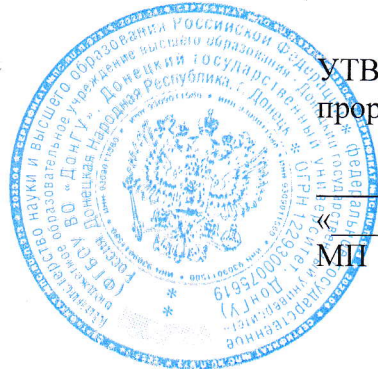


Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Юридический факультет
Кафедра конституционного и международного права



УТВЕРЖДАЮ

проректор

П.А. Машаров

« » 2024 г.

МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение информационной безопасности»

Укрупненная группа направлений подготовки	10.00.00 Информационная безопасность
Программа высшего образования	Программа бакалавриат
Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Квалификация	Бакалавр
Форма обучения	очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины **«Организационное и правовое обеспечение информационной безопасности»** для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 (с изм. и доп.). Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:
старший преподаватель
кафедры конституционного и
международного права



А.В. Голубцов

Рабочая программа одобрена на заседании кафедры конституционного и
международного права
Протокол от 25.03.2024 г. № 12


Заведующий кафедрой



Л.Ю. Одегова

СОГЛАСОВАНО:

И.о. декана физико-технического факультета
28.03.2024 г.



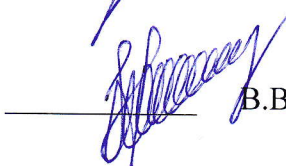
С.А. Фоменко

Учебно-методическая комиссия физико-технического факультета
Протокол от 27.03.2024 г. № 2
Председатель



В. Н. Котенко

Руководитель основной профессиональной
образовательной программы
д-р тех. наук, проф.
26.03.2024 г.



В.В. Данилов

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

базовая подготовка по обществознанию в объёме программы средней школы;

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Научный семинар по вопросам математического анализа, Гармонический анализ, Производственная практика: научно-исследовательская работа (обязательная), Производственная практика: преддипломная практика (обязательная).

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.03.01 Информационная безопасность (Программа бакалавриата: 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем))
Шифр и название в соответствии с учебным планом	Б1.Б.М2.7 Организационное и правовое обеспечение информационной безопасности
Часть образовательной программы	Базовая часть
Количество зачетных единиц / всего часов	2/ 72

2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная	4	7	30	–	-	42	72	зачёт

3. ЦЕЛИ ДИСЦИПЛИНЫ

Углубленная подготовка в области организационного и правового обеспечения информационной безопасности; изучение нормативных правовых актов в сфере информационной безопасности.

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1. Компетенции

Компетенции	Индикаторы	Результаты обучения
ОПК-5.	ОПК-5.1. Выбирает нормативные и правовые акты, методические документы и использует в	ОПК-5.1.1. Знает нормативные и правовые акты и методические документы. ОПК-5.1.2. Умеет выбирать и использовать необходимые нормативные правовые акты и методические документы; применять их для решения задач, связанных с обеспечением информационной безопасности.

	профессиональной деятельности	ОПК-5.1.3. Аргументированно выбирает нормативные и правовые акты и методические документы.
--	-------------------------------	--

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Раздел 1. Обеспечение информационной безопасности в условиях глобализации информационного пространства.	1.1. Информационная безопасность в информационном обществе. 1.2. Современное информационное противоборство и обеспечение информационной безопасности.
Раздел 2. Теоретические и методологические вопросы организационного и правового обеспечения информационной безопасности.	2.1. Информационная безопасность в системе национальной безопасности Российской Федерации. 2.2. Базовые принципы обеспечения информационной безопасности. 2.3. Правовое регулирование информационной безопасности в системе российской информационного права. 2.4. Правовые средства обеспечения безопасности информационной инфраструктуры Российской Федерации. 2.5. Правовые средства обеспечения информации. 2.6. Организационное обеспечение информационной безопасности Российской Федерации.
Раздел 3. Правовые режимы обеспечения безопасности информации ограниченного доступа.	3.1. Ограничение доступа к информации в целях защиты интересов личности, общества и государства. 3.2. Правовые режимы тайн в системе организационного и правового обеспечения безопасности информации ограниченного доступа. 3.3. Правовой режим защиты государственной тайны. 3.4. Правовой режим коммерческой тайны. 3.5. Правовой режим обеспечения безопасности персональных данных. 3.6. Актуальные вопросы режима служебной тайны.
Раздел 4. Актуальные проблемы правового и организационного обеспечения информационной безопасности.	4.1. Противодействие экстремистской деятельности в информационной сфере. 4.2. Защита детей от информации, причиняющей вред их здоровью и развитию. 4.3. Правовые проблемы обеспечения информационной безопасности в сети Интернет.
Раздел 5. Особенности организационно-правового обеспечения защиты информационных систем.	5.1. Особенности организационно-правового обеспечения процессов создания, автоматизированных систем в защищённом исполнении. 5.2. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства. 5.3. Практика разработки и реализации политики информационной безопасности корпоративных информационных систем.
Раздел 6. Юридическая ответственность за правонарушения в информационной сфере.	6.1. Понятие и виды юридической ответственности в области обеспечения информационной безопасности. Субъекты и объекты правоотношений в области обеспечения информационной безопасности.

	6.2. Преступность в информационной сфере как угроза информационной безопасности при формировании информационного общества в условиях глобализации. 6.3. Проблемы уголовно-правовой ответственности за информационные преступления.
--	---

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 4, семестр – 7

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Раздел 1. Обеспечение информационной безопасности в условия глобализации информационного пространства.	4	–	–	6	10
Раздел 2. Теоретические и методологические вопросы организационного и правового обеспечения информационной безопасности.	6	–	–	10	16
Раздел 3. Правовые режимы обеспечения безопасности информации ограниченного доступа.	8	–	–	10	18
Раздел 4. Актуальные проблемы правового и организационного обеспечения информационной безопасности.	4	–	–	6	10
Раздел 5. Особенности организационно-правового обеспечения защиты информационных систем.	4	–	–	5	9
Раздел 6. Юридическая ответственность за правонарушения в информационной сфере.	4	–	–	5	9
ИТОГО ЗА СЕМЕСТР	30	–	–	42	72

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

1. Основное содержание понятия «обеспечение информационной безопасности» человека на территории Российской Федерации; коммерческой и некоммерческой организаций; федерального органа исполнительной власти.
2. Функциональная направленность правового режима информационной безопасности для сети общего пользования.
3. Функциональная направленность организационного режима информационной безопасности публичной библиотеки.
4. «Информационное противоборство» и причины его возникновения.
5. Проявления «информационного противоборства» в информационно-технической области.
6. Правовые средства противодействия вредоносному использованию информационных технологий государствами.
7. Правовые средства противодействия использования системы массовой информации для вмешательства во внутренние дела других государств.

8. Государственная политика в области обеспечения национальной безопасности.
9. Стратегические национальные приоритеты России в области национальной безопасности.
10. Приоритеты устойчивого развития общества.
11. Факторы, обуславливающие влияние информационной безопасности на национальную безопасность.
12. Основные содержания понятия «информационная инфраструктура».
13. Угрозы безопасности информационной инфраструктуре.
14. Общая структура правовых средств противодействия угрозам безопасности информационной инфраструктуры.
15. Основные формы существования и свойства информации.
16. Особенности основных видов информации как объектов обеспечения безопасности.
17. Основные угрозы безопасности информации и способы их возможного проявления.
18. Основные источники права в области обеспечения безопасности информации.
19. Понятие «правового режима безопасности информации» и его содержание.
20. Содержание организационного обеспечения информационной безопасности Российской Федерации.
21. Система организационного обеспечения информационной безопасности
22. Основные уполномоченные федеральные органы исполнительной власти в области обеспечения информационной безопасности.
23. Содержание права на доступ к информации и его ограничение в целях защиты интересов личности, общества и государства.
24. Содержание понятия тайны.
25. Классификация тайн.
26. Определение и признаки государственной тайны.
27. Порядок отнесения сведений к государственной тайне и их засекречивания.
28. Распоряжение сведениями, составляющими государственную тайну.
29. Процедура допуска к государственной тайне.
30. Осуществление контроля и надзора за обеспечением защиты государственной тайны.
31. Понятие коммерческой тайны и признаки информации, составляющей коммерческую тайну.
32. Права и обязанности обладателя информации, составляющей коммерческую тайну.
33. Ответственность за нарушение законодательства о коммерческой тайне.
34. Понятие и виды персональных данных.
35. Принципы и условия обработки персональных данных.
36. Права и обязанности оператора при обработке персональных данных.
37. Контроль и надзор за обработкой персональных данных.
38. Полномочия государственного органа, осуществляющего контроль и надзор за обработкой персональных данных.
39. Ответственность за нарушение положений законодательства о персональных данных.
40. Проблема правового режима служебной тайны.
41. Содержание конституционного права на информацию и его ограничения.
42. Понятие экстремистских материалов, согласно действующему законодательству Российской Федерации.
43. Основные положения российского законодательства о противодействии распространению экстремистских материалов.

44. Порядок ограничения доступа к информационным ресурсам в сети Интернет, распространяющих экстремистские материалы.
45. Ответственность за распространение экстремистских материалов.
46. Информация, запрещённая к распространению среди детей.
47. Информация, ограниченная к распространению среди детей.
48. Требования, касающиеся защиты детей от информации, причиняющей вред их здоровью и развитию, закреплённые в законодательстве о средствах массовой информации.
49. Требования к обороту информационной продукции, содержащей информацию, запрещённую или ограниченную к распространению среди детей.
50. Основные положения российского законодательства о защите детей от информации, причиняющей вред их здоровью и развитию, распространяемой посредством информационно-телекоммуникационных сетей.
51. Контроль за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и/или развитию.
52. Ответственность за нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и развитию.
53. Особенности информационных отношений в сети Интернет.
54. Правовые основания мониторинга и блокирования доступа к информационной сети Интернет.
55. Особенности организационно-правового обеспечения управления защитой общегосударственных информационно-телекоммуникационных систем.
56. Правовые нормы и обязательные требования по защите информации в автоматизированных системах.
57. Основные требования по созданию защищённой автоматизированной системы.
58. Основное содержание технического задания на создание автоматизированной системы в защищённом исполнении.
59. Основной состав комплексной системы защиты информации автоматизированной системы.
60. Осуществление контроля и регистрации действий пользователей и событий информационной безопасности автоматизированной системы согласно нормативным правовым актам РФ и служебным документам.
61. Особенности обеспечения информационной безопасности автоматизированных систем в условиях модернизации информационной инфраструктуры судебной системы России.
62. Сущность реализации принципа единства судебной системы в информационно-телекоммуникационной сфере и обеспечения понятийного единства в области обеспечения информационной безопасности судопроизводства.
63. Виды юридической ответственности за правонарушения в информационной сфере.
64. Отличия дисциплинарной, административной и уголовной ответственности за правонарушения в информационной сфере.
65. Классификация преступлений в информационной сфере.
66. Особенности ответственности субъектов сети Интернет за преступления в информационной сфере.

7.2. Образец содержания экзаменационного билета (при наличии экзамена по дисциплине)

В случае ведения учебного процесса с использованием электронного обучения и дистанционных образовательных технологий, содержание билета может отличаться от приведенного.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Донецкий государственный университет

Физико-технический факультет

Кафедра радиофизики и инфокоммуникационных технологий

Программа высшего образования	Программа бакалавриата
Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Форма обучения	Очная
Семестр	7
Дисциплина	Организационное и правовое обеспечение информационной безопасности

Экзаменационный билет № 1

1. Основное содержание понятия «обеспечение информационной безопасности» человека на территории Российской Федерации; коммерческой и некоммерческой организаций; федерального органа исполнительной власти.
 2. Ответственность за нарушение законодательства о коммерческой тайне.
 - 3.
- (все вопросы и задания билета)

Утверждено на заседании кафедры радиофизики и инфокоммуникационных технологий,
протокол № ___ от __.__.202__ г.

Заведующий кафедрой

В.В. Данилов

Экзаменатор

А.В. Голубцов

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

8.1. Семестр 1

Номера разделов	Виды работ	Максимальное количество баллов
1-3	Организационно-учебная работа в аудитории	20
	Самостоятельная работа	40
ИТОГО		60
Зачёт		40
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет

90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в корпусе №4 ДонГУ (г. Донецк, пр. Театральный, 13). Для проведения лекционных и практических занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.405).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511239> (дата обращения: 19.04.2024).

2. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/510644> (дата обращения: 19.04.2024).

3. Кубанков, А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект : учебное пособие / А. Н. Кубанков, Н. Н. Куняев ; под редакцией А. В. Морозов. — Москва : Всероссийский государственный университет юстиции (РПА Минюста России), 2014. — 78 с. — ISBN 978-5-89172-850-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/47262.html> (дата обращения: 19.04.2024). — Режим доступа: для авторизир. пользователей

11.2. Дополнительная литература

4. Кожуханов, Н. М. Правовые основы информационной безопасности : учебное пособие / Н. М. Кожуханов, Е. С. Недосекова. — Москва : Российская таможенная академия, 2013. — 88 с. — ISBN 978-5-9590-0725-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/69749.html> (дата обращения: 19.04.2024). — Режим доступа: для авторизир. пользователей.

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. **Национальная электронная библиотека (НЭБ):** федеральная государственная информационная система / Министерство Культуры РФ; Российская

государственная библиотека. – Москва, 2019- . – URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный, подписка. Необходима установка программного обеспечения. – Текст: электронный.

2. **eLIBRARY.RU**: научная электронная библиотека: сайт. – Москва, 2000- . – URL: <https://elibrary.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

3. Научная электронная библиотека «**КиберЛенинка**»: сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/>. – Режим доступа: свободный. – Текст: электронный.

4. Электронно-библиотечная система «**Лань**»: [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

5. **ЭБС Юрайт**: электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

6. **Электронно-библиотечная система ДонГУ**: сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный. – Текст: электронный.

7. **Электронный каталог** Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: 01.09.2023). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.

8. **Электронный архив ДонГУ**: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения)