

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г. ЧЕРНЫШЕВСКОГО»

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ

Декан факультета

Миронов С. В.



«31» августа 2021 г.

Рабочая программа дисциплины
Организационное и правовое обеспечение информационной
безопасности

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Квалификация выпускника

Специалист по защите информации

Форма обучения

Очная

Саратов,

2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Гортинский А. В.		31.08.2021 г.
Председатель НМК	Кондратова Ю. Н.		31.08.2021 г.
Заведующий кафедрой	Абросимов М. Б.		31.08.2021 г.
Специалист Учебного управления			31.08.2021 г.

1. Цели освоения дисциплины

Целью освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» является овладение основами использования нормативно-правовых актов для разработки организационно-распорядительной документации, организации и планирования деятельности по защите информации.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к обязательной части Блока 1 «Дисциплины (Модули)» учебного плана ООП и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Теория информации», «Физика», «Информационные технологии и программирование», «Аппаратные средства вычислительной техники», «Компьютерные сети», «Основы информационной безопасности», «Сети и системы передачи информации».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин «Основы компьютерной экспертизы», «Защита в операционных системах», «Основы построения защищенных компьютерных сетей», «Основы управленческой деятельности».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Модели безопасности компьютерных систем» и «Защита информации от утечки по техническим каналам».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ОПК-5.1.2 знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые	Знать основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	<p>акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;</p> <p>ОПК-5.2.2 умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации</p>	<p>акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности;</p> <p>Уметь обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации</p>

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	<p>по требованиям безопасности информации; формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; ОПК-5.2.3 умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации; ОПК-5.3.1 владеет навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации.</p>	<p>по требованиям безопасности информации; формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации; Владеть навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации.</p>
<p>ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.</p>	<p>ОПК-6.1 знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту</p>	<p>Знать систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту</p>

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	<p>информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем;</p> <p>ОПК-6.2 умеет разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы;</p> <p>ОПК-6.3 владеет навыками при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными</p>	<p>информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя компьютерных систем;</p> <p>Уметь разрабатывать модели угроз и модели нарушителя компьютерных систем; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы;</p> <p>Владеть навыками при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими</p>

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	методическими документами Федеральной службы Российской Федерации, Федеральной службы по техническому и экспортному контролю.	документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоемкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
1	Нормативно-правовые и методические основы защиты информации	6	1-6	12	12	–	0,8	34	<i>Контрольная работа на 15-й неделе</i>
2	Организация защиты информации на предприятии		7-14	16	16	–	0,8	34	
3	Документационное обеспечение информационной безопасности на предприятии		15-16	4	4	–	0,4	10	
Промежуточная аттестация									Зачёт, курсовая работа
ИТОГО в 6-м семестре				32	32	–	2	78	–

Содержание дисциплины

Нормативно-правовые и методические основы защиты информации.

Понятие информационной безопасности, система защиты информации в Российской Федерации, нормативно-правовые основы защиты информации, оценочные стандарты и методические документы в сфере защиты информации.

Организация защиты информации на предприятии. Общие вопросы организации защиты информации, основные мероприятия по обеспечению информационной безопасности, защита автоматизированных информационных систем, особенности защиты информации в госучреждениях, защита персональных данных в организации.

Документационное обеспечение информационной безопасности на предприятии. Построение частной модели угроз безопасности информации, инструкции и обязанности персонала по обеспечению и соблюдению режима информационной безопасности.

План лабораторных занятий

На лабораторных занятиях студенты, используя компьютерные средства и выданные преподавателем файлы, содержащие нормативно-правовые и методические руководящие документы, а также используя лекционный материал, зафиксированный в конспектах, отыскивают мотивированные ответы на вопросы, поставленные преподавателем. Преподаватель может добиваться нескольких вариантов ответа или более полного ответа, если текущий отвечающий полностью не раскрывает вопрос.

№ занятия	Тема	Задания для лабораторного практикума
1	2	3
1	Нормативно-правовые и методические основы защиты информации. Понятие информационной безопасности.	№1
2	Нормативно-правовые и методические основы защиты информации. Система защиты информации в Российской Федерации.	№2
3-4	Нормативно-правовые и методические основы защиты информации. Нормативно-правовые основы защиты информации.	№3
5-6	Нормативно-правовые и методические основы защиты информации. Оценочные стандарты и методические документы в сфере защиты информации.	№4
7-9	Организация защиты информации на предприятии. Общие вопросы организации защиты информации.	№5
10	Организация защиты информации на предприятии. Основные мероприятия по обеспечению информационной безопасности.	№6
11	Организация защиты информации на предприятии.	№7

	Защита автоматизированных информационных систем.	
12-13	Организация защиты информации на предприятии. Особенности защиты информации в госучреждениях,	№8
14	Организация защиты информации на предприятии. Защита персональных данных в организации.	№9
15-16	Документационное обеспечение информационной безопасности на предприятии. Построение частной модели угроз безопасности информации. Инструкции и обязанности персонала по обеспечению и соблюдению режима информационной безопасности.	№10

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как семинары-беседы по вопросам по тематике предыдущих лекций. На первом лабораторном занятии слушателям выдаётся набор нормативно-правовых и методических документов. На последующих занятиях на основе лекционного материала слушатели ищут ответы на заданные вопросы в этих документах и обсуждают отношение тех или иных извлечённых положений к обсуждаемой ситуации.

На первых занятиях предусмотрен просмотр фильмов об организации защиты информации и проведении специальных исследований и проверок.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом образовательных возможностей обучающихся.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты изучают материалы предыдущих лекций и соотносят их с соответствующими положениями нормативно-правовых актов, указанных в списке литературы лекции.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачет), темы курсовых работ. Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Организационное и правовое обеспечение информационной безопасности».

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции и	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
6	10	5	0	5	0	40	40	100

Программа оценивания учебной деятельности студента

6 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 10 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий в течение одного семестра – от 0 до 5 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Контроль результатов самостоятельной работы, которая состоит в сопоставлении материалов лекции и указанных в ней оригинальных документов, осуществляется в течение лабораторных занятий. Студенты, работавшие самостоятельно, быстрее ориентируются в нормативных и методических документах и, соответственно, быстрее отвечают на вопросы.

Выполнение заданий в рамках самостоятельной работы в течение семестра – от 0 до 5 баллов.

0 - 3 баллов – слабо изучал необходимые нормативные акты и методические документы в рамках озвученных на лекции тематик, не находит ответов на вопросы, слабо ориентируется в нормативных актах.

4-5 баллов – достаточно хорошо подготовился, сопоставил содержимое нормативных актов и методических документов и материалы лекций, как следствие быстро находит ответы в необходимом количестве документов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа относится к типу расчетно-графическая. Она должна быть аккуратно оформлена по стандарту оформления реферата, схемы помещений, зданий, контролируемой зоны, технических каналов утечки информации должны быть выполнены в цвете. Вся работа должна быть разбита на главы согласно пунктам в типовом документе. Оценивается – от 0 до 40 баллов, а именно

работа на «отлично» оценивается от 35 до 40 баллов;

работа на «хорошо» оценивается от 30 до 34 баллов;

работа на «удовлетворительно» оценивается от 20 до 29 баллов;

работа на «неудовлетворительно» оценивается от 0 до 19 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой устный *зачет*.

При проведении промежуточной аттестации

ответ на «отлично» / «зачтено» оценивается от 35 до 40 баллов;

ответ на «хорошо» / «зачтено» оценивается от 30 до 34 баллов;

ответ на «удовлетворительно» / «зачтено» оценивается от 20 до 29 баллов;

ответ на «неудовлетворительно» / «не зачтено» оценивается от 0 до 19 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 6 семестр по дисциплине «Организационное и правовое обеспечение информационной безопасности» составляет **100** баллов.

Таблица 2.2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Организационное и правовое обеспечение информационной безопасности» в оценку (зачет)

50 баллов и более	«зачтено»
меньше 50 баллов	«не зачтено»

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
6	0	0	0	40	0	20	40	100

Программа оценивания учебной деятельности студента

6 семестр

Лекции

Не предусмотрено.

Лабораторные занятия

Не предусмотрено.

Практические занятия

Не предусмотрено.

Самостоятельная работа

Оценивается сбор, анализ и систематизация теоретической, научно-практической информации по тематике курсовой работы; обоснованный выбор методов и инструментальных средств для проведения вычислительного эксперимента; планирование, проведение и анализ результатов вычислительного эксперимента, грамотность в оформлении – от 0 до 40 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности – от 0 до 20 баллов

Оценивается планомерная работа над курсовой работой во время семестра, регулярные консультации с научным руководителем, своевременное представление курсовой работы на защиту – от 0 до 10 баллов; участие в научных мероприятиях по тематике курсовой работы или ином публичном представлении результатов курсовой работы, в том числе участие в создании объектов интеллектуальной собственности; публикация результатов исследований, выполненных в рамках курсовой работы – от 0 до 10 баллов.

Промежуточная аттестация – зачет – от 0 до 40 баллов

Включает в себя соблюдение требований к оформлению текста курсовой работы; подготовка презентации выступления для защиты курсовой работы; грамотность и логичность выступления с результатами работы на защите курсовой работы; исчерпывающие, правильные и уверенные ответы на вопросы в ходе защиты курсовой работы.

При проведении промежуточной аттестации

результат работы на «отлично» / «зачтено» оценивается от 32 до 40 баллов;

результат работы на «хорошо» / «зачтено» оценивается от 24 до 31 баллов;

результат работы на «удовлетворительно» / «зачтено» оценивается от 16 до 23 баллов;

результат работы на «неудовлетворительно» / «не зачтено» оценивается от 0 до 15 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за шестой семестр по курсовой работе составляет **100** баллов.

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по курсовой работе в оценку (зачет)

70 баллов и более	«зачтено»
меньше 70 баллов	«не зачтено»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Гортинский, А. В. Организационно-правовые основы защиты персональный данных [Электронный ресурс] : Учебное пособие / А. В. Гортинский. - Саратов, 2012. - 98 с. URL: http://elibrary.sgu.ru/uch_lit/621.pdf. Загл. с экрана. Яз. Рус. ✓

2) Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности : учебное пособие / Жигулин Г.П.. — Санкт-Петербург : Университет ИТМО, 2014. — 174 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/67451.html>. Загл. с экрана. Яз. Рус. ✓

3) Кармановский Н.С. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Кармановский Н.С., Михайличенко О.В., Прохожев Н.Н.. — Санкт-Петербург : Университет ИТМО, 2016. — 169 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/67452.html>. Загл. с экрана. Яз. Рус. ✓

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Microsoft Office, Microsoft Windows. *недет*

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходимы аудитория, оборудованная компьютером с установленным любым программным обеспечением, позволяющим читать следующие форматы файлов данных: pdf, doc, docx, ppt, pptx и подключаемый к нему проектор.

Для проведения лабораторных занятий необходимы аудитории, оборудованные компьютерами класса не ниже Pentium IV, с установленным любым программным обеспечением, позволяющим читать следующие форматы файлов данных: pdf, doc, docx.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Доцент кафедры теоретических основ компьютерной безопасности и криптографии, к. ю. н., доцент

А. В. Гортинский

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «31» августа 2021 года, протокол № 1.