

Федеральное государственное образовательное бюджетное учреждение
высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ
РОССИЙСКОЙ ФЕДЕРАЦИИ»**

(Финансовый университет)

Ярославский филиал Финуниверситета

Кафедра «Экономика и финансы»

СОГЛАСОВАНО

Директор ООО Юридическая
компания «Константа»

Ю.В. Колесникова

«14» апреля 2026 г.

УТВЕРЖДАЮ

Директор
Ярославского филиала
Финуниверситета

В.А. Кваша

«21» апреля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Направление подготовки: 40.03.01 «Юриспруденция»

Профиль «Экономическое право»

Автор: И.А. Девятковская

*Одобрено на заседании кафедры «Экономика и финансы» Ярославского филиала
Финуниверситета
(протокол № 8 от 06.04.2026)*

Ярославль, 2026

1. Наименование дисциплины

Дисциплина «Правовое обеспечение кибербезопасности» имеет порядковый номер Б.1.2.2.2.2.2 в структуре основной образовательной программы по направлению бакалавриат 40.03.01 Юриспруденция, профиль «Экономическое право» для очной формы обучения.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами усвоения образовательной программы

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесённые с компетенциями/индикаторами достижения компетенции
ПКП-1	Способность использовать фундаментальные знания в области частного права и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	1. Демонстрирует знания нормативных правовых актов, а также прогнозирует результат экономической деятельности для решения практических задач. 2. Использует фундаментальные знания в области частного и публичного права в современных условиях. 3. Оказывает помощь в реализации правовых норм субъектами гражданского оборота.	Знать: основные положения нормативных правовых актов в области обеспечения кибербезопасности; позиции высших судебных инстанций; Уметь: ориентироваться в проблематике обеспечения кибербезопасности и на данной основе прогнозировать результат экономической деятельности. Знать: фундаментальные частного и публичного права в современных условиях применительно к проблематике кибербезопасности Уметь: соотносить юридические факты с законодательством; систематизировать необходимый материал и анализировать практику правоприменения в информационно правовой сфере; осуществлять выбор оптимального варианта правомерного поведения в информационных правоотношениях с учетом фактических обстоятельств дела. Знать: основные положения нормативных правовых актов в области обеспечения кибербезопасности, угрозы кибербезопасности и правовые меры обеспечения информационной безопасности; Уметь: оказывать помощь в

			реализации правовых норм для обеспечения кибербезопасности субъектам гражданского оборота.
ПКП-2	Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять правонарушения при осуществлении предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению.	1. Действует с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера. 2. Выявляет правонарушения при осуществлении предпринимательской деятельности. 3. Дает юридически обоснованные предложения по преодолению и устранению правонарушений при осуществлении предпринимательской деятельности.	Знать: кризисных ситуаций в экономике, вызываемых рисками нарушения кибербезопасности; Уметь: анализировать кризисные ситуации в экономике, вызываемых рисками нарушения кибербезопасности; противодействовать различным проявлениям информационных угроз. Знать: основные направления обеспечения кибербезопасности; требования нормативных правовых актов к субъектам предпринимательской деятельности по обеспечению кибербезопасности; Уметь: выявлять правонарушения в ходе обеспечения кибербезопасности при осуществлении предпринимательской деятельности. Знать: основные направления правового обеспечения кибербезопасности; Уметь: вырабатывать обоснованные предложения по преодолению и устранению правонарушений при обеспечении кибербезопасности при осуществлении предпринимательской деятельности.

3. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Вид учебной работы по дисциплине	Всего (в з.е. и часах)	Семестр 7
Общая трудоемкость дисциплины	3 / 108	108

Аудиторные занятия	34	34
Лекции (Л)	16	16
Практические и семинарные занятия, т.ч. занятия в интерактивных формах (С)	18	18
Самостоятельная работа	74	74
Текущий контроль	Контрольная работа	
Промежуточный контроль	Зачет	

4. Нормативно-правовые документы, определяющие процедуру оценивания результатов текущего контроля и промежуточной аттестации студентов

Процедура оценивания результатов текущего контроля и промежуточной аттестации обучающихся регулируется соответствующими локальными нормативными актами Финансового университета и филиала, регламентирующими порядок организации и проведения контроля уровня освоения дисциплин и сформированности компетенций у обучающихся.

5. Примеры оценочных средств для проверки сформированности компетенций

Компетенция	Типовые задания
ПКП-1 Способность использовать фундаментальные знания в области частного права и публичного права в современных условиях и оказывать помощь в реализации правовых норм субъектами гражданского оборота	1. Демонстрирует знания нормативных правовых актов, а также прогнозирует результат экономической деятельности для решения практических задач. Задание. Возможно ли разместить в сети «Интернет» схему водоснабжения города Смоленска? 2. Использует фундаментальные знания в области частного и публичного права в современных условиях. Задание. Охарактеризуйте взаимосвязь процессов обеспечения национальной безопасности с обеспечением информационной безопасности и кибербезопасности. 3. Оказывает помощь в реализации правовых норм субъектами гражданского оборота. Укажите, с какими государственными органами должен взаимодействовать юрист организации, выполняющий указание руководителя по разработке положения о кибербезопасности предприятия.
ПКП-2 Способность действовать с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера, анализировать проблемные ситуации на рынке товаров, работ, услуг, а также выявлять	1. Действует с учетом кризисных ситуаций в экономике, вызываемых рисками правового и экономического характера. Задание. Каким образом осуществить взаимодействие в случае обнаружения факта компьютерной атаки на ресурсы субъекта хозяйственной деятельности и как минимизировать причиненный ущерб? 2. Выявляет правонарушения при осуществлении предпринимательской деятельности. Задание. Правомерно ли требование, что индивидуальный предприниматель должен: - иметь круглосуточный выход в сеть «Интернет»; - создать официальный электронный адрес и официальный сайт;

правонарушения при осуществлении предпринимательской деятельности и давать юридически обоснованные предложения по их преодолению и устранению	- обеспечивать кибербезопасность своих информационных ресурсов. 3. Дает юридически обоснованные предложения по преодолению и устранению правонарушений при осуществлении предпринимательской деятельности. Задание. В ходе проверки было установлено, что информационная система российского банка «РоСаБанк» располагается на ресурсах израильского провайдера хостинга. Является ли выявленный факт правонарушением?
---	---

6. Материалы для промежуточной аттестации

6.1 Примерный перечень вопросов для зачета

Примерные вопросы для подготовки к зачету:

1. Понятия Национальная безопасность и Информационная безопасность.
2. Определения киберпространства и кибербезопасности.
3. Необходимость правового регулирования кибербезопасности.
4. Методы обеспечения кибербезопасности.
5. Принципы обеспечения кибербезопасности.
6. Национальная киберинфраструктура.
7. Стратегия развития информационного общества в Российской Федерации.
8. Проблемы формирования понятийного (терминологического) аппарата в области кибербезопасности.
9. Проблемы развития информационной сферы как системообразующего фактора жизни общества.
10. Понятие и виды источников информационного права.
11. Структура, состав и особенности информационного законодательства.
12. Конституционные основы информационного законодательства.
13. Базовый закон информационной сферы.
14. Объекты и субъекты информационных правоотношений.
15. Права и обязанности обладателя информации.
16. Государство как субъект информационных отношений.
17. Правовой статус государственных организаций и учреждений в области обеспечения кибербезопасности.
18. Субъекты кибербезопасности.
19. Киберпреступность.
20. Компьютерные атаки и инциденты.
21. Защита конечных пользователей.
22. Проблемы выявления, идентификации, классификации, оценки угроз информационной безопасности.
23. Научно-технические проблемы развития современных информационных технологий, индустрии средств информатизации, телекоммуникации и связи.
24. Проблемы защиты личности в ходе трансграничного использования информационных технологий.
25. Международные стандарты кибербезопасности.
26. Конвенция о киберпреступности.
27. Cybersecurity Act.
28. Проблемы международно-правового обеспечения кибербезопасности.
29. Кибербезопасность как компонент международных отношений.
30. Правовые гарантии свободы коммуникации.

31. Нормативно правовая база Российской Федерации об обеспечении кибербезопасности.
32. Проблемы разработки Стратегии кибербезопасности Российской Федерации.
33. Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности.
34. Критерии и методы оценки эффективности систем и средств обеспечения информационной безопасности и кибербезопасности.
35. Мониторинг киберугроз и система реагирования на них
36. Проблемы влияния информационной сферы на конкурентоспособность России на современном этапе.
37. Проблемы оценки информационной безопасности личности, общества и государства.
38. Проблемы развития нормативного правового и нормативного технического обеспечения кибербезопасности.
39. Понятие критической информационной инфраструктуры.
40. Принципы, задачи, функции и стандарты обеспечения безопасности критической информационной инфраструктуры.
41. ГосСОПКА.
42. Полномочия ФСТЭК, ФСБ и иных государственных органов в сфере обеспечения кибербезопасности.
43. Проблемы нормативного правового обеспечения устойчивости функционирования и безопасности использования информационных систем и телекоммуникационных сетей, в том числе в составе глобальной информационной инфраструктуры.
44. Проблемы противодействия использованию информационных технологий в террористических целях для оказания деструктивного воздействия на элементы критической информационной инфраструктуры.
45. Особенности правового регулирования общественных отношений в сети «Интернет».
46. Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.
47. Правовой статус организатора распространения информации в сети "Интернет".
48. Регулирование социальных сетей
49. Особенности распространения информации в сети "Интернет".
50. Особенности распространения информации иностранными субъектами.
51. Понятия киберпреступности, киберпреступления и административного правонарушения в сфере кибербезопасности.
52. Уголовная ответственность за киберпреступления.
53. Административная ответственность за правонарушения в сфере кибербезопасности.

6.2. Пример экзаменационного билета с указанием компетенций, проверяемых в каждом вопросе

Пример билета для проведения зачёта

**Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Ярославский филиал Финуниверситета)**

Кафедра «Экономика и финансы»

Дисциплина «Правовое обеспечение кибербезопасности»

Филиал Ярославский

Форма обучения Очная

Семестр 7 Направление 40.03.01 «Юриспруденция», профиль «Экономическое право»

БИЛЕТ ДЛЯ ЗАЧЁТА № 1

№ п/п	Вопросы билета	Максимальный балл
1	Особенности распространения информации иностранными субъектами.	30 баллов
2	Понятия киберпреступности, киберпреступления и административного правонарушения в сфере кибербезопасности.	30 баллов

Подготовил

(подпись и ФИО преподавателя)

Утверждаю:

Заведующий кафедрой
«Экономика и финансы»

Сироткин С.А.

Дата _____ 20__ г.

7. Формы внеаудиторной самостоятельной работы студентов, предусмотренные учебным планом

7.1 Выполнение контрольной работы

Перечень примерных тем Контрольной работы:

1. Основные угрозы кибербезопасности, влияющие на темпы роста информационного общества в Российской Федерации.
2. Соотношение кибербезопасности и информационной безопасности.
3. Дискуссионные вопросы определения кибербезопасности.
4. Понятия информационного пространства и киберпространства.
5. Структура, состав и особенности информационного законодательства.
6. Конституционные основы информационного законодательства.
7. Базовый закон информационной сферы.
8. Объекты и субъекты правоотношений в сфере кибербезопасности.
9. Киберпреступность: понятие и виды.
10. Компьютерные атаки и инциденты (кибератаки)
11. Кибертерроризм.
12. Вредоносное программное обеспечение: понятие и виды.
13. Проблемы КиберБулинга.
14. Фишинг и противодействие ему.
15. DDos – атаки: понятие и противодействие.
16. Международный стандарт ISO/IEC 27032:2012: Основные положения.
17. Будапештская Конвенция Совета Европы по киберпреступлениям ETS 185 от 23 ноября 2001 г.
18. Регламент 2019/881 Об Агентстве ЕС по кибербезопасности (ENISA) и сертификации по кибербезопасности информационных и коммуникационных технологий (Cybersecurity Act) 2019 г.
19. Стратегия развития информационного общества в Российской Федерации об обеспечении кибербезопасности.
20. Проблемы разработки Стратегии кибербезопасности Российской Федерации.
21. Государственные (национальные) стандарты РФ и руководящие документы по кибербезопасности.

22. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
23. Повышение информированности общества в сфере кибербезопасности.
24. Органы, ответственные за обеспечение кибербезопасности критической информационной инфраструктуры.
25. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 : основные требования.
26. Особенности правового регулирования общественных отношений в сети «Интернет».
27. Требования к безопасности информационных ресурсов в сети «Интернет».
28. Правовое регулирование социальных сетей.
29. Защита персональных данных в сети «Интернет»
30. Деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет».
31. Актуальные вопросы ограничения доступа к сайтам в сети «Интернет» с информацией, распространяемой с нарушением законодательства РФ.
32. Понятие киберпреступления и правонарушения в сфере кибербезопасности.
33. Уголовная ответственность за киберпреступления.
34. Административная ответственность за нарушения в области обеспечения кибербезопасности.

2. Рекомендуемые источники информации:

А). Основная литература

1. Информационное право : учебник для вузов / М. А. Федотов [и др.]; под редакцией М. А. Федотова. — Москва: Юрайт, 2021. — 497 с. — (Высшее образование).— Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469790> (дата обращения: 17.10.2022). — Текст: электронный.

2. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху: монография / О. А. Степанов. — Москва : Юрайт, 2022. — 103 с. — (Актуальные монографии). — ISBN 978-5-534-12775-1. Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496448> (дата обращения: 17.10.2022).— Текст: электронный

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2022. — 325 с. — (Высшее образование). — Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844> (дата обращения: 17.10.2022). — Текст: электронный.

Б). Дополнительная литература

4. Актуальные проблемы информационного права : учебник / РАН, Ин-т государства и права ; под ред. И. Л. Бачило, М. А. Лапиной. - Москва: Юстиция, 2016. - 534 с.— Текст: непосредственный. Актуальные проблемы информационного права: учебник / под ред. И. Л. Бачило, М. А. Лапиной. — Москва: Юстиция, 2020. — 592 с. — (магистратура, аспирантура). — ЭБС BOOK.ru. - URL: <https://book.ru/book/935207> (дата обращения: 17.10.2022)

5. Жарова, А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации: монография / А. К. Жарова. — Москва : Юрайт, 2022. — 301 с. — (Актуальные монографии). — Текст : электронный— Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496939> (дата обращения: 17.10.2022).

3. Работа должна быть представлена в печатном варианте.

Требования к контрольной работе:

Выполнение контрольной работы осуществляется после усвоения лекционного материала, практических занятий по дисциплине и самостоятельного систематического

изучения теоретического материала до начала экзаменационной сессии. Выполненную контрольную работу студент представляет в учебную часть для проверки ее преподавателем за месяц до начала сессии.

Все контрольные теоретические вопросы являются составной частью экзаменационных вопросов, поэтому работа над изучением материала контрольных теоретических, практических вопросов и контрольных тестовых заданий позволит качественно подготовиться к экзамену.

1. Ответ на теоретический вопрос предполагает изложение его сущности, проиллюстрированное при необходимости графиками, формулами и таблицами. При рассмотрении теоретического вопроса приводятся статистические данные по Российской Федерации, а также нормативные правовые документы в области безопасности жизнедеятельности. При использовании литературных источников в обязательном порядке должны быть сделаны ссылки на них. Ссылки по тексту изложения теоретического материала на литературные источники оформляются в квадратных скобках и нумеруются в соответствии с библиографическим списком, представленном в контрольной работе студента.

2. Выполнение тестовых заданий предполагает выбор одного правильного варианта ответа из нескольких предложенных. При этом необходимо не только дать правильный ответ на контрольное тестовое задание, но и обязательно привести его обоснование со ссылкой на литературный источник, а на собеседовании по контрольной работе – объяснить свой выбор.

3. Для выполнения практического задания студент должен ответить на поставленные вопросы, разобрать ситуации, дать пояснения и сделать выводы. При разработке практического задания основное внимание следует уделить правильности подбора фактологического материала, т.е. необходимо учесть, что данные должны быть достоверными и позволяют раскрыть содержание предлагаемой проблемы. Опираясь на теоретические положения, представленные в научной литературе, в обязательном порядке должны быть сделаны ссылки на них. Ссылки оформляются в квадратных скобках и нумеруются в соответствии с библиографическим списком, представленном в контрольной работе студента.