МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение

высшего образования

«Российский государственный университет им. А.Н. Косыгина

(Технологии. Дизайн. Искусство)»

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Направление(я) подготовки:**29.06.01 Технологии легкой промышленности**

Направленность(и):**Технология кожи, меха, обувных и кожевенно-галантерейных изделий**

Форма обучения: очная

Квалификация: Исследователь. Преподаватель-исследователь

Нормативный срок освоения образовательной программы – 3 года

Кафедра художественного моделирования, конструирования и технологии изделий из кожи

**Москва 2022 г.**

**1. Цели освоения учебной дисциплины**

**Знать:**

* основные понятия и направления в защите компьютерной информации, принципы защиты информации, принципы классификации и примеры угроз безопасности компьютерным системам, современные методы и средства защиты продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности, основные инструменты обеспечения многоуровневой безопасности в информационных системах.

**Уметь:**

* конфигурировать встроенные средства безопасности в операционной системе, проводить анализ защищенности компьютера и сетевой среды; выявлять угрозы информационной безопасности; устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; использовать нормативные правовые документы по информационной безопасности.

**Владеть:**

* методами аудита безопасности информационных систем, методами системного анализа информационных систем; навыками определения угроз информационной безопасности; приемами разработки политики безопасности предприятия; навыками использования методов и средств обеспечения информационной безопасности.

**2.Место учебной дисциплины в структуре программы аспирантуры**

Дисциплина «Информационная безопасность» включена в Вариативную часть 1 Дисциплины по выбору Б1.В.ДВ.1, семестр 4.

Дисциплина базируется на знаниях, умениях и навыках, полученных при освоении предыдущих дисциплин: Информационные процессы и системы, Дискретная математика, Теория вероятностей и математическая статистика, Операционные системы, Информационные системы и технологии, Проектирование информационных систем, Информатика и программирование; Вычислительные системы, сети и телекоммуникации.

**3.Компетенции, формируемые в результате освоения учебной дисциплины**

**Таблица 1**

|  |  |  |
| --- | --- | --- |
| Код и содержание компетенции | Критерии результатов обучения | Технологииформированиякомпетенций |
| **УК-1-** способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях | **Знать:** способы постановки исследовательских задач и выбора путей их решения;**Уметь:** логически мыслить, анализировать, обобщать, критически осмысливать информацию**Владеть:** навыками постановки исследовательских задач и выбора путей их решения критического анализа и оценки современных научных достижений, генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях; | *лекции (Л),* *практические* *занятия (ПЗ),* *самостоятельная* *работа (СР),* |
| **УК-2** способностью проектировать иосуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки | **Знать:** способы проектирования и комплексных исследований в том числе междисциплинарных**Уметь:** проектировать иосуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения**Владеть:** навыками применения современных способов проектирования и осуществления комплексных исследований, в том числе междисциплинарных, на основе целостного системного научного миро-воззрения с использованием знаний в области истории и философии науки | *лекции (Л),* *практические* *занятия (ПЗ),* *самостоятельная* *работа (СР)* |
| **ОПК-2** - владением методологией исследований в области, соответствующей направлению подготовки | **Знать:** требования к защите информации определенного типа**Уметь:** подобрать и обеспечить защиту информации**Владеть:** современными средствами защиты информации методологией исследований в области, соответствующей направлению подготовки | *лекции (Л),* *практические* *занятия (ПЗ),* *самостоятельная* *работа (СР),* |
| **ОПК-3**-владением культурой научного исследования, в том числе с использованием новейших информационно-коммуникационных технологий | **Знать:** методы, способы и средства получения, хранения и переработки информации, принципы построения современных информационно-коммуникационных технологий;**Уметь:** использовать источники технической, экономической и управленческой информации;**Владеть:** навыками применения современных методов сбора, обработки и анализа данных, культурой научного исследования, в том числе с использованием новейших информационно-коммуникационных технологий | *лекции (Л),* *практические* *занятия (ПЗ),* *самостоятельная* *работа (СР),* |
| **ОПК-4 -**способностью к применению эффективных методов исследования в самостоятельной научно-исследовательской деятельности в области, соответствующей направлению подготовки | **Знать:** виды и источники угроз безопасности информации для различных профессиональных областей; законодательную базу в сфере информационной безопасности;основные требования к информационной безопасности.**Уметь:** определять актуальные источники угроз безопасности для различныхПрофессиональных областей.**Владеть:** навыками применения современных средств информационной безопасности, эффективных методов исследования в самостоятельной научно-исследовательской деятельности в области, соответствующей направлению подготовки | *лекции (Л),* *практические* *занятия (ПЗ),* *самостоятельная* *работа (СР)* |
| **ПК-3-** способность к разработке методов оптимизации кожевенного, обувного и кожгалантерейного производства на основе научного прогнозирования, применения математических методов и вычислительной техники и т.д. | **Знать:** методы, способы и средства получения, хранения и переработки информации для оптимизации кожевенного, обувного и кожгалантерейного производства**Уметь:** использовать методы, способы и средства получения и переработки информации для оптимизации кожевенного, обувного и кожгалантерейного производства на основе научного прогнозирования, применения математических методов и вычислительной техники и т.д.**Владеть:** навыками применения современных средств для разработки методов оптимизации кожевенного, обувного и кожгалантерейного производства на основе научного прогнозирования, применения математических методов и вычислительной техники и т.д. | *лекции (Л),* *практические* *занятия (ПЗ),* *самостоятельная* *работа (СР)* |

**4.Объем и содержание дисциплины**

**4.1. Объем дисциплины**

**Таблица 2**

|  |  |
| --- | --- |
| **Показатель объема дисциплины** | **Трудоемкость** |
|
| Объем дисциплины в зачетных единицах | 4 |
| Объем дисциплины в часах | 144 |
| Лекции (ч) | 36 |
| Практические занятия (семинары) (ч) | 36 |
| Самостоятельная работа (ч) | 45 |
| Контроль (ч) | 27 |
| Форма контроля (зач. /экз.) | экзамен |

**4.2 Содержание разделов учебной дисциплины**

**Таблица 3**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование раздела учебной дисциплины**  | **Лекции** | **Наименование практических (семинарских) занятий** | **Оценочные средства** |
| **№ и тема лекции** | **Трудоемкость, час** | **№ и тема практического занятия** | **Трудоемкость, час** |
| Общие вопросы информационной безопасности |  Понятия информация, информационная система, информационная безопасность. Средства защиты информации.. Требования к защите информации.  | 2 | Основные понятия и общеметодологические принципы теории информационнойбезопасности | 2 | Реферат, коллоквиум, индивидуальные домашние задания |
|  Понятие угрозы. Классификация угроз информационной безопасности. | 2 | Понятие и виды угроз информационной безопасности  | 2 |
| Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации. Международные стандарты информационного обмена | 2 | Отечественные и зарубежные стандарты в области информационной безопасности. | 2 |
| Криптографические методы защиты информации |  Основные понятия и классификация средств криптографической защиты информации. | 2 | Основные понятия и общеметодологические принципы теории информационнойбезопасности | 2 | Реферат, коллоквиум, индивидуальные домашние задания |
| Математические основы криптографии. Обеспечиваемая шифром степень защиты. | 2 | Методы и средства обеспечения информационной безопасности компьютерныхсистем | 2 |
| Криптоанализ и атаки на криптосистемы. | 2 | Формальные модели безопасности автоматизированных систем | 2 |
|  Симметричные криптосистемы. Криптографические генераторы случайных чисел. | 2 | Принципы построения симметричные криптосистем | 2 |
|  Алгоритмы шифрования ГОСТ 28147-89, DES. | 2 | Провести анализ криптосистемы DES. | 2 |
| . Ассиметричные криптосистемы. Алгоритмы шифрования на основе задачи о рюкзаке, RSA. | 2 | Провести анализ криптосистемы RSA | 2 |
| Электронная цифровая подпись. Функции хэширования. | 2 | Российские и международные стандарты формирование цифровой подписи . | 2 |
| Алгоритмы цифровой подписи ГОСТ 34.10.-2001, ГОСТ 34.11-94и Эль Гамаля. | 2 | Сравнительный анализ различных методов формирования цифровой подписи.  | 2 |
| Архитектура защищенных информационных систем |  Основные технологии построения защищенных информационных систем.  | 2 | Рассмотреть технологию построения защищенных информационных систем | 2 | Реферат, коллоквиум, индивидуальные домашние задания |
| Виды возможных нарушений информационных систем. Основные положения теории информационной безопасности информационных систем. | 2 | Механизмы защиты информации в автоматизированных системах  | 2 |
| Функции защиты информации. | 2 | Методы и критерии оценки защищенности компьютерных систем | 2 |
|  Аутентификация и идентификация. Аутентификация на основе симметричных алгоритмов.  | 2 | Сравнительный анализ методов аутентификация пользователей на основе симметричных алгоритмов.  | 2 |
| Аутентификация на основе ассиметричных алгоритмов. | 2 | Сравнительный анализ методов аутентификация пользователей на основе асимметричных алгоритмов. | 2 |
|  Классы задач защиты информации. Архитектура систем защиты информации.  | 2 | Критерии оценки защищенности компьютерных систем.. | 2 |
|  Ядро и ресурсы средств защиты информации. Стратегии защиты информации. | 2 | Формальные модели безопасности автоматизированных систем | 2 |
| **ВСЕГО часов в семестре** | **.**  | **36** |  | **36** | **Экзамен** |

**5.Самостоятельная работа обучающихся**

**Таблица 4**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела учебной дисциплины**  | **Содержание самостоятельной работы** | **Трудоемкость в часах** |
| 1 | Общие вопросы информационной безопасности | Изучение лекционного материала, научной и учебной литературы | 15 |
| 2 | Криптографические методы защиты информации | 15 |
| 3 | Архитектура защищенных информационных систем | 15 |
| 4 | Контроль | Подготовка к экзамену | 27 |
| **ВСЕГО часов в семестре:** | **72** |

**6.Образовательные технологии**

При освоении дисциплины «Информационная безопасность»используются следующие образовательные технологии:

- лекции (Л),

- практические занятия (ПЗ),

- самостоятельная работа (СР),

**7.Фонд оценочных средств для проведения текущей и промежуточной аттестации по дисциплине**

**7.1 Примерная тематика курсовых проектов (работ) –** не предусмотрены**.**

**7.2 Примеры используемых оценочных средств для текущего контроля**

**Реферат** - продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

**Варианты тем рефератов:**

1. Требования к комплексным системам защиты информации

2. Атаки на криптосистемы

3. Шифры замены. Сравнительный анализ

4. Шифры перестановки. Сравнительный анализ

5. Сравнительный анализ режимов шифрования DES и ГОСТ 28147-89.

6. Сравнительный анализ алгоритмов шифрования RSA и Эль-Гамаля

7. Алгоритм цифровой подписи Эль Гамаля

8. Российский стандарт цифровой подписи

9. Российский стандарт хэш-функции

10. Управление криптографическими ключами

11. Обеспечение безопасности в приложениях MS Word и Excel

**Вопросы для коллоквиума** по дисциплине Информационная безопасность.

1. Понятия «информационная безопасность» и «защита информации». Основные составляющие информационной безопасности.

2. Объекты защиты. Категории и носители информации.

3. Средства защиты информации.

4. Криптография. Основные термины и определения.

5. Классификация криптографических систем.

6. Шифры замены. Классификация и основные методы шифрования.

7. Шифры перестановки. Классификация и основные методы шифрования.

8. Шифры гаммирования. Классификация и основные методы шифрования.

9. Схема режима шифрования DES.

10. Схема режима шифрования простой замены ГОСТ 28147-89.

11. Шифрование с открытым ключом. Основные понятия.

12. Алгоритм шифрования RSA.

13. Алгоритм шифрования Эль-Гамаля.

14. Алгоритм шифрования на основе задачи об укладке ранца.

15. Эллиптические кривые. Основные понятия. Сложение и умножение точки.

16. Алгоритм шифрования на основе эллиптических кривых.

17. Хэш-функции. Основные понятия и разновидности.

18. Криптографические протоколы. Основные понятия.

19. Протоколы обмена ключами.

20. Протоколы аутентификации. Разновидности и краткая характеристика.

21. Парольная идентификация/аутентификация.

22. Протокол идентификации/аутентификации на основе шифрования с открытым ключом.

23. Сервер аутентификации Kerberos.

24. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.

25. ЭЦП на базе алгоритма RSA.

26. Алгоритм цифровой подписи ГОСТ 34.10-94.

27. Алгоритм цифровой подписи ГОСТ 34.10-2001.

28. Протоколы контроля целостности. Разновидности и краткая характеристика.

29. Основные сведения о криптоанализе и атаки на криптосистемы.

**Темы для индивидуальных домашних заданий** по дисциплине Информационная безопасность

1. Реализовать шифрование и дешифрацию содержимого файла по методу Цезаря с ключевым словом.

2. Реализовать шифрование и дешифрацию файла с использованием метода биграмм.

3. Реализовать шифрование и дешифрацию файла с использованием квадрата Кардано размером 4х4.

4. Реализовать шифрование и дешифрацию файла с использованием перестановочного шифра с ключевым словом.

5. Реализовать систему симметричного блочного шифрования ГОСТ 28147-89.

6. Реализовать систему симметричного блочного шифрования DES

7. Реализовать систему шифрования на основе задачи о рюкзаке

8. Реализовать систему шифрования RSA

9. Реализовать систему постановки цифровой подписи по алгоритму Эль Гамаля

**Критерии оценивания:**

**Рефераты**

|  |  |
| --- | --- |
| Оценка | Критерии оценки |
| отлично | Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, осуществлены обзор источников и анализ различных точек зрения на рассматриваемую проблему, иваемую проблему и проблему и аконфликтует.ольной работылогично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к оформлению, даны правильные ответы на дополнительные вопросы при защите реферата |
| хорошо | Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; нарушена логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; в списке использованных источников отсутствуют наиболее авторитетные и общепризнанные издания и информационные ресурсы; на дополнительные вопросы при защите даны неполные ответы |
| удовлетворительно | Имеются существенные отступления от требований к реферированию. В частности, тема освещена лишь частично; отсутствует логическая последовательность в суждениях; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; при защите реферата обучающийся затрудняется с формулировкой основных выводов по работе |
| неудовлетворительно | Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы; обнаружен факт полного заимствования материала реферата без ссылок на источник заимствования |

**Коллоквиум**

Оценка «Неудовлетворительно» ставится, если аспирант не сумел продемонстрировать знания ключевых положений курса.

Оценка «Удовлетворительно» ставится, если аспирант продемонстрировал уверенное знание ключевых положений курса.

Оценка «Хорошо» ставится, если аспирант продемонстрировал уверенное владение всеми материалами курса.

Оценка «Отлично» ставится, если аспирант продемонстрировал уверенное владение материалами лекционного курса, а также материалами дополнительных источников по теме курса

**Индивидуальные домашние задания**

Оценка «Неудовлетворительно» ставится, если аспирант проявил недостаточность знаний, умений, навыков.

Оценка «Удовлетворительно» ставится, если аспирант проявил отсутствие отдельных знаний, умений, навыков, испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Оценка «Хорошо» ставится, если аспирант продемонстрировал на среднем уровне основные знания, умения, но допускал незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

Оценка «Отлично» ставится, если аспирант продемонстрировал всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, умеет свободно выполнять практические задания, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.

**7.3 Примеры используемых оценочных средств для промежуточной аттестации**

**Перечень вопросов при сдаче экзамена**

1. Какова длина ключа алгоритма DES?

2. Что представляет собой операция по модулю два?

3. Что такое криптология, криптограмма, криптография, криптоанализ?

4. В чем состоит основная идея шифрования данных?

5. В чем различие и в чем сходство шифрования и кодирования?

6. Опишите схему симметричного шифрования информации.

7. Приведите упрощенную схему алгоритма шифрования DES?

8. Приведите упрощенную схему алгоритма расшифрования DES?

9. Приведите схему реализации функции шифрования F.

10. Что такое криптостойкость? Каковы количественные характеристики

криптостойкости?

11. Опишите алгоритм получения 48-битовых ключей K(i).

12. Докажите, что таблица «конечная перестановка» является обратной

по отношению к таблице «начальная перестановка».

13. Опишите упрощенную схему асимметричного шифрования.

14. Какова максимальная длина открытого текста в программе DES?

15. Что такое цена и ценность информации?

16. Что подразумевается под эффективностью защиты информации?

17. Что такое система безопасности?

18. В чем заключаются постулаты безопасности?

19. Чем достигается обеспечение безопасности?

20. Что такое способы защиты информации?

21. В чем состоят цели защиты информации?

22. Охарактеризуйте физические системы защиты информации.

23. В чем проявляются угрозы информации?

24. Что такое информационная безопасность?

25. Что такое защита информации?

26. Перечислите возможные виды утечек информации.

27. Охарактеризуйте методы симметричного шифрования данных.

28. Что называется полным набором вычетов по модулю n (n – целое чис-

ло)?

29. Сформулируйте основные законы модулярной арифметики.

30. Дайте определение величины, обратной целому числу *a* по модулю *n*.

31. Охарактеризуйте основные способы нахождения обратных по модулю

величин.

32. Что такое дискретный логарифм? В чем заключается проблема дис-

кретного логарифмирования?

33. Что такое криптосистема Эль Гамаля?

34. Решение какой задачи лежит в основе реализации криптосистемы Эль

Гамаля?

35. В чем состоят достоинства и недостатки алгоритма Эль Гамаля?

36. Что представляет собой алгоритм шифрования RSA?

37. Какая проблема лежит в основе реализации алгоритма RSA?

38. В чем состоят достоинства и недостатки алгоритма RSA?

39. Докажите корректность алгоритма Эль Гамаля.

40. Докажите корректность алгоритма RSA.

41. В чем состоит системно-концептуальный подход при решении задач

защиты информации в компьютерных системах?

42. Каковы требования к комплексным системам защиты информации?

43. Охарактеризуйте атаки на криптосистемы.

44. Что такое однонаправленная функция? Приведите примеры.

45. Что такое аутентификация? Какова ее цель?

46. Что такое цифровая подпись?

47. Опишите алгоритм цифровой подписи на основе криптосистемы RSA.

48. Что такое хэш-функция? Для каких целей она используется?

49. Чем отличаются методы криптографической защиты данных от других методов защиты информации?

50. Как записывается и что означает операция «исключающего или»?

Как она связана с операцией суммирования по модулю два?

51. Перечислите алгоритмы трех уровней ГОСТ 28147–89.

52. Что такое «основной шаг» криптопреобразования в ГОСТ 28147–89?

53. Что представляет собой «таблица замен» для ключевой информации

в ГОСТ 28147–89?

54. Что представляет собой алгоритм «основного шага» криптопреобра-

зования?

55. Какие алгоритмы входят в «базовые циклы» ГОСТ 28147–89?

56. Каковы режимы работы алгоритмов шифрования ГОСТ 28147–89?

57. В чем заключаются особенности режима шифрования простой заме-

ной?

58. Для каких целей используется режим простой замены в ГОСТ 28147–89?

59. Какие две проблемы решаются с помощью режима гаммирования?

60. Почему алгоритмы зашифрования и расшифрования в режиме гам-

мирования идентичны?

61. Каковы особенности гаммирования как режима шифрования?

62. Почему в режиме гаммирования изменение бита шифрованного тек-

ста на противоположное значение приводит к аналогичному изменению бита открытого текста на противоположное значение? Что дает это свойство злоумышленнику?

63. Чем отличаются режим гаммирования и режим гаммирования с обратной связью?

64. Как влияют искажения шифрованного текста на соответствующий открытый текст в режиме гаммирования и в режиме гаммирования с обратной связью?

65. Как влияют искажения шифрованного текста на соответствующий

открытый текст в режиме простой замены?

66. Сравните DES и ГОСТ 28147–89 по функциональному содержанию и

удобству реализации.

67. Охарактеризуйте источники угроз и сами угрозы в сетевой среде.

68. Каковы основные направления защиты информации в сетях?

69. Какие компоненты могут быть отнесены к стратегии построения

безопасных сетей?

70. В чем состоят принципы построения архитектуры безопасности сети?

71. Что такое гарантированная безопасность? Как она достигается?

72. Охарактеризуйте основные задачи управления безопасностью сети.

73. Кратко охарактеризуйте средства защиты информации в сетях.

74. Опишите общую схему асимметричной криптосистемы.

75. В чем заключается отличие атак на симметричные и асимметричные

криптосистемы?

**Критерии оценки при сдаче экзамена**

Оценка «**отлично**» ставится обучающемуся, ответ которого содержит:

- глубокое знание программного материала, включая как основное содержание лекционного курса и основной литературы, так и сведений из дополнительной учебной и научной литературы; знание концептуально-понятийного аппарата всего курса;

а также свидетельствует о способности:

- самостоятельно критически оценивать основные положения курса; увязывать теорию с практикой.

Оценка «**хорошо**» ставится обучающемуся, ответ которого свидетельствует:

- о полном знании материала по программе и лекционному курсу;

- о знании рекомендованной основной литературы,

а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка «**удовлетворительно**» ставится обучающемуся, ответ которого содержит:

- поверхностные знания важнейших разделов программы и содержания лекционного курса;

- затруднения с использованием научно-понятийного аппарата, терминологии курса и сведений из рекомендованной основной литературы;

- стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

Оценка «**неудовлетворительно**» ставится обучающемуся, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

**8.Учебно-методическое и информационное обеспечение учебной дисциплины**

**8.1 Перечень основной и дополнительной учебной литературы**

**Таблица 5**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Автор(ы) | Наименование издания | Вид издания (учебник, учебное пособие, ….) | Издательство | Год издания |
|
| 1 | 2 | 3 | 4 | 5 | 6 |
| **Основная литература**  |
| 1. | Шаньгин В.Ф. | Информационная безопасность. | Учебное пособие | «ДМК Пресс» | 2014 |
| 2. | Беломойцев Д.Е., Волосатова Т.М.. Радионов С.В. | Основные методы криптографической обработки данных  | Учебное пособие | MГТУ им. Н.Э. Баумана  | 2014 |
| 3. | [Свинарёв Н.А.](http://www.knigafund.ru/authors/31750), [Ланкин О.В.](http://www.knigafund.ru/authors/31751), [Данилкин А.П.](http://www.knigafund.ru/authors/31752), [Потехецкий С.П.](http://www.knigafund.ru/authors/31753), [Перетокин О.И.](http://www.knigafund.ru/authors/31754) | Инструментальный контроль и защита информации | Учебное пособие | ВГУИТ | 2013 |
| **Дополнительная литература** |
| 1 | [Скрипник Д.А.](http://www.knigafund.ru/authors/31511) | [Обеспечение безопасности персональных данных](http://www.knigafund.ru/books/173615) | Учебное пособие | ИНТУИТ | 2011 |
| 2 | [Жуков А.Е.](http://www.knigafund.ru/authors/32709) | Системы блочного шифрования: | Учебное пособие | МГТУ им. Н.Э. Баумана | 2013 |

**8.2. Электронные издания**

**Таблица 6**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Автор(ы) | Наименование издания | Вид издания (учебник, учебное пособие, ….) | Издательство, год издания | Адрес сайта ЭБС или др. источника |
|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | Андрианов В.В., Зефиров СЛ. и др. | Обеспечение информационной безопасности бизнеса | Учебник | М.: Альпина . 2011 | <http://biblioclub.ni/iiidex.php?page=bookc1feid=235577&si-l> |
| 2 | Бирюков А.А. | Информационная безопасность: защита и нападение | Учебник | «ДМК Пресс», 2012. | <http://e.lanbook.com> books element.php?pll\_id=39990 |

**8.3 Перечень ресурсов информационно-телекоммуникационной сети Интернет, электронных образовательных ресурсов локальных сетей РГУ им. А.Н. Косыгина, необходимых для освоения дисциплины**

1. Библиотека РГУ им. А.Н. Косыгина <http://biblio.mgudt.ru/jirbis2/>.

2. Электронно-библиотечная система (ЭБС) «ИНФРА-М» «Znanium.com» <http://znanium.com/>.

3. Реферативная база данных «Web of Science» <http://webofknowledge.com/> .

4. Реферативная база данных «Scopus» <http://www.scopus.com/> .

5. Патентная база данных компании «QUESTEL – ORBIT» <https://www37.orbit.com/#PatentEasySearchPage>.

6. Электронные ресурсы издательства «SPRINGERNATURE» <http://www.springernature.com/gp/librarians>.

7. ООО «ИВИС» <http://dlib.eastview.com/>.

8. Научная электронная библиотека «eLIBRARY.RU» <http://www.elibrary.ru/>.

9. Национальная электронная библиотека («НЭБ») [http://нэб.рф/](http://xn--90ax2c.xn--p1ai/).

10. База данных издательства **«**Wiley**»** http://onlinelibrary.wiley.com/

**9.Материально-техническое обеспечение дисциплины**

|  |  |  |
| --- | --- | --- |
| Наименование специальных помещений и помещений для самостоятельной работы | Оснащенность специальных помещений и помещений для самостоятельной работы | Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа |
| Помещение для проведения занятий семинарского типа,  | Стол преподавательский – 1 шт., доска – 1 шт., , письменный стол – 15 шт., стул – 30 шт., персональный компьютер – 15 шт.. | 1. Microsoft Office Standard 2016 Russian OLPNL Academic Edition, 60 лицензий, артикул 021-10548, Договор бюджетного учреждения с ЗАО «Софт Лайн Трейд» №511/2015 от 15.12.2015г.2. Mat Lab Simulink Math Works, unlimited №DVD10B.3. MicrosoftVisualStudioProfessionalw/MSDNALNGLisSAPkOLPNLAcademicEditionQ1fd, 1 лицензия, артикул 77D-00085, Контракт бюджетного учреждения с ЗАО «Софт Лайн Трейд» №509/2015 от 15.12.2015г. |