Приложение 7 ОП ВО

**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

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

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

Б1.В.ДВ.03.01 Информационная безопасность

*(индекс, наименование дисциплины, в соответствии с учебным планом)*

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

Санкт-Петербург, 2017 г.

**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, соотнесенных с планируемыми результатами освоения образовательной программы
 |
| 1. Объем и место дисциплины в структуре образовательной программы
 |
| 1. Содержание и структура дисциплины
 |
| 1. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации4.2. Материалы текущего контроля успеваемости обучающихся4.3. Оценочные средства для промежуточной аттестации4.4. Методические материалы |
| 1. Методические указания для обучающихся по освоению дисциплины
 |
| 1. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине
 |
| 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.03.01 «Информационная безопасность» обеспечивает овладение следующими компетенциями:**

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| Код компетенции | Наименованиекомпетенции | 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 |

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: * 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: * 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:* 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 академ. Часов.

Таблица 3

Очная форма обучения

|  |  |
| --- | --- |
|  Вид работы | Трудоемкость (акад/астр.часы) |
| **Общая трудоемкость** | 72/54 |
| ***Аудиторная работа*** | 36/24 |
| Лекции | 16/12 |
| Семинары и практические занятия | 20/15 |
| ***Самостоятельная работа*** | 30/22,5 |
| Виды текущего контроля | Тестирование, контрольная работа, реферат, зачет |
| Вид промежуточного контроля | Зачет (6) |

Общий объем дисциплины составляет 72 академ. Часа (2 ЗЕТ).

Таблица 3

Заочная форма обучения

|  |  |
| --- | --- |
|  Вид работы | Трудоемкость (акад/астр.часы) |
| **Общая трудоемкость** | 72/54 |
| ***Аудиторная работа*** | 12/9 |
| Лекции | 4/3 |
| Семинары и практические занятия | 8/6 |
| ***Самостоятельная работа*** | 54/40,5 |
| Виды текущего контроля | Тестирование, контрольная работа, реферат, зачет |
| Вид промежуточного контроля | Зачет (6) |

**Место дисциплины в структуре ОП ВО**

Дисциплина Б1.В.ДВ.03.01 «Информационная безопасность» 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.03.01 «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 «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**  | **Объем дисциплины (модуля), час.** | **Форматекущего контроля успеваемости, промежуточной аттестации** |
| **Всего** | **Контактная работа обучающихся с преподавателемпо видам учебных занятий** | **СР** |
| **Л** | **ЛР** | **ПЗ** | **КСР** |  |
| **Очная форма обучения** |
| Тема 1 | Категория информационной безопасности. Каналы силового деструктивного воздействия на информацию | 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 сети | 12 | 2 | - | 4 |  | 6 | Круглый стол/Т |
| Промежуточная аттестация | 6 |  |  |  |  |  | Зачет |
| Всего (акад./астр. Часы): | 72/54 | 16/12 |  | 20/15 |  | 30/22,5 |  |

***Заочная форма обучения***

Таблица 5

|  |  |  |  |
| --- | --- | --- | --- |
|  **№ п/п** | **Наименование тем**  | **Объем дисциплины (модуля), час.** | **Форматекущего контроля успеваемости, промежуточной аттестации** |
| **Всего** | **Контактная работа обучающихся с преподавателемпо видам учебных занятий** | **СР** |
| **Л** | **ЛР** | **ПЗ** | **КСР** |
|  |
| Тема 1 | Категория информационной безопасности. Каналы силового деструктивного воздействия на информацию | 13 | 1 | - | 2 |  | 10 | Задание (З) |
| Тема 2 | Технические каналы утечки информации | 12 | 1 | - | 1 |  | 10 | Т |
| Тема 3 | Угрозы несанкционированного доступа к информации | 8 |  | - |  |  | 8 | Круглый стол/Т |
| Тема 4. | Криптографическая защита информации | 13 | 1 | - | 2 |  | 10 | Д,Т |
| Тема 5. | Методы и средства разграничения и контроля доступа к информации | 11 | 1 | - | 2 |  | 8 | Устный опрос |
| Тема 6. | Системы предотвращения утечки информации из корпоративной сети | 9 |  | - | 1 |  | 8 | Круглый стол/Т |
| Промежуточная аттестация | 6 |  |  |  |  | 6 | Зачет |
| Всего (акад./астр. Часы):: | 72/54 | 4/3 |  | 8/6 |  | 30/22,5 |  |

*тестирование (Т), диспут (Д)*

**Содержание дисциплины**

**Тема 1. Категория информационной безопасности. Каналы силового деструктивного воздействия на информацию**

Понятие национальной безопасности. Виды безопасности. Средства оценки информационной безопасности. Программные и аппаратные средства обеспечения информационной безопасности. Понятие информационной безопасности. Обеспечение информационной безопасности. Соотношение понятий угроза, риск, воздействие.

**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 сети**

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

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

* 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 6

|  |  |
| --- | --- |
| Тема (раздел) | Формы (методы) текущего контроля успеваемости |
| Тема 1. Категория информационной безопасности. Каналы силового деструктивного воздействия на информацию  | 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 |

* + 1. **Зачет проводится с применением следующих методов (средств):**

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

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

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

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

**Типовые оценочные материалы по теме 1**

Типовые тесты

1. Включение кейса с электролитическими конденсаторами в сетевую розетку офисной ЛВС является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

2. Включение кейса с электролитическими конденсаторами в офисную розетку сети электропитания является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

3. Включение электрошокера в сетевой разъем маршрутизатора является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

4. Мощный разряд молнии в непосредственной близости является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

5. Внедрение программной закладки в источник бесперебойного питания. является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

6. Подключение резонирующего емкостного накопителя ко вторичной обмотке трансформаторной подстанции является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

7. Электромагнитный импульс от генератора СВЧ-излучения, установленного в багажнике легкового автомобиля, является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

8. Прокладка мощного кабеля электропитания сварочного аппарата в одном коробе с кабелем ЛВС является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

9. Подключение сварочного аппарата в офисную розетку сети электропитания является следующим каналом силового деструктивного воздействия:

1) КСДВ – 1;

2) КСДВ – 2;

3) КСДВ – 3.

10. Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему (последовательность номеров через запятую):

1) морально-этический;

2) организационно-технический;

3) нормативно-правовой;

4) программно-аппаратный;

5) духовно-нравственный.

11. Что не является элементом системы обеспечения информационной безопасности РФ (номер по порядку):

1) Палаты Федерального собрания;

2) Президент;

3) Органы местного самоуправления;

4) Общественная Палата;

5) Органы исполнительной власти;

6) Совет безопасности?

12. 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?

13. Основанием для видов коммерческой тайны является:

1) сфера деятельности предприятия;

2) способ организации защиты тайны;

3) отраслевая принадлежность предприятия;

4) все указанное в 1)–3);

5) все указанное в 1)–2).

14. 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).

15. При отсутствии трудовых договоров охрана КТ должна включать в себя:

1) определение перечня сведений;

2) ограничение доступа;

3) учет лиц, получивших доступ;

4) регулирование отношений с контрагентами;

5) нанесение грифа «Коммерческая тайна» (неверное зачеркнуть).

16. Не подлежит засекречиванию информация о:

1) состоянии окружающей среды;

2) состоянии здоровья премьер-министра;

3) размерах золотовалютного резерва;

4) состоянии борьбы с преступностью;

5) привилегиях.

17. Какой степени секретности НЕ существует:

1) государственной важности;

2) совершенно секретно;

3) особой важности;

4) секретно?

18. Приём переизлучённого высокочастотного сигнала "навязывания", модулированного информационным сигналом является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:

1) электромагнитный;

2) воздушный (акустический);

3) электрический;

4) радиоканал;

5) параметрический;

6) оптико-электронный.

19. Приём отражённого лазерного излучения, модулированного информационным сигналом, является инцидентом информационной безопасности и соответствует следующему типу технического канала утечки информации:

1) электромагнитный;

2) воздушный (акустический);

3) электрический;

4) радиоканал;

5) параметрический;

6) оптико-электронный.

20. 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).

21. По видам возможных источников различаются угрозы НСД к информации, создаваемые:

1) нарушителем;

2) аппаратной закладкой;

3) вредоносными программами;

4) сетевыми атаками (лишнее зачеркнуть).

22. 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)

23. Сколько текстовой информации может быть скрыто методами стеганографии в цветной фотографии формата *bmp*, сделанной мегапиксельной камерой мобильного телефона?

1) 108 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5);

2) 71 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5);

3) 23 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5)?

24. Сколько текстовой информации может быть скрыто методами стеганографии в 30 секундах моно-звучания на ПК музыкального фрагмента в формате wav?

1) 108 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5);

2) 71 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5);

3) 23 страниц формата А4 (шрифт Times New Roman, фонт 14, интервал 1,5)?

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 вопросы круглого стола

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

Ключ к тестам

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Тест | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Ключ | 2) | 1) | 2) | 3) | 1) | 1) | 3) | 2) |
| Тест | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Ключ | 1) | 3),2),4),1),5) | 4) | 3) | 5) | 3) | 1), 2) | 4) |
| Тест | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| Ключ | 1) | 5) | 6) | 5) | 4) | 6) | 3) | 1) |

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

Таблица 7

|  |  |  |  |
| --- | --- | --- | --- |
| Код компетенции | Наименованиекомпетенции | 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 |

Таблица 8

| Этап освоения компетенции | Показательоценивания | 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 стандартов информационной 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.

**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 9

|  |  |
| --- | --- |
| **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 10

|  |  |
| --- | --- |
| 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 11

|  |  |  |
| --- | --- | --- |
| №п/п | Наименование темы или раздела дисциплины (модуля)  | Контрольные вопросы для самопроверки |
|
| 1 | Тема 1. Категория информационной безопасности. Каналы силового деструктивного воздействия на информацию | 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 сети | 1. Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети.
2. Понятие и функционал DLP-систем.
3. Объем и структура данных защищаемых DLP-системами.
4. Каналы коммуникаций, контролируемые DLP-системами.
5. 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. 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>
4. 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>

Все источники основной литературы взаимозаменяемы.

**6.2 Дополнительная литература**

1. 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.
2. 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.
3. 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.
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>
5. 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>
6. 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.**

1. Положение o организации самостоятельной работы студентов федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (в ред. приказа РАНХиГС от 11.05.2016 г. № 01-2211);
2. Положение о курсовой работе (проекте) выполняемой студентами федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (в ред. приказа РАНХиГС от 11.05.2016 г. № 01-2211)

**6.4. Нормативные правовые документы.**

Не используются

**6.5. Интернет-ресурсы.**

Рекомендуется использовать следующий интернет-ресурсы

<http://serg.fedosin.ru/ts.htm>

<http://window.edu.ru/resource/188/64188/files/chernyshov.pdf>

## **Электронно-образовательные ресурсы на сайте научной библиотеки СЗИУ РАНХиГС** (<http://nwipa.ru>)

1. Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс» <http://www.nwapa.spb.ru/index.php?page_id=76>
2. Электронные учебники электронно-библиотечной системы (ЭБС) «Лань» <http://www.nwapa.spb.ru/index.php?page_id=76>
3. Электронные учебники электронно-библиотечной системы (ЭБС) [«IPRbooks»](http://www.iprbookshop.ru/) <http://www.nwapa.spb.ru/index.php?page_id=76>
4. Электронные учебники электронно-библиотечной системы (ЭБС) «Юрайт»

 <http://www.nwapa.spb.ru/index.php?page_id=76>

1. Научно-практические статьи по экономике и финансам Электронной библиотеки ИД «Гребенников» <http://www.nwapa.spb.ru/index.php?page_id=76>
2. Статьи из журналов и статистических изданий Ист-Вью <http://www.nwapa.spb.ru/index.php?page_id=76>
3. 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.
4. **Emerald eJournals Premier -** крупнейшее мировое издательство, специализирующееся на электронных журналах и базах данных по экономике и менеджменту.

**6.6. Иные источники.**

Не используются.

**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.