

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Андрей Драгомирович Хлутков  
Должность: директор  
Дата подписания: 03.12.2024 20:09:15  
Уникальный программный ключ:  
880f7c07c583b07b775f6604a630281b13ca9fd2

**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 иностранных языков

УТВЕРЖДЕНО

Директор СЗИУ РАНХиГС Хлутков А.Д.

**ПРОГРАММА БАКАЛАВРИАТА**

**Лингвистика и межкультурная коммуникация**  
*(наименование образовательной программы)*

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,  
реализуемой без применения электронного (онлайн) курса**

**Б1.В.ДВ.01.01 Информационная безопасность**  
*(код и наименование РПД)*

**45.03.02 Лингвистика**  
*(код, наименование направления подготовки)*

**Очная**  
*(форма обучения)*

Год набора – 2024

Санкт-Петербург, 2024 г.

**Автор-составитель:**

Доцент кафедры иностранных языков СЗИУ РАНХиГС, кандидат филол. наук А.А. Яковлев.

Заведующий кафедрой  
кандидат культурологии, доц. А.Е. Дельва

РПД «Б1.В.ДВ.01.01 Информационная безопасность» одобрена на заседании кафедры иностранных языков. Протокол №3 от 25.12.2023.

## СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Материалы текущего контроля успеваемости обучающихся
5. Оценочные материалы промежуточной аттестации по дисциплине
6. Методические материалы для освоения дисциплины
7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет"
  - 7.1. Основная литература
  - 7.2. Дополнительная литература
  - 7.3. Нормативные правовые документы и иная правовая информация
  - 7.4. Интернет-ресурсы
  - 7.5. Иные источники
8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Дисциплина Б1.В.ДВ.01.01 «Информационная безопасность» обеспечивает овладение следующими компетенциями:

*Таблица 1*

Код компетенции	Наименование компетенции	Код компонента компетенции	Наименование компонента компетенции
ПК-2	Способность осуществлять подготовку к выполнению перевода, включая поиск информации в справочной, специальной литературе и компьютерных сетях	ПК-2.2	Способен находить достоверную информацию в справочной, специальной литературе и компьютерных сетях, использовать информационные технологии
ПК-11	Способность работать с основными информационно-поисковыми и экспертными системами, системами представления знаний, синтаксического и морфологического анализа, автоматического синтеза и распознавания речи, обработки лексикографической информации и автоматизированного перевода, автоматизированными системами идентификации и верификации личности	ПК-11.1	Способен корректно использовать профильные информационные ресурсы информационно-поисковых и экспертных систем
		ПК-11.2	Способен использовать рациональные приемы поиска и применения программных продуктов автоматизированного перевода
		ПК-11.3	Способен работать с автоматизированными системами идентификации и верификации личности

2.1 В результате освоения дисциплины у студентов должны быть сформированы:

*Таблица 2*

ОТФ/ТФ	Код компонента компетенции	Результаты обучения
Письменный перевод (в том числе с использованием специализированных инструментальных средств) Перевод аудиовизуальных произведений	ПК-2.2	Способен находить достоверную информацию в справочной, специальной литературе и компьютерных сетях

<p>Управление качеством перевода  Технологическая обработка  материалов переводческих и  локализационных проектов  Автоматизация переводческих и  локализационных проектов  Редакционно-технический контроль  перевода  Управление производственным  процессом перевода</p>		
<p>Письменный перевод (в том числе с  использованием специализированных  инструментальных средств)  Перевод аудиовизуальных  произведений  Управление качеством перевода  Технологическая обработка  материалов переводческих и  локализационных проектов  Автоматизация переводческих и  локализационных проектов  Редакционно-технический контроль  перевода  Управление производственным  процессом перевода</p>	ПК-11.1	Способен корректно использовать профильные информационные ресурсы информационно-поисковых и экспертных систем
<p>Письменный перевод (в том числе с  использованием специализированных  инструментальных средств)  Перевод аудиовизуальных  произведений  Управление качеством перевода  Технологическая обработка  материалов переводческих и  локализационных проектов  Автоматизация переводческих и  локализационных проектов  Редакционно-технический контроль  перевода  Управление производственным  процессом перевода</p>	ПК-11.2	Способен использовать рациональные приемы поиска и применения программных продуктов автоматизированного перевода
<p>Письменный перевод (в том числе с  использованием специализированных  инструментальных средств)  Перевод аудиовизуальных  произведений  Управление качеством перевода  Технологическая обработка  материалов переводческих и  локализационных проектов  Автоматизация переводческих и  локализационных проектов  Редакционно-технический контроль</p>	ПК-11.3	Способен работать с автоматизированными системами идентификации и верификации личности

перевода Управление производственным процессом перевода		
---	--	--

## 2. Объем и место дисциплины в структуре ОП ВО

**Объем дисциплины.** Общая трудоемкость дисциплины «Информационная безопасность» составляет 3 зачётных единицы, 108 академ. часов, 81 астрономический час.

Дисциплина реализуется с применением дистанционных образовательных технологий (далее - ДОТ).

Вид работы	Трудоемкость (в академ. часах / в астроном. часах)
<b>Общая трудоемкость</b>	108/81
<b>Контактная работа с преподавателем</b>	54/40,5 2/1,5 ч. консультация
Лекции	26/19,5
Практические занятия	28/21
Лабораторные занятия	-
<b>Практическая подготовка</b>	-
<b>Самостоятельная работа</b>	16/12
Контроль	36/27
Формы текущего контроля	Устный опрос, тестирование
<b>Форма промежуточной аттестации</b>	Экзамен – 1 семестр

**Место дисциплины в структуре ОП ВО.** Дисциплина Б1.В.ДВ.01.01 «Информационная безопасность» относится к вариативной части учебной программы направления 45.03.02-Лингвистика.

Учебная дисциплина «Информационная безопасность» создает предпосылки для освоения программы такой дисциплины по выбору студента, как Б1.В.ДВ.01.02 «Работа в интернет».

Дисциплина читается на 1 курсе в 1 семестре по очной форме обучения.

Формой промежуточного контроля в соответствии с учебным планом является экзамен.

Доступ к системе дистанционных образовательных технологий осуществляется каждым обучающимся самостоятельно с любого устройства на портале: <https://lms.ranepa.ru/>. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате.

Все формы текущего контроля, проводимые в системе дистанционного обучения, оцениваются в системе дистанционного обучения. Доступ к видео и материалам лекций предоставляется в течение всего семестра. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется на ограниченное время согласно регламенту дисциплины, опубликованному в СДО. Преподаватель оценивает выполненные обучающимся работы не позднее 10 рабочих дней после окончания срока выполнения

### 3. Содержание и структура дисциплины

#### 3.1. Структура дисциплины

Таблица 4

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.					СР	Форма текущего контроля успеваемости*, промежуточной аттестации**
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					
			Л/ДОТ	ЛР/ДОТ	ПЗ/ДОТ	КСР		
Тема 1	Основные понятия защиты информации и информационной безопасности	10	4		4		2	УО
Тема 2	Политика и стандарты информационной безопасности	10	4		4		2	УО, Т
Тема 3.	Принципы криптографической защиты информации	10	4		4		2	УО, Т
Тема 4.	Технологии защиты межсетевого обмена данными	10	4		4		2	УО, Т
Тема 5.	Основы технологии виртуальных защищенных сетей	16	4		6		4	УО, Т
Тема 6.	Технологии обнаружения вторжений	18	6		6		4	УО, Т
Промежуточная аттестация		<b>36/27</b>				<b>2</b>		<b>Экзамен</b>
<b>Всего:</b>		<b>108/81</b>	<b>26/19,5</b>		<b>28/21</b>		<b>16/12</b>	

Используемые сокращения:

Л – занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся)<sup>1</sup>;

ЛР – лабораторные работы (вид занятий семинарского типа)<sup>2</sup>;

ПЗ – практические занятия (виды занятий семинарского типа за исключением лабораторных работ)<sup>3</sup>;

<sup>1</sup> Абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

<sup>2</sup> См. абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

КСР – индивидуальная работа обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации)<sup>4</sup>;

ДОТ – занятия, проводимые с применением дистанционных образовательных технологий, в том числе с применением виртуальных аналогов профессиональной деятельности.

СР – самостоятельная работа, осуществляемая без участия педагогических работников организации и (или) лиц, привлекаемых организацией к реализации образовательных программ на иных условиях.

*Примечание:* УО – устный опрос; Т – тестирование

### 3.2. Содержание дисциплины

Таблица 3.2

Номер темы (раздела)	Содержание разделов (тем)
1	Базовые понятия и основы информационной безопасности. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Введение в сетевой информационный обмен. Анализ угроз информационной безопасности. Обеспечение информационной безопасности сетей. Угрозы и уязвимости беспроводных сетей.
2	Основные понятия политики безопасности. Структура политики безопасности организации. Базовая и специализированные политики безопасности. Процедуры безопасности. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Стандарты для беспроводных сетей. Стандарты информационной безопасности в Интернете. Отечественные стандарты безопасности информационных технологий.
3	Основные понятия криптографической защиты информации. Симметричные, асимметричные и комбинированная криптосистемы шифрования. Электронная цифровая подпись и функция хэширования. Управление криптоключами. Криптографические алгоритмы и их классификации. Блочные алгоритмы шифрования данных. Алгоритм шифрования RSA. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.
4	Обеспечение безопасности операционных систем (ОС). Проблемы обеспечения безопасности ОС. Угрозы безопасности. Архитектура подсистемы защиты ОС. Основные функции подсистемы защиты ОС. Идентификация, аутентификация и авторизация субъектов доступа. Функции межсетевых экранов (МЭ). Особенности функционирования МЭ на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ. Формирование политики

<sup>3</sup> См. абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)

<sup>4</sup> Абзац 2 пункта 31 Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Минобрнауки России от 05 апреля 2017 г. № 301 (ред. от 17.08.2020) (зарегистрирован Минюстом России 14 июля 2017г., регистрационный № 47415)



	межсетевого взаимодействия. Персональные и распределительные сетевые экраны. Проблемы безопасности МЭ.
5	Концепция построения виртуальных защищенных сетей VPN. Основные понятия и функции сети VPN. Варианты построения виртуальных защищенных каналов. Средства обеспечения безопасности VPN. Достоинства применения технологий VPN. Протоколы формирования защищенных каналов на канальном уровне (PPTP и L2TP). Протоколы формирования защищенных каналов на сеансовом уровне (SSL/TLS и SOCKS). Защита на сетевом уровне – протокол IPSEC. Инфраструктура защиты на прикладном уровне. Организация защищенного удаленного доступа. Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO). Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.
6	Анализ защищенности и обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Технологии обнаружения атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Методы реагирования. Защита от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Основные каналы распространения вирусов и других вредоносных программ. Антивирусные программы и комплексы. Построение системы антивирусной защиты корпоративной сети.

#### 4. Материалы текущего контроля успеваемости обучающихся

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

- при проведении занятий лекционного типа (с ДОТ): тестирование (ДОТ);
- при проведении занятий семинарского типа (аудиторно): опрос, дискуссия (устные ответы на вопросы преподавателя по теме занятия, групповое обсуждение вопросов); преподаватель, реализующий дисциплину, определяет самостоятельно планы семинарских занятий;
- при контроле результатов самостоятельной работы студентов (аудиторно): устный экзамен по билетам / тест.

С применением ДОТ проводятся тестирования. Для успешного освоения курса учащемуся рекомендуется ознакомиться с литературой, размещенной в разделе 6, и материалами, выложенными в ДОТ.

Таблица 6

№	Тема и / или раздел	Методы текущего контроля успеваемости в аудитории
1	Основные понятия защиты информации и информационной безопасности	Устный опрос
2	Политика и стандарты информационной безопасности	Устный опрос, тестирование
3	Принципы криптографической защиты информации	Устный опрос, тестирование
4	Технологии защиты межсетевого обмена данными	Устный опрос, тестирование
5	Основы технологии виртуальных защищенных сетей	Устный опрос, тестирование
6	Технологии обнаружения вторжений	Устный опрос, тестирование
7	Основные понятия защиты информации и	Устный опрос, тестирование

## 4.2. Типовые материалы текущего контроля успеваемости обучающихся

### Типовые материалы для проведения тестирования:

1. Тест на владение профессиональной лексикой. Пример:

1. \_\_\_\_\_ - это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

- а) защита информации от утечки
- б) защита информации
- в) защита информации от несанкционированного воздействия
- г) защита информации от непреднамеренного воздействия

2. \_\_\_\_\_ - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

- а) защита информации от несанкционированного доступа
- б) защита информации от агентурной разведки
- в) защита информации от разглашения
- г) защита информации от несанкционированного воздействия

3. \_\_\_\_\_ - проверка соответствия организации и эффективности защиты информации установленным требованиям и (или) нормам в области защиты информации

- а) контроль состояния защиты информации
- б) способ защиты информации
- в) средство защиты информации
- г) средство контроля эффективности защиты информации

## 5. Оценочные материалы промежуточной аттестации по дисциплине

5.1. Экзамен проводится в устной форме по билетам по окончании 1 семестра.

### 5.2. Оценочные средства для промежуточной аттестации

Таблица 7

Компонент компетенции	Промежуточный / ключевой индикатор оценивания	Критерий оценивания
ПК-2.2 Умеет находить достоверную информацию в справочной, специальной литературе и компьютерных сетях	Способен находить достоверную информацию в справочной, специальной литературе и компьютерных сетях, использовать информационные технологии	Способен на высоком уровне находить достоверную информацию в справочной, специальной литературе и компьютерных сетях Способен на хорошем уровне находить достоверную информацию в справочной, специальной литературе и компьютерных сетях Способен на низком уровне находить достоверную

		<p>информацию в справочной, специальной литературе и компьютерных сетях находить достоверную информацию в справочной, специальной литературе и компьютерных сетях</p> <p>Не способен находить достоверную информацию в справочной, специальной литературе и компьютерных сетях</p>
<p>ПК-11.1</p> <p>Корректно использует профильные информационные ресурсы информационно-поисковых и экспертных систем</p>	<p>Способен корректно использовать профильные информационные ресурсы информационно-поисковых и экспертных систем</p>	<p>Способен на высоком уровне корректно использовать профильные информационные ресурсы информационно-поисковых и экспертных систем</p> <p>Способен на хорошем уровне корректно использовать профильные информационные ресурсы информационно-поисковых и экспертных систем</p> <p>Способен на низком уровне корректно использовать профильные информационные ресурсы информационно-поисковых и экспертных систем</p> <p>Не способен корректно использовать профильные информационные ресурсы информационно-поисковых и экспертных систем</p>
<p>ПК-11.2</p> <p>Использует рациональные приемы поиска и применения программных продуктов автоматизированного перевода</p>	<p>Способен использовать рациональные приемы поиска и применения программных продуктов автоматизированного перевода</p>	<p>Способен на высоком уровне использовать рациональные приемы поиска и применения программных продуктов автоматизированного перевода</p> <p>Способен на хорошем уровне использовать рациональные приемы поиска и применения программных продуктов автоматизированного перевода</p> <p>Способен на низком уровне использовать рациональные приемы поиска и применения программных продуктов автоматизированного перевода</p> <p>Не способен использовать рациональные приемы поиска</p>

		и применения программных продуктов автоматизированного перевода
ПК-11.3 Знаком с автоматизированными системами идентификации и верификации личности	Знаком с автоматизированными системами идентификации и верификации личности	Отлично знаком с автоматизированными системами идентификации и верификации личности Хорошо знаком с автоматизированными системами идентификации и верификации личности Удовлетворительно знаком с автоматизированными системами идентификации и верификации личности Плохо знаком с автоматизированными системами идентификации и верификации личности

### Типовые оценочные материалы промежуточной аттестации

#### Типовые вопросы, выносимые на экзамен:

1. Эволюция каналов передачи информации.
2. Понятия и определения области информационной безопасности.
3. Информационные угрозы и способы защиты от них.
4. Доктрина информационной безопасности РФ.
5. Законодательный уровень защиты информации.
6. Процедурный уровень обеспечения информационной безопасности.
7. Компьютерные вирусы и антивирусные программы.
8. Методы и технологии борьбы с компьютерными вирусами.
9. Криптография.
10. Биометрия.
11. Индивидуальная и государственная защита информации.
12. Информационная война.
13. Особенности управления информацией в городах.
14. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни.
15. Информационная экономика.
16. Глобальная информатизация общества.
17. Реклама как источник информационной опасности.
18. Информационные образовательные технологии XXI века.
19. Географические информационные системы.
20. Априорный анализ надежности.

#### Шкала оценивания

Оценка результатов производится на основе балльно-рейтинговой системы (БРС).

Использование БРС осуществляется в соответствии с приказом от № 306 от 6.09.2019 «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.

При накопительной системе оценивания результатов освоения дисциплины с использованием БРС возможно получение зачета/экзамена по результатам текущего контроля («автоматически») без прохождения промежуточной аттестации.

Аттестация может проводиться как в виде эссе, так и в виде тестирования в системе LMSMoodle.

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:

Расчет итоговой рейтинговой оценки:

Количество баллов	Оценка	
	прописью	буквой
96-100	отлично	А
86-95	отлично	В
71-85	хорошо	С
61-70	хорошо	Д
51-60	удовлетворительно	Е

Перевод балльных оценок в академические отметки «отлично», «хорошо», «удовлетворительно»

- «Отлично» (А) - от 96 по 100 баллов – теоретическое содержание курса освоено полностью, без пробелов необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено максимальным числом баллов.

- «Отлично» (В) - от 86 по 95 баллов – теоретическое содержание курса освоено полностью, без пробелов необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

- «Хорошо» (С) - от 71 по 85 баллов – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.

- «Хорошо» (Д) - от 61 по 70 баллов – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным

материалом сформированы недостаточно, большинство предусмотренных программой обучения учебных заданий выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.

- «Удовлетворительно» (Е) - от 51 по 60 баллов – теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий выполнены с ошибками.

## **6. Методические указания для обучающихся по освоению дисциплины**

Рабочей программой дисциплины предусмотрены следующие виды аудиторных занятий: лекции, практические занятия, контрольные работы. На лекциях рассматриваются наиболее сложный материал дисциплины. Лекция сопровождается презентациями, компьютерными текстами лекции, что позволяет студенту самостоятельно работать над повторением и закреплением лекционного материала. Для этого студенту должно быть предоставлено право самостоятельно работать в компьютерных классах в сети Интернет.

Практические занятия предназначены для самостоятельной работы студентов по решению конкретных задач дискретно математики. Ряд практических занятий проводится в компьютерных классах с использованием Excel. Каждое практическое занятие сопровождается домашними заданиями, выдаваемыми студентам для решения внеаудиторное время. Для оказания помощи в решении задач имеются тексты практических заданий с условиями задач и вариантами их решения.

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».

С целью активизации самостоятельной работы студентов в системе дистанционного обучения Moodle разработан учебный курс «Имитационное моделирование», включающий набор файлов с текстами лекций, практикума, примерами задач, а также набором тестов для организации электронного обучения студентов.

Для активизации работы студентов во время контактной работы с преподавателем отдельные занятия проводятся в интерактивной форме. В основном, интерактивная форма занятий обеспечивается при проведении занятий в компьютерном классе. Интерактивная форма обеспечивается наличием разработанных файлов с заданиями, наличием контрольных вопросов, возможностью доступа к системе дистанционного обучения, а также к тестеру.

Для работы с печатными и электронными ресурсами СЗИУ имеется возможность доступа к электронным ресурсам. Организация работы студентов с электронной библиотекой указана на сайте института (странице сайта – «Научная библиотека»).

### **Методические рекомендации по самостоятельной работе**

Положение об 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). — URL: [http://www.ranepa.ru/images/docs/prikazy-ranhigs/Pologenie\\_o\\_samostoyatelnoi\\_rabote.pdf](http://www.ranepa.ru/images/docs/prikazy-ranhigs/Pologenie_o_samostoyatelnoi_rabote.pdf).  
Режим свободного доступа.

## 7. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

### 7.1. Основная литература

1. Суворова, Г. М. Информационная безопасность: учебное пособие / Г. М. Суворова. — Саратов: Вузовское образование, 2019. — 214 с.
2. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов : Ай Пи Эр Медиа, 2019. — 227 с.
3. Чернова Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с.
4. Шаньгин В.Ф. Информационная безопасность и защита информации: учеб. пособие / В.Ф. Шаньгин.- Саратов:Профобразование, 2017.- 702с.

Все источники основной литературы взаимозаменяемы

### 7.2 Дополнительная литература

1. Артемов А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с.
2. Нестеров С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2018. — 321 с.
3. Мельников Д.А. Информационная безопасность открытых систем: учебник для студентов, обучающихся по направлению "Прикладная информатика" / Д.А. Мельников.- Москва:Флинта [и др.], 2013.- 442.с
4. Петров С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с.
5. Родичев Ю.А. Информационная безопасность: нормативно - правовые аспекты: учеб. пособие / Ю.А. Родичев.- Санкт-Петербург [и др.]:Питер, 2008.- 272с.

### 7.3. Нормативные правовые документы

Не используются

### 7.4. Интернет-ресурсы

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

#### *Русскоязычные ресурсы*

- *Электронные учебники* электронно - библиотечной системы (ЭБС) «Айбукс»

- *Электронные учебники* электронно – библиотечной системы (ЭБС) «Лань»

Рекомендуется использовать следующий интернет-ресурсы

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

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

### 7.5. Иные источники

Не используются.

## 8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Часть практических занятий проводится в компьютерном классе. Учебная дисциплина включает использование программного обеспечения Microsoft Power Point для подготовки графических иллюстраций.

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).

Система дистанционного обучения Moodle.