МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
**Федеральное государственное автономное**
**образовательное учреждение высшего образования**
**«Национальный исследовательский**
**Нижегородский государственный университет им. Н.И. Лобачевского»**

Радиофизический факультет
(факультет / институт / филиал)

УТВЕРЖДАЮ:

Декан _____ Матросов В.В.

« 29 » июня 2020 г.

# Рабочая программа дисциплины

Б1.Б.20 Организационное и правовое обеспечение информационной безопасности
(наименование дисциплины (модуля))

Уровень высшего образования
специалитет
(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность
10.05.02 Информационная безопасность телекоммуникационных систем
(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы
Системы подвижной цифровой защищенной связи
(указывается профиль / магистерская программа / специализация)

Квалификация (степень)
специалист
(бакалавр / магистр / специалист)

Форма обучения
очная
(очная / очно-заочная / заочная)

Нижний Новгород

2018

## 1. Место и цели дисциплины в структуре ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к дисциплинам базовой части основной профессиональной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», преподается в 9 семестре.

Изучение студентами дисциплины «Организационное и правовое обеспечение информационной безопасности» базируется на знаниях и умениях, полученных в результате изучения дисциплин «Правоведение», «Основы информационной безопасности».

**Цели освоения дисциплины**

Учебная дисциплина «Организационное и правовое обеспечение информационной безопасности» является важной составляющей общей профессиональной подготовки специалистов в области информационной безопасности. Она призвана обеспечить освоение слушателями практических навыков работы с нормативно-правовой базой деятельности в области обеспечения безопасности информации.

## 2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

| **Формируемые компетенции** | **Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций** |
|---|---|
| ОК-4. Способность использовать основы правовых знаний в различных сферах деятельности. | З1 (ОК-4). Знать содержание основных законодательных и правовых актов, нормативных и методических документов в области защиты информации и перспективы их дальнейшей разработки.<br>У1 (ОК-4). Уметь эффективно реализовывать требования нормативных и методических руководящих документов, действующего законодательства по вопросам защиты информации в организациях.<br>В1 (ОК-4). Владеть навыками работы с нормативными и правовыми документами в области защиты информации в организации. |
| ОПК-7. Способность применять нормативные правовые акты в своей профессиональной деятельности. | З1 (ОПК-7). Знать систему организации комплексной защиты информации в организации.<br>З2 (ОПК-7). Знать требования основных законодательных и правовых актов по лицензированию деятельности по технической защите информации (ТЗИ), созданию средств защиты информации (СЗИ).<br>У1 (ОПК-7). Уметь организовывать контроль и оценку состояния защищенности информации в организации.<br>В1 (ОПК-7). Владеть навыками работы с правовыми базами данных по объектам защиты, угрозам безопасности информации в организации.<br>В2 (ОПК-7). Владеть навыками работы с законодательными и правовыми базами данных по лицензированию |

| | |
|---|---|
| | деятельности по технической защите информации (ТЗИ), созданию средств защиты информации (СЗИ). |
| ПК-11. Способность организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы. | З1 (ПК-11). Знать принципы организации работы малых коллективов исполнителей, управленческих решений в сфере профессиональной деятельности.<br>У1 (ПК-11). Уметь организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы.<br>В1 (ПК-11). Владеть способностью организовывать работу малых коллективов исполнителей, принимать управленческие решения в сфере профессиональной деятельности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью телекоммуникационной системы. |
| ПК-12. Способность выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности. | З1 (ПК-12). Знать методы выполнения технико-экономические обоснования, оценки затрат и результатов деятельности организации в области обеспечения информационной безопасности.<br>У1 (ПК-12). Уметь выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности.<br>В1 (ПК-12). Владеть способностью выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности. |
| ПК-13. Способность организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем. | З1 (ПК-13). Знать требования режима защиты информации ограниченного доступа, принципы разработки проектов документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем.<br>У1 (ПК-13). Уметь организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем.<br>В1 (ПК-13). Владеть способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем. |

## 3. Структура и содержание дисциплины «Организационное и правовое обеспечение информационной безопасности»

Объем дисциплины составляет 2 зачетные единицы, всего 72 часа, из которых 33 часа составляет контактная работа обучающегося с преподавателем (32 часа занятия лекционного типа, в том числе 2 часа – мероприятия текущего контроля успеваемости, 1 час – мероприятия промежуточной аттестации), 39 часов составляет самостоятельная работа обучающегося.

| **Наименование и краткое содержание разделов и тем дисциплины,**<br><br>**форма промежуточной аттестации по дисциплине** | **Всего (часы)** | В том числе | | | | |
|---|---|---|---|---|---|---|
| | | **Контактная работа (работа во взаимодействии с преподавателем), часы из них** | | | | **Самостоятельная работа обучающегося, часы** |
| | | **Занятия лекционного типа** | **Занятия семинарского типа** | **Занятия лабораторного типа** | **Всего** | |
| 1. Основные положения руководящих документов полномочных органов государственной власти Российской Федерации в области защиты информации | 24 | 10 | | | 10 | 12 |
| 2. Создание системы защиты информации. Организация защиты информации | 24 | 10 | | | 10 | 14 |
| 3. Лицензирование деятельности по технической защите информации, созданию средств защиты информации. Сертификация средств | 24 | 12 | | | 12 | 13 |

| | | | | | | |
|---|---|---|---|---|---|---|
| защиты информации по требованиям безопасности информации | | | | | | |
| В т.ч.текущий контроль | 2 | 2 | | | 2 | |
| **Промежуточная аттестация:** зачет | | | | | | |

## 4. Образовательные технологии

**Образовательные технологии, способствующие формированию компетенций.**
***используемые на занятиях лекционного типа*:**
- лекции с изложением учебного материала.

## 5. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает следующие виды:
- изучение дополнительных разделов дисциплины с использованием учебной литературы;
- изучение содержания нормативных актов и руководящих документов полномочных органов государственной власти Российской Федерации в области защиты информации.
Текущий контроль усвоения материала проводится путем проведения опроса.

## 6. Фонд оценочных средств для промежуточной аттестации по дисциплине, включающий:

**6.1. Перечень компетенций выпускников образовательной программы** с указанием результатов обучения (знаний, умений, владений), характеризующих этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования.

| Индикаторы компетенции | Критерии оценивания | |
|---|---|---|
| | «незачтено» | «зачтено» |
| Знания | Наличие грубых ошибок в основном материале | Знание основного материалом, возможно с рядом погрешностей |
| Умения | Наличие грубых ошибок при выполнении стандартных заданий | Способность выполнения всех стандартных заданий, возможно с незначительными погрешностями |
| Навыки | Отсутствие навыка | Достаточное владение навыком |

**6.2. Описание шкал оценивания.**
Итоговый контроль качества усвоения студентами содержания дисциплины проводится в виде зачета.

**Критерии оценок.**

| Оценка | Уровень подготовки |
|---|---|
| Зачтено | В целом хорошая подготовка с возможными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы. |
| Не зачтено | Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на дополнительные вопросы. |

**6.3. Критерии и процедуры оценивания результатов обучения по дисциплине, характеризующих этапы формирования компетенций.**

Для оценивания результатов обучения в виде **знаний** используются следующие процедуры и технологии: зачет, проводимый в письменной форме с дальнейшим индивидуальным собеседованием.

Для оценивания результатов обучения в виде **умений** и **навыков** используются результаты обсуждения типовых решений по обеспечению защиты объектов информатизации в реальных организациях.

**6.4. Типовые контрольные задания или иные материалы**, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций и (или) для итогового контроля сформированности компетенции.

**Типовые задания для текущего контроля успеваемости.**

6.4.1. Задания для оценки компетенций «ОК-4», «ОПК-7», «ПК-11», «ПК-12», «ПК-13»:

1. Перечислить мероприятия, проводимые для обеспечения защиты информации, содержащейся в информационной системе.
2. Перечислить мероприятия, которые включает внедрение системы защиты информации информационной системы.
3. Назвать порядок проведения организацией аттестации объектов информатизации, обрабатывающих конфиденциальную информацию.
4. Пояснить невыполнение каких требований считается грубым нарушением лицензионных требований.
5. Назвать формы осуществления лицензионного контроля.
6. Назвать порядок сертификации средств защиты информации по требованиям безопасности информации.

**Типовые задания (оценочные средства), выносимые на зачет.**

6.4.2. Задания для оценки компетенции «ОК-4»:

1. Какие основные законы РФ используются для организации деятельности по защите информатизации
2. Какие нормативные и методические документы используются при организации технической защиты конфиденциальной информации (аттестации объектов информатизации, обрабатывающих конфиденциальную информацию)

3. Какие основные нормативные правовые акты, используются при лицензировании деятельности по технической защите информации, созданию средств защиты информации

6.4.3. Задания для оценки компетенции «ОПК-7»:
1. Что собой представляет система защиты информации объекта информатизации
2. Какие мероприятия проводятся для обеспечения защиты информации, содержащейся в информационной системе
3. Какие мероприятия включает внедрение системы защиты информации информационной системы
4. Как осуществляется обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы
5. Чем достигается обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы
6. Дать определение лицензируемому виду деятельности
7. Что собой представляют лицензионные требования

6.4.4. Задания для оценки компетенции «ПК-11»:
1. Какие мероприятия проводятся для обеспечения защиты информации, содержащейся в информационной системе
2. Какие мероприятия включает внедрение системы защиты информации информационной системы
3. Что собой представляют требования безопасности информации
4. Какие бывают объекты информатизации, обрабатывающие информацию
5. В каких формах осуществляется лицензионный контроль

6.4.5. Задания для оценки компетенции «ПК-12»:
1. Какие бывают объекты информатизации, обрабатывающие информацию
2. Чем достигается обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы
3. Что собой представляют лицензионные требования
4. В каких формах осуществляется лицензионный контроль
5. Что собой представляет система сертификации средств защиты информации по требованиям безопасности информации

6.4.5. Задания для оценки компетенции «ПК-13»:
1. Что собой представляют требования безопасности информации
2. Назовите порядок проведения организацией аттестации объектов информатизации, обрабатывающих конфиденциальную информацию
3. Как осуществляется обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы
4. Дать определение лицензируемому виду деятельности
5. Что собой представляют лицензионные требования
6. Невыполнение каких требований считается грубым нарушением лицензионных требований
7. Что собой представляет система сертификации средств защиты информации по требованиям безопасности информации

### 6.5. Методические материалы, определяющие процедуры оценивания.

Положение «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в ННГУ», утверждённое приказом ректора ННГУ от 13.02.2014 г. №55-ОД.

Положение «О фонде оценочных средств», утвержденное приказом ректора ННГУ от 10.06.2015 г. №247-ОД.

## 7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Ярочкин В.И. Информационная безопасность : учеб. для вузов / В.И. Ярочкин. - 4-е изд. - М. Академ. проект, 2006. - 543 с.
2. Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности. – М.: Издательство Юрайт, 2017. – 325 с.

б) дополнительная литература:

1. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»
2. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
3. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
4. Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».
5. Распоряжение Президента Российской Федерации от 16 апреля 2005 года № 151-рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне».
6. Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
8. Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
9. Постановление Правительства Российской Федерации от 18.09.2012 № 940 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю».

10. Постановление Правительства Российской Федерации от 24.11.2009 № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской федерации и федеральных органов исполнительной власти».
11. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».
12. Постановление Правительства Российской Федерации от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».
13. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности».
14. Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
15. Постановление Правительства Российской Федерации от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».
16. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
17. Приказ ФСТЭК России от 11.02.2013 № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
18. Приказ ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
19. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.
20. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.
21. Приказ ФСТЭК России от 17.07.2017 № 134 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».
22. Приказ ФСТЭК России от 17.07.2017 № 133 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации».
23. Приказ ФСТЭК России от 20.07.2012 № 89 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации»
24. Приказ ФСТЭК России от 20.07.2012 № 90 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по контролю за соблюдением лицензионных

требований при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации».

25. «Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации», одобрено решением Гостехкомиссии России от 14.03.1995 № 32.
26. «Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в организациях», одобрено решением Гостехкомиссии России от 14.03.1995 № 32.
27. Приказ Минздравсоцразвития России от 22.04.2009 № 205 «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».
28. ГОСТ Р 50922-2006 «Национальный стандарт российской федерации. Защита информации. Основные термины и определения».

в) программное обеспечение и Интернет-ресурсы:

1. Доктрина информационной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации от 05.12.2016 г. № 646 (интернет-ресурс: http://www.kremlin.ru/acts/bank/41460)
2. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) (интернет-ресурс: http://fstec.ru/)

## 8. Материально-техническое обеспечение дисциплины

Аудиторный фонд ННГУ для проведения лекций.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ОПОП ВПО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор _____ С.В. Алексеенко

Рецензент (ы) _____ С.Н. Жуков

Заведующий кафедрой «Безопасность информационных систем» _____ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от «25» июня 2020 года, протокол № 03/20.