

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Артеменков Михаил Николаевич  
Должность: Ректор  
Дата подписания: 07.10.2026 12:25:58  
Уникальный программный ключ:  
a63b74166e8f4fc17bd1e0462725f79e393bdfd9

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Смоленский государственный университет»  
Кафедра информатики

«Утверждаю»  
Проректор по учебно-методической деятельности  
\_\_\_\_\_ Ю.А. Устименко  
«25» декабря 2025 г.

**Рабочая программа дисциплины  
Б1.В.02.ДВ.01.01 Основы информационной безопасности**

Направление подготовки **44.03.05 Педагогическое образование (с двумя профилями подготовки)**

Направленность (профиль) **Математика, Физика и информатика**

Форма обучения: очная

Курс – 5

Семестр – 9

Всего зачетных единиц – 2, часов – 72

Форма отчетности: зачет – 9 семестр

Программу разработал: кандидат физико-математических наук, доцент Кристалинский В.Р.

Одобрена на заседании кафедры  
«20»ноября 2025 г., протокол № 5

Заведующий кафедрой \_\_\_\_\_ С.В. Козлов

Смоленск  
2025

## 1. Место дисциплины в структуре ОП

Дисциплина «Основы информационной безопасности» относится к дисциплинам по выбору, формируемой участниками образовательных отношений, основной образовательной программы по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), направленность (профиль) образовательной программы: Математика, Физика и информатика. При изучении данной дисциплины необходимы компетенции студентов, сформированные при изучении таких дисциплин, как «Алгоритмы и структуры данных», «Программирование», «Практикум по решению задач на ЭВМ».

В современных условиях, в связи с расширением сферы применения информационных технологий возрастают угрозы, связанные с неправомерным доступом к информации, содержащей государственную или иную охраняемую законом тайну, персональные данные граждан, несанкционированным внесением изменений в информационные системы, противоправными действиями в сети Интернет в отношении детей и подростков.

Будущему специалисту важно знать существующие угрозы в сфере информационной безопасности и уметь им противодействовать. Поэтому компетенции, сформированные при изучении дисциплины, необходимы для написания выпускной квалификационной работы бакалавра и его дальнейшей профессиональной деятельности.

В связи с этим курс «Информационная безопасность» занимает важное место в предметной подготовке бакалавров по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки), направленность (профиль) образовательной программы: Математика, Физика и информатика.

Изучение курса основано на традиционных методах высшей школы, тесной взаимосвязи со смежными курсами.

## 2. Планируемые результаты обучения по дисциплине

| Компетенция                                                                                                                                                                                                | Индикаторы достижения                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ПК-6.</b> Способен использовать научные знания в предметной области (информатика) в процессе формирования предметной компетенции обучающихся в рамках реализации основной общеобразовательной программы | <b>Знать:</b> назначение, структуру и содержание курса информатики, современное состояние и перспективы развития информатики как учебной дисциплины, ее место и роль, фундаментальное ядро современного школьного курса информатики, принципы построения методической системы обучения информатике, ее основных компонентов. <b>Уметь:</b> анализировать цели и содержание школьного курса информатики, проектировать образовательный процесс, использовать дидактический потенциал средств информационных технологий в реализации образовательного процесса по курсу информатики;<br><b>Владеть:</b> основными видами профессиональной деятельности учителя информатики, профессиональными навыками реализации методики обучения основным разделам курса информатики, современными информационно-коммуникационными средствами для эффективного осуществления профессиональной деятельности. |

## 3. Содержание дисциплины

**Основные составляющие информационной безопасности.** Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.

**Криптографические способы защиты информации.** Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard.

**Антивирусная защита.** Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы.

**Сетевая безопасность.** Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS.

#### 4. Тематический план

| № п/п        | Разделы и темы                                     | Всего часов | Формы занятий |                      |                        |
|--------------|----------------------------------------------------|-------------|---------------|----------------------|------------------------|
|              |                                                    |             | лекции        | лабораторные занятия | самостоятельная работа |
| 1            | Основные составляющие информационной безопасности. | 8           | 2             | —                    | 6                      |
| 2            | Криптографические способы защиты информации        | 28          | 6             | 16                   | 6                      |
| 3            | Антивирусная защита                                | 18          | 4             | 8                    | 6                      |
| 4            | Сетевая безопасность                               | 18          | 4             | 8                    | 6                      |
| <b>ИТОГО</b> |                                                    | <b>72</b>   | <b>16</b>     | <b>32</b>            | <b>24</b>              |

#### 5. Виды образовательной деятельности

##### Занятия лекционного типа

**Лекция №1. Основные составляющие информационной безопасности.** Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты

информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.

**Лекция №2. Криптографические способы защиты информации.** Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля.

**Лекция №3. Криптографические способы защиты информации.** Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка.

**Лекция №4. Криптографические способы защиты информации.** Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard.

**Лекция №5. Антивирусная защита.** Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ.

**Лекция №6. Антивирусная защита.** Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы.

**Лекция №7. Сетевая безопасность.** Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения.

**Лекция №8. Сетевая безопасность.** Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS.

#### **Занятия семинарского типа**

#### **Лабораторные занятия.**

**Лабораторное занятие № 1-2.** *Программирование алгоритма шифра Цезаря*

**Цель занятия:** разработать программу, реализующую шифр Цезаря

Задание для аудиторной работы

**Задание.** Построить программу, реализующую шифр Цезаря.



#### **Лабораторное занятие № 3 -4. Программирование алгоритма шифра Полибия**

**Цель занятия:** разработать программу, реализующую шифр Полибия

Задание для аудиторной работы

**Задание.** Построить программу, реализующую шифр Полибия.

#### **Лабораторное занятие № 5-6. Программирование алгоритма шифра Lucifer**

**Цель занятия:** разработать программу, реализующую шифр Lucifer

Задание для аудиторной работы

**Задание.** Построить программу, реализующую шифр Lucifer.

#### **Лабораторное занятие № 7-8. Программирование алгоритма шифра DES**

**Цель занятия:** разработать программу, реализующую шифр DES

Задание для аудиторной работы

**Задание.** Построить программу, реализующую шифр DES.

#### **Лабораторное занятие № 9-12. Знакомство со средствами антивирусной защиты.**

**Цель занятия:** Ознакомить студентов со средствами антивирусной защиты

Задание для аудиторной работы

Задание 1. Найти в сети Internet информацию о средствах антивирусной защиты. Данные записать в отчет.

Задание 2. Осуществить проверку различными антивирусными средствами флеш-карты. Результат записать в отчет.

#### **Лабораторное занятие № 13-16. Программирование алгоритма построения электронной цифровой подписи.**

**Цель занятия:** разработать программу, реализующую алгоритм построения электронной цифровой подписи.

Задание для аудиторной работы

**Задание.** Построить программу, реализующую алгоритм построения электронной цифровой подписи.

Задания для лабораторных работ по дисциплине «Информационная безопасность» в логистике» предоставляется студентам на занятиях в электронном виде.

#### **Самостоятельная работа**

Самостоятельная работа направлена на углубление и закрепление знаний студентов и развитие их практических умений. Она заключается в работе с лекционными материалами, поиске и обзоре литературы и электронных источников, информации по заданным темам курса, опережающей самостоятельной работе, в изучении тем, вынесенных на самостоятельную проработку, подготовке к лабораторным занятиям.

Самостоятельная внеаудиторная работа студентов состоит в:

- проработке лекционного материала, составлении конспекта лекций по темам, вынесенным на самостоятельное изучение;
- выполнении заданий для самостоятельной работы.

#### **Темы для самостоятельного изучения**

1. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
2. Шифрование с помощью аналитических преобразований.
3. Модульная арифметика.
4. Методы защиты от вредоносных программ.
5. Антивирусные комплексы.
6. Основы построения локальной компьютерной сети.

7. Управление ключами шифрования и безопасность сети.
8. Цифровая подпись.
9. Система обнаружения вторжений (IDS).
10. Контроллеры целостности файлов.

### **Задания для самостоятельной работы**

- Задание 1. Проанализировать угрозы для личного цифрового пространства.  
Задание 2. Разработать программу-менеджер надежных паролей.  
Задание 3. Разработать программное приложение для распознавания фишинговых атак.  
Задание 4. Настроить уровни безопасности браузера и ОС.  
Задание 5. Разработать программу аналитики политики ИБ для малого бизнеса.

## **6. Критерии оценивания результатов освоения дисциплины (модуля)**

### **6.1. Оценочные средства и критерии оценивания для текущей аттестации**

#### **Теоретические вопросы**

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Что понимается под средствами защиты государственной тайны?
4. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
5. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
6. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
7. Что такое криптография?
8. Что такое криптографический ключ?
9. Что такое криптографическая система?
10. Что такое шифр?
11. Как классифицируются алгоритмы шифрования?
12. Что такое криптостойкость?
13. Какие требования предъявляют к шифрам?
14. Что такое криптоанализ?
15. В чем заключается фундаментальное правило криптоанализа?
16. Что такое криптографическая атака?
17. Каковы виды криптографических атак?
18. Чем различаются блочные и поточные шифры?
19. Описать алгоритм работы сети Файстеля.
20. Как работает SP-сеть?
21. Описать алгоритм работы криптосистемы Lucifer.
22. Что такое асимметричные криптосистемы?
23. Каковы особенности асимметричных криптосистем?
24. Что такое однонаправленная функция? Примеры однонаправленных функций.
25. Как работает криптосистема RSA? Привести пример.
26. Как работает алгоритм Диффи-Хеллмана? Привести пример.
27. Как работает алгоритм Эль-Гамала? Привести пример.
28. Какие злоумышленные действия могут производиться с электронными документами?
29. Что такое электронная цифровая подпись?
30. Описать алгоритм электронной цифровой подписи RSA.
31. Какие процедуры включает система ЭЦП?
32. Какую информацию содержит ЭЦП?
33. Что такое стандарты и спецификации в области информационной безопасности?

34. Какой документ называется «Оранжевой книгой»?
35. По каким критериям оценивается степень доверия, которую можно оказать информационной системе?
36. Что такое доверенная вычислительная база?
37. Что такое ядро и периметр безопасности?
38. Какие элементы должна включать в себя политика безопасности?
39. Что такое средства подотчетности?
40. Какие классы безопасности определены в «Оранжевой книге»?
41. Что такое рекомендации X.800
42. Какие сервисы безопасности выделяются в этих рекомендациях?
43. Какие механизмы используются для реализации этих функций?
44. На какие направления распределяется администрирование средств безопасности?
45. Что такое «Общие требования»?
46. Что такое класс, семейство, компонент и элемент?
47. Что такое профиль защиты и задание по безопасности?
48. Каковы классы функциональных требований «Общих критериев»?
49. Каковы оценочные уровни доверия?
50. Каков основной критерий классификации межсетевых экранов согласно требованиям Гостехкомиссии России?
51. Что такое вредоносные программы?
52. Как распространяются вредоносные программы?
53. Что такое уязвимость?
54. Каковы могут быть последствия заражения вредоносными программами?
55. Какими могут являться последствия заражения?
56. Каковы типы вредоносных программ?
57. Что такое компьютерные вирусы и какими они бывают?
58. Что такое сетевой червь?
59. Что такое троян?
60. Каковы жизненные циклы вирусов, червей и троянов?
61. Какие еще бывают вредоносные программы?
62. Какова юридическая ответственность за распространение вредоносных программ?
63. Что такое удаленная атака?
64. Каковы основные причины уязвимости хостов сети?
65. Что такое анализ сетевого трафика?
66. Что такое подмена доверенного объекта или субъекта РВС?
67. Как осуществляется внедрение ложного объекта?
68. Как ложный объект может быть использован для организации удаленной атаки?
69. Что такое удаленная атака «отказ в обслуживании» и какие они бывают?
70. Какие типовые уязвимости позволяют реализовать успешные удаленные атаки?
71. Как ложный ARP-сервер позволяет осуществлять удаленную атаку «Ложный объект РВС»?
72. Что такое DNS-сервер?
73. Как осуществляется внедрение ложного DNS-сервера путем перехвата DNS-запроса?
74. Как осуществляется внедрение ложного DNS-сервера путем создания направленного «шторма» ложных DNS-ответов на атакуемый хост ?
75. Как осуществляется внедрение в сеть ложного сервера?
76. Как создается ложный маршрутизатор?
77. Как осуществляется подмена субъекта TCP-соединения?
78. Как нарушается работоспособность хоста?
79. Что такое межсетевой экран?
80. Каковы виды межсетевых экранов?
81. Что такое межсетевые экраны прикладного уровня?
82. Что такое межсетевые экраны с пакетной фильтрацией?

83. Что такое гибридные межсетевые экраны?
84. Что такое виртуальная частная сеть и какими характеристиками она обладает?
85. Что такое пользовательская VPN?
86. Что такое узловая VPN?
87. Каковы технологии функционирования VPN?
88. Каковы типы систем VPN?
89. Что такое IDS?
90. Каковы цели использования IDS?
91. Каковы типы IDS?
92. Какие бывают датчики IDS?
93. Что такое сетевая IDS?
94. Каковы действия при обнаружении вторжения?
95. Что такое цифровой сертификат?
96. Что такое бюро сертификатов?
97. Что такое иерархическая модель доверия?
98. Что такое сетевая модель доверия?
99. Как осуществляется сеанс SSL между клиентом и сервером?
100. Каковы преимущества использования электронной почты?
101. Каковы основные риски, связанные с использованием электронной почты?
102. Каковы требования к системам контроля содержимого электронной почты?
103. Что такое политика использования электронной почты?
104. Каковы методики отнесения электронных писем к спаму?

#### **Критерии оценивания ответов на теоретические вопросы**

| Показатель                                                                            | Количество баллов |
|---------------------------------------------------------------------------------------|-------------------|
| 1) Полнота и глубина изложения ответа (усвоенные теории, понятия, факты)              | 1                 |
| 2) Логика изложения материала                                                         | 1                 |
| 3) Примеры использования описанных явлений, теорий и устройств на практике            | 1                 |
| 4) Использование при подготовке ответа на вопрос дополнительных источников информации | 1                 |
| 5) Грамотность и связность ответа                                                     | 1                 |
| Итоговая (суммарная) оценка                                                           | Max - 5           |

#### **Задания для лабораторных занятий**

Задачи по темам курса предложены к каждому лабораторному занятию.

Задания для лабораторных и самостоятельной работ, образцы решений основных типовых задач практики также размещены в системе дистанционного обучения СмолГУ ([www.moodle.smolgu.ru](http://www.moodle.smolgu.ru)).

#### **Образец задания**

1. Построить программу, реализующую шифр Полибия.

#### **Критерии оценивания выполнения лабораторных работ**

Нормы оценивания каждой лабораторной работы:

| №п/п | Структурная часть работы                                                                                      | Количество баллов (*) |
|------|---------------------------------------------------------------------------------------------------------------|-----------------------|
| 1    | Ответ на теоретические вопросы по теме лабораторной работы                                                    | 1 балл                |
| 2    | Демонстрация выполнения конкретного задания, предложенного для самостоятельного решения к лабораторной работе | 2 балла               |

(\*) с возможностью градации до 0,25 балла.

Шкала оценивания. Оценка «зачтено» за лабораторную работу выставляется, если набрано не менее 2 баллов, в противном случае за работу выставляется «не зачтено».

## 6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

### Зачетная работа

1. Построить программу, реализующую шифр Вижинера.
2. Создать описание алгоритма программы.
3. Подготовить документацию по программе.

### Критерии оценивания зачетной работы

Нормы оценивания работы

| № п/п | Структурная часть зачетной работы         | Количество баллов (*) |
|-------|-------------------------------------------|-----------------------|
| 1     | Правильно реализован каждый метод решения | 1 балл                |
| 2     | Анализ результатов                        | 2 балла               |

(\*) Возможна градация в 0,25 балла.

Шкала оценивания работы:

| п/п | Оценка              | Количество баллов |
|-----|---------------------|-------------------|
| 1   | Отлично             | 4,75-5            |
| 2   | Хорошо              | 3,75-4,5          |
| 3   | Удовлетворительно   | 3-3,5             |
| 4   | Неудовлетворительно | менее 3           |

### Критерии получения зачета

Зачет выставляется по результатам работы студента в течение семестра

Для получения зачета студент должен:

- выполнить задания лабораторных работ на оценку «зачтено»;
- ответить на теоретические вопросы на оценку «зачтено»;
- выполнить зачетную работу на оценку не ниже «удовлетворительно».

## 7. Перечень основной и дополнительной учебной литературы

### 7.1 Основная литература

1. Щербак, А. В. Информационная безопасность: учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/569267>.

2. Суворова, Г. М. Информационная безопасность: учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567672>.

### 7.2. Дополнительная литература

1. Зенков, А. В. Информационная безопасность и защита информации: учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567915>.

2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2021. — 473 с. — (Высшее

образование). — ISBN 978-5-534-12474-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469133> (дата обращения: 19.09.2021).

### **7.3. Перечень ресурсов информационно-телекоммуникационной сети Интернет**

1. [www.servernews.ru](http://www.servernews.ru) – информационные материалы о средствах ИТ и средствах обеспечения ИБ
2. [www.fstec.ru](http://www.fstec.ru) – сайт ФСТЭК РФ
3. [www.infosec.ru](http://www.infosec.ru) – группа компаний Информзащита
4. [www.anti-malware.ru](http://www.anti-malware.ru) – аналитический центр Anti-Malware

## **8. Материально-техническое обеспечение**

**Учебная аудитория для проведения занятий лекционного типа**, оснащенная стандартной учебной мебелью, мультимедиапроектором, ноутбуком, колонками и интерактивной доской.

**Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации**, оснащенная стандартной учебной мебелью, компьютерами с доступом к сети «Интернет» и ЭИОС СмолГУ.

**Помещение для самостоятельной работы** – компьютерный класс с доступом к сети «Интернет» и ЭИОС СмолГУ.

## **9. Программное обеспечение**

MicrosoftOpenLicense (WindowsXP, 7, 8, 10, Server, Office 2003-2016), Лицензия 66920993 от 24.05.2016, ежегодное обновление.

Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), Лицензия 66975477 от 03.06.2016, ежегодное обновление.

Операционная система Linux.

KasperskyEndpointSecurityЛицензия 1FB6151216081242, ежегодное обновление.

**Электронные библиотечные системы и электронная информационно-образовательная среда**

Электронная библиотечная система «ЭБС ЮРАЙТ», Договор № 3074 от 15.11.2017, ежегодное обновление.

СДО Русский Moodle 3KL Norm с техническим обслуживанием, Акт на передачу прав №УТДЮ0001785 от 06.12.2016, ежегодное обновление.

Система программирования MS Visual Studio 22 (язык программирования C#).

Поисковые системы сети Интернет.