжко, А. Л. Информационные системы управления производственной компанией : учебник для вузов / А. Л. Рыжко, А. И. Рыбников, Н. А. Рыжко. — Москва : Издательство Юрайт, 2020. — 354 с. — (Высшее образование). — ISBN 978-5-534-00623-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450340 (дата обращения: 15.06.2021).

8.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

1. Личный кабинет студента РГГМУ. [Электронный ресурс] – режим доступа URL: https://lk.rshu.ru/.
2. Система дистанционного обучения РГГМУ. [Электронный ресурс] – режим доступа URL: http://moodle.rshu.ru/login/index.php.
3. Электронно-библиотечная система elibrary. [Электронный ресурс] – режим доступа URL: https://www.elibrary.ru/
4. База данных Scopus. [Электронный ресурс] – режим доступа URL: https://www.scopus.com/.
5. База данных ORCID (Open Researcher and Contributor ID)/ [Электронный ресурс] – режим доступа URL: https://orcid.org/.

8.3. Перечень программного обеспечения

1. Пакет офисных приложений MS Office

2. Программа для организации видеоконференций Zoom.

3 Среда виртуализации операционных систем Virtual Box или VmWare Workstation Player

4 Анализатор трафика tcpdump или wireshark

5 Пакет для шифрования электронной почты и файлов Gpg4win

8.4. Перечень информационных справочных систем

1. Консультант Плюс. Официальный сайт компании «Консультант–Плюс» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru, свободный.

2. ЭБС «ЮРАЙТ» – учебники и учебные пособия издательства. [Электронный ресурс] – режим доступа URL: https:// https://www.biblio–online.ru/.

3. Электронная библиотечная система ZNANIUM.COM [Электронный ресурс] – режим доступа URL: http://znanium.com/.

4. ЭБС «Лань» [Электронный ресурс] – режим доступа URL: https://e.lanbook.com/.

8.5. Перечень профессиональных баз данных

1. База данных Scopus
2. Электронно-библиотечная система elibrary

9. Материально-техническое обеспечение дисциплины

Материально–техническое обеспечение программы соответствует действующим санитарно-техническим и противопожарным правилам и нормам и обеспечивает проведение всех видов лекционных, лабораторных занятий и самостоятельной работы обучающихся.

Учебный процесс обеспечен аудиториями, комплектом лицензионного программного обеспечения, библиотекой РГГМУ.

Учебная аудитория для проведения занятий лекционного типа укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации, презентационной переносной техникой.

Учебная аудитория для проведения лабораторных занятий укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации, презентационной переносной техникой, а также оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечено доступом в электронную информационно–образовательную среду организации.

Учебная аудитория для текущего контроля и промежуточной аттестации – укомплектована специализированной (учебной) мебелью.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечено доступом в электронную информационно–образовательную среду организации.

10. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

11. Возможность применения электронного обучения и дистанционных образовательных технологий

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий