**Федеральное государственное бюджетное образовательное**

**учреждение высшего образования**

**«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА   
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ**

**ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ – филиал РАНХиГС**

Кафедра экономики и финансов

|  |  |
| --- | --- |
|  | УТВЕРЖДЕНА  решением методической комиссии по направлениям 38.03.05 «Бизнес-информатика», 09.06.01 «Информатика и вычислительная техника» Северо-Западный институт управления – филиал РАНХиГС  Протокол от «10» мая 2017 г. № 5 |

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Б1.В.ДВ.03.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**

ИБ

*(краткое наименование дисциплины)*

09.06.01 Информатика и вычислительная техника

*(код,наименование направления подготовки)*

«Системный анализ, управление и обработка информации»

*(направленность)*

Исследователь. Преподаватель-исследователь

*(квалификация)*

очная/заочная

*(форма обучения)*

Год набора – 2017

**Автор–составитель:**

Кандидат технических наук, кандидат педагогических наук, доцент, доцент кафедры экономики и финансов Сухостат Валентина Васильевна

Заведующий кафедрой Экономики и финансов

доктор исторических наук профессор Исаев Алексей Петрович

**СОДЕРЖАНИЕ**

|  |
| --- |
| 1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы |
| 1. Объем и место дисциплины (модуля) в структуре образовательной программы |
| 1. Содержание и структура дисциплины (модуля) |
| 1. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю) |
| 1. Методические указания для обучающихся по освоению дисциплины (модуля) |
| 1. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине (модулю) |
| 6.1. Основная литература |
| 6.2. Дополнительная литература |
| 6.3. Учебно-методическое обеспечение самостоятельной работы |
| 6.4. Нормативные правовые документы |
| 6.5. Интернет-ресурсы |
| 6.6. Иные источники |
| 1. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы |

# Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения программы

* 1. **Дисциплина Б1.В.ДВ.03.02 «Информационная безопасность и защита информации» обеспечивает овладение следующими компетенциями:**

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| Код  компетенции | Наименование  компетенции | Код  этапа освоения компетенции | Наименование этапа освоения компетенции |
| ОПК - 2 | владение культурой научного исследования, в том числе с использованием современных информационно-коммуникационных технологий | ОПК-2.2 | умение решать задачи научного исследования на базе системного анализа, использования современных инфокоммуникационных технологий, методов и технологий информационной безопасности |
| ПК-1 | владеть способностью формализации и постановки задач системного анализа, оптимизации, управления, принятия решений и обработки информации | ПК-1.3 | Способность решать задачи системного анализа экономических систем, математической экономики, эконометрики |

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

Таблица 2

|  |  |  |
| --- | --- | --- |
| ОТФ/ТФ  (при наличии профстандарта)/ профессиональные действия | Код этапа освоения компетенции | Результаты обучения |
| Выполнение трудовой функции «Управление информационной безопасностью ресурсов ИТ» в соответствии с обобщенной трудовой функцией профессионального стандарта «Менеджер информационных технологий» - управление ресурсами ИТ. | ОПК-2.2 | **на уровне знаний:**  **Знать:**   * структуру и основные положения нормативной базы РФ и национальных стандартов в области информационной безопасности и защиты информации; * основные каналы несанкционированного доступа к информации; * базовые методы и средства защиты информации от несанкционированного доступа; * современное состояние компьютерной преступности и ответственность за нарушения и преступления в сфере информационной безопасности.   **на уровне умений:**  **Уметь:**   * ориентироваться в нормативно-правовой базе и стандартах в области информационной безопасности и защиты информации; * идентифицировать основные угрозы безопасности ИТ-инфраструктуры современного предприятия; * создавать защищенные учетные записи и защищать электронные документы; * классифицировать компьютерные преступления;   на уровне навыков:  **Владеть:**   * профессиональной терминологией в сфере информационной безопасности и защиты информации; * проблематикой и методологией решения задач управления информационной безопасностью. |
| работа с компьютером как средством управления информацией, работа с информацией из различных источников, в том числе в глобальных компьютерных сетях, способность выполнять обобщенную трудовую функцию по управлению информационной средой на основе профессионального стандарта «Менеджер по информационным технологиям». | ПК-1.3 | На уровне знаний:  Знать:  -понятия и свойства информационной безопасности;  -основные каналы утечки информации, методы и средства защиты и обеспечения информационной безопасности;  -возможности систем обеспечения информационной безопасности;  -методы системного анализа рисков ИТ и информационной безопасности.  На уровне умений:  Уметь:  -идентифицировать угрозы информационной безопасности;  -решать задачи научного исследования на базе системного анализа, использования современных инфокоммуникационных технологий, методов и технологий информационной безопасности;  -исследовать риски и угрозы информационной безопасности.  На уровне владений:  -владеть инструментальными средствами мониторинга информационной безопасности. |

# Объем и место дисциплины в структуре ОП ВО

**Объем дисциплины**

Общая трудоемкость дисциплины составляет 3 зачетных единицы /108 часов.

Таблица 3

|  |  |
| --- | --- |
| Вид работы | Трудоемкость  (в академ.часах) |
| **Общая трудоемкость** | 72 |
| **Контактная работа с преподавателем** | 36 |
| Лекции | 16 |
| Практические занятия | 20 |
| Лабораторные занятия | - |
| **Самостоятельная работа** | 30 |
| Контроль | - |
| Форма текущего контроля | Устный и письменный опрос |
| **Форма промежуточной аттестации** | Зачет |

**Место дисциплины в структуре ОП ВО**

Дисциплина Б1.В.ДВ.03.02 «Информационная безопасность и защита информации» относится к дисциплинам по выбору вариативной части учебного плана образовательной программы по направлению 09.06.01 – Информатика и вычислительная техника, специальность 05.13.01 – Системный анализ, управление и обработка информации. Преподавание дисциплины Б1.В.ДВ.03.02 «Информационная безопасность» основано на дисциплинах – Б1.В.02 «Методы системного анализа»; Б1.В.01 «Информационно-коммуникационные технологии и информационные системы».

Данная дисциплина создаёт необходимые предпосылки для освоения программ таких дисциплин, как Б2.В «Практики по получению профессиональных умений и опыта профессиональной деятельности; научно-исследовательская практика», Б3.В «Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук»

Формой промежуточной аттестации в соответствии с учебным планом является зачет.

# Содержание и структура дисциплины

***Очная форма обучения***

Таблица 4

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование тем (разделов),** | **Объем дисциплины (модуля), час.** | | | | | | **Форма текущего  контроля успеваемости\*\*, промежуточной аттестации\*\*\*** |
| **Всего** | **Контактная работа обучающихся с преподавателем по видам учебных занятий** | | | | **СР** |
| **Л** | **ЛР** | **ПЗ** | **КСР** |
| **Очная форма обучения** | | | | | | | | |
| Тема 1 | Информационная безопасность и защита информации | 10 | 4 | - | 2 |  | 4 | Задание (З) |
| Тема 2 | Технические каналы утечки информации | 8 | 2 | - | 2 |  | 4 | Т |
| Тема 3 | Угрозы несанкционированного доступа к информации | 8 | 2 | - | 2 |  | 4 | Круглый стол/Т |
| Тема 4. | Криптографическая защита информации | 16 | 4 | - | 6 |  | 6 | Д,Т |
| Тема 5. | Методы и средства разграничения и контроля доступа к информации | 12 | 2 | - | 4 |  | 6 | Устный опрос |
| Тема 6. | Системы предотвращения утечки информации из корпоративной информационной системы | 12 | 2 | - | 4 |  | 6 | Круглый стол/Т |
| Промежуточная аттестация | | 6 |  |  |  |  |  | Зачет |
| Всего: | | 72 | 16 |  | 20 |  | 30 |  |

*Примечание:*

*\* – при применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом;*

*\*\* – разработчик указывает необходимые формы текущего контроля успеваемости: курсовые проекты (КП), курсовые работы (КР), контрольные работы (К), опрос (О), тестирование (Т), коллоквиум (Кол), эссе (Эс), реферат (Реф), диспут (Д) и др.*

Используемые сокращения приводятся после таблицы в примечании.

*\*\*\* - разработчик указывает необходимые формы промежуточной аттестации: экзамен (Экз), зачет (За), зачет с оценкой (ЗаО) и др.*

Используемые сокращения приводятся после таблицы в примечании.

**Содержание дисциплины**

**Тема 1. Информационная безопасность и защита информации**

Понятие информационной безопасности. Понятие защиты информации. Правовое понятие тайны. Видя тайн в российском законодательстве. Конфиденциальная информация. Конфиденциальное делопроизводство. Информационная безопасность. Каналы воздействий.

**Тема 2. Технические каналы утечки информации**

Классификация технических каналов утечки информации. Модель и способы утечки по радиоканалу. Модель и способы утечки по электрическому каналу. Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому) каналу. Модель и способы утечки по параметрическому (смешанному)каналу. Модель и способы утечки по оптическому (оптико-электронному) каналу. Модель и способы утечки по каналу ПЭМИН.

**Тема 3. Угрозы несанкционированного доступа к информации**

Классификация угроз несанкционированного доступа (НСД) к информации. Категории нарушителей безопасности информации и их возможности. Общая характеристика уязвимостей. Способы реализации угрозы НСД к информации. Понятие и обобщенная модель нетрадиционного информационного канала. Методы сокрытия информации в текстовых файлах. Методы сокрытия информации в графических файлах. Методы сокрытия информации в звуковых файлах. Методы сокрытия информации в сетевых пакетах и исполняемых файлах.

**Тема 4. Криптографическая защита информации**

Модель криптосистемы. Историография и классификация шифров. Примеры криптографических алгоритмов. Криптосистема с симметричными и несимметричными ключами. Электронная цифровая подпись.

**Тема 5. Методы и средства разграничения и контроля доступа к информации**

Мандатная и дискреционная модели доступа. Процедура идентификации, аутентификации и авторизации. Система паролирования. Системы контроля и управления доступом. Система охраны периметра

**Тема 6. Системы предотвращения утечки информации из корпоративной информационной системы (КИС)**

Принципы комплексной защиты корпоративной информации.

Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети. Понятие и функционал DLP-систем. Объем и структура данных защищаемых DLP-системами. Каналы коммуникаций, контролируемые DLP-системами. Критерии оценки программных продуктов, реализующих функциональность DLP. Примеры DLP-систем. Борьба с инсайдерами.

# Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

**4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.**

В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Таблица 5

|  |  |
| --- | --- |
| Тема (раздел) | Формы (методы) текущего контроля успеваемости |
| Тема 1. Информационная безопасность и защита информации | Устный опрос, деловая игра «Проблемы и приоритеты в сфере информационной безопасности» |
| Тема 2. Технические каналы утечки информации | Защита задания |
| Тема 3. Угрозы несанкционированного доступа к информации | Круглый стол/Тестирование |
| Тема 4. Криптографическая защита информации | Диспут, тестирование |
| Тема 5. Методы и средства разграничения и контроля доступа к информации | Устный опрос |
| Тема 6. Системы предотвращения утечки информации из корпоративной сети | Круглый стол, тестирование |

**4.1.2.** **Зачет проводится с применением следующих методов (средств) :**

Зачет проводится в компьютерном классе. Во время зачета проверяется этап освоения компетенций ОПК - 2.2, а также ПК-1.3

Во время проверки сформированности этапа компетенции ОПК - 2.2, ПК-1.3 оцениваются:

* правильность и полнота ответов во время зачета;
* выполнение работ с информационной системой обеспечения информационной безопасности;
* тестирование.

**4. 2.** **Материалы текущего контроля успеваемости обучающихся.**

**Типовые оценочные материалы по теме 1**

Типовые тесты

1. Определите КСДВ (1, 2, 3)?

1. Кейс с электролитическими конденсаторами включили в сетевую розетку офисной ЛВС.
2. Кейс с электролитическими конденсаторами включили в офисную розетку сети электропитания.
3. Электрошокер воткнули в сетевой разъем маршрутизатора.
4. Резонирующий емкостной накопитель подключили ко вторичной обмотке трансформаторной подстанции.
5. Мощный разряд молнии в непосредственной близости.
6. Внедрение программной закладки в источник бесперебойного питания.
7. Электромагнитный импульс от генератора СВЧ-излучения, установленного в багажнике легкового автомобиля.
8. Прокладка мощного кабеля электропитания сварочного аппарата в одном коробе с кабелем ЛВС.
9. Сварочные работы вблизи включенного системного блока.
10. Подключение сварочного аппарата в офисную розетку сети электропитания.

Ответ: \_\_\_\_\_\_\_\_\_\_\_\_ номер по порядку.

1. Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему: **1**) морально-этический; **2**) организационно-технический; **3**) нормативно-правовой; **4**) программно-аппаратный; **5**) духовно-нравственный?

Ответ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(последовательность номеров через запятую)

2. Что НЕ является элементом системы обеспечения информационной безопасности РФ: 1) Палаты Федерального собрания; **2**) Президент; **3**) Органы местного самоуправления; **4**) Общественная Палата; **5**) Органы исполнительной власти; **6**) Совет безопасности?

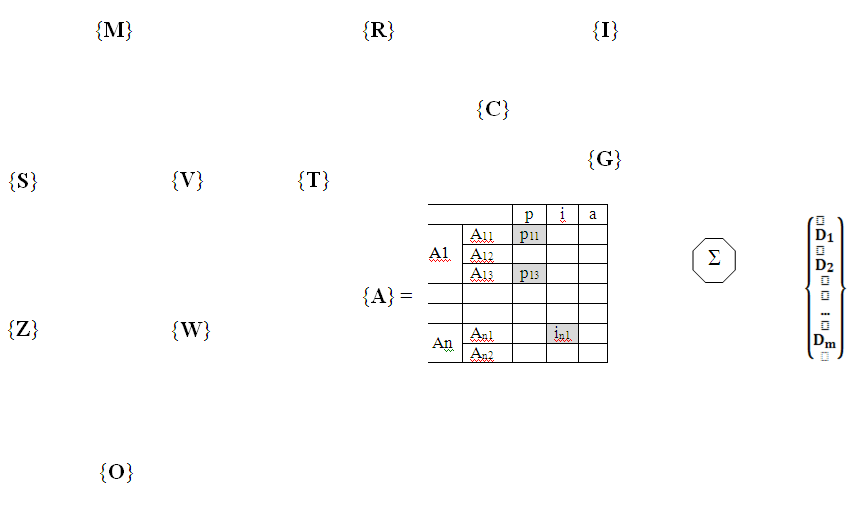
Ответ: \_\_\_(номер по порядку)

3. Кто НЕ наделен полномочиями по отнесению сведений к государственной тайне: **1**) Министр сельского хозяйства; **2**) Председатель Банка РФ; **3**) Руководитель Росгидромета; **4**) Руководитель Федеральной таможенной службы?

Ответ: \_\_(номер по порядку)

4. Режим коммерческой тайны не может быть установлен в отношении сведений: 1) о задолженности по выплате зарплаты; **2**) о размерах доходов некоммерческих организаций; **3**) о составе имущества предприятия любой формы собственности; **4**) о системе оплаты труда (неверное зачеркнуть)

5. Установите все парные связи между элементами «ландшафта» информационной безопасности, где: {**I**} − множество требований к оператору; {**М**} − множество защитных мер; {**S**} − множество источников угроз; {**V**} − множество уязвимостей; {**Z**} − множество зон безопасности; {**W**} − множество состава оборудования; {**D**} − множество нарушений; {**R**} − множество методов и средств оценки рисков; {**С**} − множество методов и средств проверки выполнения требований; {**T**} − множество угроз; {**А**} − множество активов; {**с**} − ущерб конфиденциальности актива; {**i**} − ущерб целостности актива; {**a**} − ущерб доступности актива.



**Типовые оценочные материалы по теме 2**

Типовые вопросы

2. Выберите тип (или типы) технического(ких) канала(ов) утечки информации, соответствующий инциденту информационной безопасности:

1. Перехват побочных электромагнитных излучений от работы ПЭВМ и ВТСС
2. Съём наводок информационных сигналов с посторонних проводников
3. Съём информационных сигналов с цепей заземления и электропитания
4. Беспроводной прием информации, передаваемой аппаратными закладками
5. Приём переизлученных высокочастотных колебаний, модулированных информационным сигналом
6. Перехват речевых сигналов направленными микрофонами
7. Перехват акустических (речевых) сигналов микрофонами, скомплексированными с портативными устройствами звукозаписи
8. Перехват акустических (речевых) сигналов скрытно установленными микрофонами, соединёнными с устройствами звукозаписи сигнальным кабелем
9. Перехват акустических (речевых) сигналов микрофонами, комплексированными с микрорадиопере-датчиками (радиозакладками)
10. Перехват акустических (речевых) сигналов микрофонами, комплексированными с устройствами передачи информации по электросети 220 В
11. Перехват акустических (речевых) сигналов контактными микрофонами (стетоскопами), соединёнными с электронными усилителями
12. Перехват акустических (речевых) сигналов контактными микрофонами, комплексированными с радиостетоскопами
13. Приём переизлучённого высокочастотного сигнала "навязывания", модулированного информационным сигналом
14. Приём отражённого лазерного излучения, модулированного информационным сигналом

**Ответ**: электромагнитный, воздушный (акустический), вибрационный, радиоканал, акустоэлектрический, оптико-электронный, параметрический, оптический, электрический (неверное зачеркнуть)

**Типовые оценочные материалы по теме 3**

1. По виду защищаемой информации различаются угрозы НСД к: **1**) речевой информации; **2**) видовой информации; **3**) сигнальной информации; **4**) логической информации; **5**) тестовой информации (лишнее зачеркнуть)

2. По видам возможных источников различаются угрозы НСД к информации, создаваемые: **1**) нарушителем; **2**) аппаратной закладкой; **3**) вредоносными программами; **4**) сетевыми атаками (лишнее зачеркнуть)

3. По виду нарушаемого свойства информации различаются угрозы: **1**) конфиденциальности; **2**) целостности; **3**) доступности; **4**) идентифицируемости (лишнее зачеркнуть)

4. По способам реализации различаются угрозы с применением: **1**) программных средств операционной системы; **2**) специально разработанного программного обеспечения; **3**) вредоносных программ; **4**) пользовательских программ (лишнее зачеркнуть)

5. По используемой уязвимости различаются угрозы: **1**) системного программного обеспечения; **2**) прикладного программного обеспечения; **3**) вызванные аппаратной закладкой; **4**) протоколов сетевого взаимодействия; **5**) недостатков организации технической защиты информации от НСД; **6**) вызванные наличием технических каналов утечки информации; **7**) недостатков системы защиты информации: **8**) специальных воздействий (лишнее зачеркнуть)

6. По объекту воздействия различаются угрозы: **1**) информации, обрабатываемой на АРМ; **2**) информации, обрабатываемой в выделенных технических средствах обработки информации; **3**) информации, передаваемой по сетям; **4**) прикладным программам обработки информации; **5**) системному программному обеспечению; **6**) пользовательским программам (лишнее зачеркнуть)

**Типовые оценочные материалы по теме 4**

Типовые тесты

1. Сколько текстовой информации может быть скрыто методами стеганографии в:

1. цветной фотографии, сделанной 3-х мегапиксельной камерой мобильного телефона?
2. цветной фотографии формата *bmp*, сделанной мегапиксельной камерой мобильного телефона?
3. 30 секундах моно-звучания на ПК музыкального фрагмента в формате *wav*?
4. 30 секундах стерео-звучания на ПК музыкального фрагмента в формате *wav*?
5. 1 странице текстового файла на русском языке?
6. 1 странице текстового файла на английском языке?
7. электронном 300-страничном томике Пушкина?
8. электронном 300 страничном томике Шекспира на языке оригинала?
9. 100-минутном фильме, записанном на DVD-диск в стандарте SECAM?
10. 100-минутном фильме, записанном на DVD-диск в стандарте NTSC?

Ответ: \_\_\_страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5).

1. Используя шифр «Цезаря», расшифруйте первое слово и зашифруйте второе слово **тем же** ключом:
2. дгодзф, посуда
3. ёехцшп, чайник
4. иътсжф, цветок
5. кыьфуи, дерево
6. лкылщь, голова
7. сжзпфж, трасса
8. бьиптс, баллон
9. жётхкц, камера
10. тцумщц, прицеп
11. ьшъцшс, комета
12. эюлюяк, дракон
13. чмэмюи, нянька
14. меиеье, корень
15. цчпулч, разряд
16. эиуычщ, палата

3. Напишите в клетках (можно использовать не все) пароль, устойчивый к атакам: по словарю, «грубой силы», поиск «слабого пользователя», поиск «слабого пароля».

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Типовые оценочные материалы по теме 5**

Типовые вопросы (устный опрос):

1. Определение понятий «идентификация», «аутентификация», «авторизация», «админитрирование».
2. Что понимают под решением задач ААА?
3. Какие задачи решает подсистема управления идентификацией и доступом IAM?
4. Перечислите атаки на протоколы аутентификации?
5. Опишите метод аутентификации на основе:

- многоразовых паролей;

- одноразовых паролей.

Каковы достоинства и недостатки каждого метода?

6) Объясните принцип управления доступом по схеме однократного входа с авторизацией SSO?

**Типовые оценочные материалы по теме 6**

Типовые вопросы круглого стола

1. Комплексный подход к обеспечению информационной безопасности корпоративной информационной системы (КИС).
2. По каким схемам можно включить контур информационной безопасности в сеть предприятия?
3. Зачем нужна фильтрация по прокси-серверам?
4. Зачем нужна фильтрация по почтовым серверам?
5. Какие виды поиска рекомендуются для структурированных документов?
6. Что такое фильтр ограничений по перехвату?
7. Что такое «белый список»?
8. Какой должен быть интервал обновления индексов?
9. Для чего применяется каталог образцов?
10. Можно ли снять цифровой отпечаток из pdf-файла?
11. Что такое шаблон регулярного выражения?

Типовые тестовые вопросы

1. Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей влечет наложение административного штрафа на должностных лиц до: **1**) 1.000 рублей; **2**) 3.000 рублей; **3**) 5.000 рублей; **4**) 10.000 рублей (неверное зачеркнуть)

2. Неправомерный доступ к компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается: **1**) штрафом в размере от 200 до МРОТ; **2**) исправительными работами на срок от 6 месяцев до 1 года; **3**) принудительными работами на срок до 18 месяцев; **4**) лишением свободы на срок до 2 лет (лишнее зачеркнуть).

3. Создание, использование и распространение вредоносных программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются **1**) штрафом; **2**) исправительными работами; **3**) принудительными работами; **4**) арестом; **5**) лишением свободы (лишнее зачеркнуть).

4. Дополните кодификатор Интерпола

|  |  |  |
| --- | --- | --- |
|  | Q \_\_ \_\_ | 27.09.2014. Вена. INTERFAX.RU − Австрийские участники хакерской группы Anonymous сообщили о краже личных данных 25 тыс. австрийских полицейских, пишет во вторник местная газета "Винер цайтунг". |
|  | Q \_\_ \_\_ | 21.11.2013. Этот случай разрушительнойкибератаки на водонапорную станцию Спрингфельде (штат Иллинойс) произошёл около двух недель тому назад. Наглое вмешательство хакеров через интернет привело к тому, что двигатель насоса водонапорной станции стал вдруг с необычайной частотой включаться и выключаться. Дело закончилось тем, что мотор сгорел. |
|  | Q \_\_ \_\_ | 25.11.2013. Хакеры взломали несколько сотен сайтов в пакистанском домене .pk, разместив на них изображения двух пингвинов на мосту. Всего сообщение хакеров появилось на 285 сайтах, включая google.com.pk, microsoft.pk, apple.pk, paypal.pk, и ebay.pk. Помимо изображения, оно включало в себя фразу на английском "PakistanDowned" ("Пакистан взломан") и текст на турецком. На взломанных сайтах говорилось, что атаку осуществил хакер Eboz. |
|  | Q \_\_ \_\_ | 01.11.2013. Выбрав определенную компанию (одну из 48), хакеры точечно рассылали ее сотрудникам электронные письма с программой PoisonIvy, которая при открытии вложенного в письмо инсталлировалась в систему и отсылала по зашифрованному каналу информацию о внутренней сети предприятия. |
|  | Q \_\_ \_\_ | 12.04.2013. 28-летний хакер был задержан в Санкт-Петербурге. По данным следствия, злоумышленник, используя вредоносную программу, "отправил" пользователей сайта ФК Зенит" с его подлинного адреса http://fc-zenit.ru на подставной в Люксембурге. На нем хакер разместил 7 страниц с оскорбительными высказываниями в адрес футбольного клуба, а также информацию о предложении услуг по взлому анкет "facebook", "icq" и др. |
|  | Q \_\_ \_\_ | 13.01.2013.Новый интернет-червь Downadup, известный также как Conficker, передал под контроль неизвестных хакеров 3,5 миллиона зараженных компьютеров, говорится на сайте компании F-Secure, занимающейся IT-безопасностью и разработкой антивирусов. |
|  | Q \_\_ \_\_ | 03.10.2013. Чертановский районный суд Москвы наказал жителя Химок Алексея Андруся годом лишения за установку нелицензионных программ 1С и Microsoft. Кроме того, что Андрусь проведет год в тюрьме, он еще и выплатит 50 тысяч компании "1С" и более 44 тысяч - Microsoft в целях возмещения ущерба. |
|  | Q \_\_ \_\_ | 16.06.2014. Злоумышленник был осужден судом Дюссельдорфа на 10 лет лишения свободы. С помощью российских серверов он проводил DDoS-атаки на букмекерские сайты, вымогая с их владельцев деньги. После блокировки 3 владельцев сайтов предпочли заплатить требуемую сумму, ещё 3 платить отказались, что привело к убыткам, исчисляющимся в шестизначных цифрах. |
|  | Q \_\_ \_\_ | 01.03.2014. Приговором Петропавловск-Камчатского городского суда Игорю Ш. назначено наказание в виде 1 года лишения свободы условно. Используя Интернет, через домашний компьютер он подключился к базе данных и удалил с сервера всю бухгалтерскую и финансовую информацию, справочные и персональные сведения о судах, коммерческих партнерах и сотрудниках. |
|  | Q \_\_ \_\_ | 23.02.2014. Житель города Якутска приобрел у неизвестного лица логины и пароли легальных пользователей для выхода в сеть Интернет через провайдера «Сахателеком». Далее, используя четырнадцать незаконно полученных сетевых идентификаторов (логин и пароль), осуществлял неправомерный выход в сеть  Интернет, в результате чего легальный пользователь не имел возможности подключиться к Интернету и необоснованно производил за него оплату. |
|  | Q \_\_ \_\_ | 11.12.2013. В Иркутске инженеры одного из крупных банков, обслуживающие банкоматы, вмонтировали в банкомат, за исправность которого несли ответственность, собственный купюроприемник и многократно проводили через терминал одну и ту же купюру в пять тысяч рублей. |

**4.3. Оценочные средства для промежуточной аттестации.**

Таблица 6

|  |  |  |  |
| --- | --- | --- | --- |
| Код  компетенции | Наименование  компетенции | Код  этапа освоения компетенции | Наименование этапа освоения компетенции |
| ОПК - 9 | владение культурой научного исследования, в том числе с использованием современных информационно-коммуникационных технологий | ОПК - 2.2 | умение решать задачи научного исследования на базе системного анализа, использования современных инфокоммуникационных технологий, методов и технологий информационной безопасности. |
| ПК-1 | владеть способностью формализации и постановки задач системного анализа, оптимизации, управления, принятия решений и обработки информации | ПК-1.3 | Способность решать задачи системного анализа экономических систем, математической экономики, эконометрики |

Таблица

| Этап освоения компетенции | Показатель  оценивания | Критерий оценивания |
| --- | --- | --- |
| ОПК-2.2 | 1. Самостоятельно решает частные задачи исследования, учитывает вопросы информационной безопасности, использует методы системного анализа, приводит результаты оценки современного состояния исследуемой предметной области. 2. Представляет реферат по теме, предложенной научным руководителем или выбранной самостоятельно. 3. Демонстрирует знание основных положений теоретических вопросов, вынесенных на экзамен по специальности | 1. Глубина исследования решаемой проблемы. 2. Полнота и правильность ответов на вопросы зачета. 3. Полнота и качество выполнения заданий и тестов. |
| ПК-1.3 | 1. Самостоятельно решает частные задачи научного исследования 2. Корректно использует методы системного анализа, современные ИКТ при исследовании экономических систем, социально-экономических процессов | 1. Активность в дискуссии, правильность выполнения тестов. 2. Глубина исследования решаемой проблемы. 3. Полнота и правильность ответов на вопросы |

Для оценки сформированности компетенций, знаний и умений, соответствующих данной компетенции, используются вопросы для зачета.

**Типовые вопросы, выносимые на зачет:**

1. Краткая история защиты информации в России.
2. Обобщенная модель информационной безопасности.
3. Институт стандартизации сферы информационной безопасности.
4. Национальные стандарты в области информационной безопасности и защиты информации.
5. Международные стандарты в области информационной безопасности и защиты информации.
6. Проблемы гармонизации стандартовинформационной безопасности.
7. Электромагнитный спектр как источник воздействия на информацию.
8. Каналы силового деструктивного воздействия (СДВ) на информацию.
9. Классификация средств СДВ.
10. Рекомендации по защите компьютерных систем от СДВ.
11. Классификация технических каналов утечки информации.
12. Модель и способы утечки по радиоканалу.
13. Модель и способы утечки по электрическому каналу.
14. Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому)каналу.
15. Модель и способы утечки по параметрическому (смешанному)каналу.
16. Модель и способы утечки по оптическому (оптико-электронному)каналу.
17. Модель и способы утечки по каналу ПЭМИН.
18. Классификация угроз несанкционированного доступа (НСД) к информации.
19. Категории нарушителей безопасности информации и их возможности.
20. Общая характеристика уязвимостей.
21. Способы реализации угрозы НСД к информации.
22. Понятие и обобщенная модель нетрадиционного информационного канала.
23. Методы сокрытия информации в текстовых файлах.
24. Методы сокрытия информации в графических файлах.
25. Методы сокрытия информации в звуковых файлах.
26. Методы сокрытия информации в сетевых пакетах и исполняемых файлах.
27. Модель криптосистемы.
28. Историография и классификация шифров.
29. Примеры криптографических алгоритмов.
30. Криптосистема с симметричными и несимметричными ключами.
31. Электронная цифровая подпись.
32. Мандатная и дискреционная модели доступа.
33. Процедура идентификации, аутентификации и авторизации.
34. Система паролирования.
35. Системы контроля и управления доступом.
36. Система охраны периметра.
37. Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети.
38. Понятие и функционал DLP-систем.
39. Объем и структура данных защищаемых DLP-системами.
40. Каналы коммуникаций, контролируемые DLP-системами.
41. Критерии оценки программных продуктов, реализующих функциональность DLP.
42. Понятие компьютерной преступности.
43. Масштабы и общественная опасность компьютерной преступности.
44. Виды и субъекты компьютерных преступлений.
45. Специфика расследования компьютерных преступлений.
46. Предупреждение компьютерных преступлений.
47. Кодификатор Интерпола.
48. Архитектура КИС.
49. Структура системы защиты информации в КИС.
50. Подсистемы информационной безопасности КИС.

**Шкала оценивания.**

Оценка результатов производится на основе балльно-рейтинговой системы (БРС). Использование БРС осуществляется в соответствии с приказом от 28 августа 2014 г. №168 «О применении балльно-рейтинговой системы оценки знаний студентов». БРС по дисциплине отражена в схеме расчетов рейтинговых баллов (далее – схема расчетов). Схема расчетов сформирована в соответствии с учебным планом направления, согласована с руководителем научно-образовательного направления, утверждена деканом факультета. Схема расчетов доводится до сведения студентов на первом занятии по данной дисциплине и является составной частью рабочей программы дисциплины и содержит информацию по изучению дисциплины, указанную в Положении о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС.

На основании п. 14 Положения о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС в институте принята следующая шкала перевода оценки из многобалльной системы в пятибалльную:

Таблица 7

|  |  |  |
| --- | --- | --- |
| **Количество баллов** | **Экзаменационная оценка** | |
| прописью | буквой |
| 86 - 100 | отлично | А |
| 78 - 85 | хорошо | В |
| 66 - 77 | хорошо | С |
| 61 - 65 | удовлетворительно | D |
| 51 – 60 | удовлетворительно | E |
| 0 - 50 | неудовлетворительно | EX |

Шкала перевода оценки из многобалльной в систему «зачтено»/ «не зачтено»:

Таблица 8

|  |  |
| --- | --- |
| от 0 до 50 баллов | «не зачтено» |
| от 51 до 100 баллов | «зачтено» |

Примечание: если дисциплина изучается в течение нескольких семестров, схема расчета приводится для каждого из них.

Баллы выставляются за посещаемость (максимум 12 баллов), результативность практических занятий (максимум 20), результат устного опроса (максимум 3 балла), результаты выполнения тестовых заданий (максимум 10 баллов), выполнение курсовой работы (максимум 25 баллов), ответ на экзамене (максимум 30 баллов). Дисциплина считается освоенной, если экзаменуемый набрал не менее 51 балла в результате выполнения всех типов заданий, включая ответ на экзамене. Минимальное количество баллов для допуска к экзамену – 45.

**4.4. Методические материалы**

Методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, включают в себя:

* комплект тестовых заданий по темам дисциплины,
* рекомендации и требования к выполнению заданий,
* требования к защите заданий и критерии их оценивания,

Методические материалы в виде презентаций размещены в Ресурсах сети СЗИУ в STUDBOX в папке кафедры ЭиФ.

**5.** Методические указания для обучающихся по освоению дисциплины

Рабочей программой дисциплины предусмотрены следующие виды аудиторных занятий: лекции, практические занятия. Преподавание дисциплины ведется с применением следующих видов образовательных технологий, обусловливающих самоорганизацию процесса освоения дисциплины.

Организация работы с информацией.

Информационные технологии:обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам (теоретически к неограниченному объему и скорости доступа), увеличения контактного взаимодействия с преподавателем, построения индивидуальных траекторий подготовки и объективного контроля и мониторинга знаний студентов.

Использование электронных образовательных ресурсов (презентационный материал, размещенный в Ресурсах сети СЗИУ) при подготовке к лекциям, практическим занятиям. Организация работы студентов с электронной библиотекой указана на сайте института (странице сайта – «Научная библиотека»).

Проблемное обучение (проблемные лекции, лекции с элементами дискуссии) с целью развитие критического мышления, стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретной проблемы. Для этого студенту должно быть предоставлено право самостоятельно работать в компьютерных классах в сети Интернет.

Развитие профессиональной компетентности:

Case-study на практических занятиях с целью формирования способности к анализу реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений.

Контекстное обучение (лекции с элементами дискуссии, практические занятия)с целью развитиямотивации бакалавров к усвоению знаний путем выявления связей между конкретным знанием и его применением.

Организация группового взаимодействия в образовательном процессе.

Деловая игра:на практическихзанятиях ро**л**евая имитация студентами реальной профессиональной деятельности с выполнением функций специалистов на различных рабочих местах, организация дискуссии, обучения на основе социального взаимодействия.

Работа в командес целью развития способности к взаимодействию студентов в группе при выполнении домашних заданий по разделам дисциплины.

Осуществление учения с учетом возрастающей роли субъектности и самостоятельности:

Обучение на основе опыта: активизация познавательной деятельности студентов за счет ассоциации и собственного опыта с предметом изучения, самоуправляемого обучения, самообразовательной деятельности

С целью контроля сформированности компетенций разработан фонд контрольных заданий. Его использование позволяет реализовать балльно-рейтинговую оценку, определенную приказом от 28 августа 2014 г. №168 «О применении балльно-рейтинговой системы оценки знаний студентов».

**Контрольные вопросы для подготовки к занятиям**

Таблица 9

|  |  |  |
| --- | --- | --- |
| №  п/п | Наименование темы или раздела дисциплины (модуля) | Контрольные вопросы для самопроверки |
|
| 1 | Тема 1. Информационная безопасность и защита информации | 1. Электромагнитный спектр как источник воздействия на информацию. 2. Каналы силового деструктивного воздействия (СДВ) на информацию. 3. Классификация средств СДВ. 4. Рекомендации по защите компьютерных систем от СДВ. |
| 2 | Тема 2. Технические каналы утечки информации | 1. Классификация технических каналов утечки информации. 2. Модель и способы утечки по радиоканалу. 3. Модель и способы утечки по электрическому каналу. 4. Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому)каналу. |
| 3 | Тема 3. Угрозы несанкционированного доступа к информации | 1. Классификация угроз несанкционированного доступа (НСД) к информации. 2. Категории нарушителей безопасности информации и их возможности. 3. Общая характеристика уязвимостей. 4. Способы реализации угрозы НСД к информации. 5. Методы сокрытия информации в текстовых файлах. 6. Методы сокрытия информации в графических файлах. 7. Методы сокрытия информации в звуковых файлах 8. Методы сокрытия информации в сетевых пакетах и исполняемых файлах. |
| 4 | Тема 4. Криптографическая защита информации | 1. Модель криптосистемы. 2. Историография и классификация шифров. 3. Примеры криптографических алгоритмов. 4. Криптосистема с симметричными и несимметричными ключами. 5. Электронная цифровая подпись. 6. Методы кодирования. 7. Приведите примеры кодов, используемых в криптографии |
| 5. | Тема 5. Методы и средства разграничения и контроля доступа к информации | 1. Мандатная и дискреционная модели доступа. 2. Процедура идентификации, аутентификации и авторизации. 3. Система паролирования. 4. Системы контроля и управления доступом. 5. Система охраны периметра |
| 6 | Тема 6. Системы предотвращения утечки информации из корпоративной информационной системы | 1. Сформулируйте основополагающие принципы постороения современных КИС. 2. Охарактеризуйте четыре уровня управления КИС. 3. Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети. 4. Понятие и функционал DLP-систем. 5. Объем и структура данных защищаемых DLP-системами. 6. Каналы коммуникаций, контролируемые DLP-системами. 7. Критерии оценки программных продуктов, реализующих функциональность DLP. |

**6.** Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

**6.1. Основная литература.**

1. Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Электрон. дан. - Орел : МАБИВ, 2014. - 256 c. <http://www.iprbookshop.ru/33430.html>
2. Басалова, Г. В. Основы криптографии [Электронный ресурс] : учеб. пособие / Г. В. Басалова. - 2-е изд., испр. - Электрон. дан. - М. : ИНТУИТ, 2016. - 282 c. <http://www.iprbookshop.ru/52158.html?replacement=1>
3. Петров, С. В. Информационная безопасность [Электронный ресурс] : учеб. пособие / С.В. Петров, П.А. Кисляков. - Электрон. дан. - Саратов : Ай Пи Ар Букс, 2015. - 326 c. <http://www.iprbookshop.ru/33857.html>
4. Скляров, Дмитрий В. Искусство защиты и взлома информации [Электронный ресурс] / Дмитрий Скляров. - Электрон. дан. - М. : БХВ-Петербург, 2014. - 276 c. <http://ibooks.ru/reading.php?productid=335110>

**6.2 Дополнительная литература**

Галатенко, Владимир Антонович. Основы информационной безопасности [Электронный ресурс] : учеб. пособие / В. А. Галатенко. - 2-е изд., испр. - Электрон. дан. - М. : ИНТУИТ, 2016. - 266 c. <http://www.iprbookshop.ru/52209.html>

Курило, А. П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Издательство"Горячая линия-Телеком", 2012 г. - 244 с.

Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М. : Горячая линия-Телеком,2012.- 130 с.

Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3 / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - М. : Горячая линия-Телеком,2012.- 170 с.

Скрипник, Д. А. Общие вопросы технической защиты информации [Электронный ресурс] : [учеб. курс] / Д.А. Скрипник. - 2-е изд., испр. - Электрон. дан. - М. : ИНТУИТ, 2016. - 429 c. <http://www.iprbookshop.ru/52161.html?replacement=1>

Фаронов, А. Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс] : учеб. пособие / А.Е. Фаронов. - 2-е изд., испр. - Электрон. дан. - М. : ИНТУИТ, 2016. - 154 c. <http://www.iprbookshop.ru/52160.html?replacement=1>

**6.3. Учебно-методическое обеспечение самостоятельной работы**.

Самостоятельная работа студентов обеспечивается наличием следующих учебно-методических материалов:

* фонд контрольных вопросов для самопроверки;
* методические рекомендации по написанию и выполнению курсовой работы (презентации Power Point);
* презентационный материал лекций.
  1. Нормативные правовые документы

1. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
2. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации").
3. Стратегии национальной безопасности Российской Федерации до 2020 года (Указ Президента РФ от 31.12.2015 N 683 "О Стратегии национальной безопасности Российской Федерации")
4. Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212).
5. Федеральный закон "О безопасности" от 28.12.2010 N 390-ФЗ.
6. Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне".
7. Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 N 99-ФЗ (последняя редакция).
8. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. 2016).
9. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ.
10. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ (последняя редакция).
11. Федеральный закон "О техническом регулировании" от 27.12.2002 N 184-ФЗ (последняя редакция)
12. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
13. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция).
14. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (последняя редакция).

**6.5. Интернет-ресурсы.**

СЗИУ располагает доступом через сайт научной библиотеки <http://nwapa.spb.ru> к следующим подписным электронным ресурсам:

**Русскоязычные ресурсы**

* Электронные учебники электронно - библиотечной системы (ЭБС) «Айбукс»
* Электронные учебники электронно – библиотечной системы (ЭБС) «Лань»
* Научно-практические статьи по финансам и менеджменту Издательского дома «Библиотека Гребенникова»
* Статьи из периодических изданий по общественным и гуманитарным наукам «Ист - Вью»
* Информационно-правовые базы - Консультант плюс, Гарант.

**Англоязычные ресурсы**

* EBSCO Publishing - доступ к мультидисциплинарным полнотекстовым базам данных различных мировых издательств по бизнесу, экономике, финансам, бухгалтерскому учету, гуманитарным и естественным областям знаний, рефератам и полным текстам публикаций из научных и научно-популярных журналов.
* Emerald- крупнейшее мировое издательство, специализирующееся на электронных журналах и базах данных по экономике и менеджменту. Имеет статус основного источника профессиональной информации для преподавателей, исследователей и специалистов в области менеджмента.

Возможно использование, кроме вышеперечисленных ресурсов, и других электронных ресурсов сети Интернет:

Интернет-ресурсы, электронные библиотечные системы:

* Российская государственная библиотека (Москва) – <http://www.rsl.ru>
* Российская национальная библиотека (Санкт-Петербург) – <http://www.nlr.ru/>
* Британская национальная библиотека (The British Library) – [http://www.bl.uk/](http://portico.bl.uk/)
* Национальная библиотека Франции (Biblioteque nationale de France) – <http://www.bnf.fr/>
* Немецкая национальная библиотека (Die Deutsche Bibliothek) – <http://www.ddb.de/>
* Европейская библиотека (The European Library) – <http://www.theeuropeanlibrary.org>
* Библиотека Конгресса США (Library of Congress, USA) – <http://www.loc.gov/>
* Национальная библиотека и архивы Канады – <http://nlc-bnc.ca>
* Крупнейшие университеты мира:
* Болонский университет, Италия, Болонья – <http://www.unibo.it/>
* Бомбейский университет, Индия, Бомбей, - <http://www.mu.ac.in/>
* Гарвардский университет, США, Кембридж, близ Бостона – <http://www.harvard.edu>
* Калифорнийский университет, США, Кампусы (городки ун-та) в Беркли, Дейвисе, Лос-Анжелесе, Ривер-Сайде, Сан-Франциско и др. – <http://www.berkeley.edu/>
* Калькуттский университет, Индия, Калькутта, - <http://www.caluniv.ac.in/>
* Кембриджский университет, Великобритания, Кембридж, - [www.cam.ac.uk](http://www.cam.ac.uk)
* Колумбийский университет, США, Нью-Йорк, - <http://www.columbia.edu/>
* Лондонский университет, Великобритания, Лондон – <http://lon.ac.uk>
* Массачусетский технологический институт, США, Кембридж, шт. Массачусетс – <http://web.mit.edu>
* Московский государственный университет имени М. В. Ломоносова, Россия, Москва – <http://www.msu.ru/>
* Мюнхенский университет, Германия, Мюнхен – <http://www.en.uni-muenchen.de>
* Оксфордский университет, Великобритания – <http://www.ox.ac.uk/>
* Парижский университет, Франция, Париж, - <http://www.sorbonne.fr/>
* Пекинский университет, Китай, Пекин – <http://www.pku.edu.cn/>
* Римский университет, Италия, Рим – <http://www.uniroma1.it/>
* Сиднейский университет, Австралия, Сидней – <http://www.usyd.edu.au/>
* Санкт-Петербургский государственный университет, Россия, Санкт-Петербург – [http://www.spbu.ru/](http://www.msu.ru/),
* Токийский университет, Япония, Токио – (<http://www.u-tokyo.ac.jp/>

6.6. Иные источники.

**7.** Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Курс включает использование программного обеспечения операционной системы Windows 10, пакет программ MS Office 2013, 2016, виртуальной машины MSWare, программной системы «Контур информационной безопасности» компании SearchInform, справочная электронной системы «Гарант» для подготовки текстового и табличного материала.

Методы обучения с использованием информационных технологий (компьютерное тестирование, демонстрация мультимедийных материалов).

Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии, справочники, библиотеки, электронные учебные и учебно-методические материалы)

Для организации дистанционного обучения используется система Moodle.