**Министерство образования и науки Российской Федерации**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Российский экономический университет имени Г.В. Плеханова»**

**Саратовский социально-экономический институт (филиал)**



**Кафедра информационных систем в экономике**

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

**Б1.В.07.01 Информационная безопасность**

**Направление подготовки 38.03.05 Бизнес-информатика**

**Направленность (профиль) программы**

***«Информационные системы управления бизнесом»***

**Уровень высшего образования *– Бакалавриат***

**Программа подготовки – *Прикладной бакалавриат***

Саратов – 2016 г.

Рабочая программа утверждена на заседании кафедры информационных систем в экономике,

протокол № 1 от 29 августа 2016 г.

Заведующий кафедрой Волошин И.П.

(Ф.И.О.)

Одобрено советом факультета экономики и менеджмента,

протокол № 1 от 08 сентября 2016 г.

Председатель Ведяева Е.С.

(Ф.И.О.)

Дополнения и изменения, внесенные в рабочую программу, утверждены на заседании кафедры информационных систем в экономике, протокол № 1 от 29 августа 2016 г.

*(изменения внесены в перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю); перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины; перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем)*

Заведующий кафедрой

(подпись) (Ф.И.О.)

Одобрено советом факультета ,

протокол № от « » 201 г.

Председатель

(подпись) (Ф.И.О.)

Дополнения и изменения, внесенные в рабочую программу, утверждены на заседании кафедры ,

протокол № от « » 201 г.

Заведующий кафедрой

(подпись) (Ф.И.О.)

Одобрено советом факультета ,

протокол № от « » 201 г.

Председатель

(подпись) (Ф.И.О.)

Дополнения и изменения, внесенные в рабочую программу «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»,

*название дисциплины*

утверждены на заседании кафедры \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 201 \_ г.

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Одобрено советом факультета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201 \_ г.

Председатель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Дополнения и изменения, внесенные в рабочую программу «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»,

*название дисциплины*

утверждены на заседании кафедры \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 201 \_ г.

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Одобрено советом факультета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201 \_ г.

Председатель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Дополнения и изменения, внесенные в рабочую программу «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»,

*название дисциплины*

утверждены на заседании кафедры \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 201 \_ г.

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Одобрено советом факультета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201 \_ г.

Председатель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Дополнения и изменения, внесенные в рабочую программу «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»,

*название дисциплины*

утверждены на заседании кафедры \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 201 \_ г.

Заведующий кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

Одобрено советом факультета \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

протокол № \_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201 \_ г.

Председатель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (Ф.И.О.)

**Содержание**

[I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ 5](#_Toc470469250)

[Цель дисциплины 5](#_Toc470469251)

[Учебные задачи дисциплины 5](#_Toc470469252)

[Место дисциплины в структуре ОПОП ВО (основной профессиональной образовательной программы высшего образования) 5](#_Toc470469253)

[Требования к результатам освоения содержания дисциплины 6](#_Toc470469254)

[Формы контроля 7](#_Toc470469255)

[II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 7](#_Toc470469256)

[III. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 8](#_Toc470469257)

[IV. УЧЕБНО-МЕТОДИЧЕСКОЕ, ИНФОРМАЦИОННОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 9](#_Toc470469258)

[Рекомендуемая литература 9](#_Toc470469259)

[Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля) 9](#_Toc470469260)

[Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости) 10](#_Toc470469261)

[Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине 10](#_Toc470469262)

[Материально-техническое обеспечение дисциплины 11](#_Toc470469263)

[V. ТЕМАТИЧЕСКИЙ ПЛАН ИЗУЧЕНИЯ ДИСЦИПЛИНЫ 12](#_Toc470469264)

[VI. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ 12](#_Toc470469265)

[Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы (см. таблицу раздела II) 13](#_Toc470469266)

[Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (см. таблицу раздела II и раздел VIII) 13](#_Toc470469267)

[Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. 13](#_Toc470469268)

[Примеры тестов для контроля знаний 14](#_Toc470469269)

[VII. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) 17](#_Toc470469270)

[VIII. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ 17](#_Toc470469271)

## I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

## Цель дисциплины

Целью дисциплины «Информационная безопасность» является получение студентами целостного представления о современных методах и средствах обеспечения информационной безопасности и их практического применения. На основе полученных знаний сформировать у студентов системный подход к решению проблем информационной безопасности.

## Учебные задачи дисциплины

Задачами дисциплины являются:

* освоение основных понятий и терминологии информационной безопасности;
* знакомство с угрозами, которым подвергается информация, а также классификацией этих угроз и их анализом;
* изучение организационно-административных и технических методов и средств защиты информации;
* изучение криптографических методов защиты информации;
* изучение нормативно-законодательной базы и стандартов информационной безопасности и защиты информации;
* изучение моделей информационной безопасности;
* обеспечение безопасности автоматизированных систем;
* обеспечение компьютерной и сетевой безопасности.

## Место дисциплины в структуре ОПОП ВО (основной профессиональной образовательной программы высшего образования)

Дисциплина «Информационная безопасность» относится к обязательным дисциплинам вариативной части Блока 1 «Дисциплины (модули)» учебного плана основной профессиональной образовательной программы по направлению подготовки 38.03.05 Бизнес-информатика, направленность (профиль) образовательной программы «Информационные системы управления бизнесом».

**Объем дисциплины и виды учебной работы**

|  |  |
| --- | --- |
| **Показатель объема дисциплины** | **Всего часов** |
| **Очная ф.о.** |
| Объем дисциплины в зачетных единицах | 4 |
| Объем дисциплины в часах | 144 |
| Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего) | 46 |
| Объем аудиторной работы (всего) | 46 |
| в том числе: |  |
| * лекции | 18 |
| * лабораторные занятия | 28 |
| * практические занятия |  |
| Объем электронного обучения |  |
| Самостоятельная работа (всего) | 62 |
| Подготовка к экз. | 36 |

Дисциплина «Информационная безопасность» основывается на знании дисциплины «Информационные технологии».

Для успешного освоения дисциплины «Информационная безопасность», студент должен:

**1)знать**: основы алгебры, математического анализа, дискретной математики, информационных технологий (ОПК-2);

**2) уметь**: использовать современные технические средства и информационные технологии для решения аналитических и исследовательских задач (ПК-2);

**3)** **владеть:** навыками эксплуатировать современное электронное оборудование и информационно-коммуникационные технологии на основе знаний естественнонаучных дисциплин, методами анализа рынка программно-технических средств, информационных продуктов и услуг для решения прикладных задач (ОПК-3).

## Требования к результатам освоения содержания дисциплины

***(Планируемые результаты обучения по дисциплине (модулю)***

В результате освоения дисциплины должны быть сформированы следующие компетенции:

**ОК-9 - способностью использовать приемы первой помощи, методы защиты в условиях чрезвычайных ситуаций**

В результате освоения компетенции **ОК- 9** студент должен:

1. **Знать:**

виды угроз и методы обеспечения информационной безопасности;

**2) Уметь:**

выявлять угрозы информационной безопасности;

**3) Владеть:**

навыками защиты от вредной информации;

**ОПК-1 - способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**

В результате освоения компетенции **ОПК- 1** студент должен:

1. **Знать:**

основные требования информационной безопасности при получении, хранении и переработке информации;

**2) Уметь:**

применять методы информационной безопасности при поиске информации, сборе и анализе конфиденциальных сведений в профессиональной деятельности;

**3) Владеть:**

современными методами защищенного сбора, обработки и анализа данных;

**ПК-9 - организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия**

В результате освоения компетенции **ПК- 9** студент должен:

1. **Знать:**

техническое и программное обеспечение для решения задач информационной безопасности;

**2) Уметь:**

обосновывать организационно-технические мероприятия по защите информации;

**3) Владеть:**

инструментальными средствами защиты информации;

**ПК-11 - умение защищать права на интеллектуальную собственность**

В результате освоения компетенции **ПК- 11** студент должен:

1. **Знать:**

состояние законодательной базы информационной безопасности;

**2) Уметь:**

оценивать защищенность информационных ресурсов;

**3) Владеть:**

навыками применения стеганографических меток на цифровых объектах интеллектуальной собственности;

## Формы контроля

*Текущий и рубежный контроль* осуществляется лектором и преподавателем, ведущим лабораторные занятия, в соответствии с тематическим планом.

*Промежуточная аттестация в 3 семестре* – **экзамен**

.

# II. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

**и описание показателей и критериев оценивания компетенций на различных этапах их формирования в процессе освоения образовательной программы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование раздела дисциплины (темы) | Содержание | Формируемые компетенции | Результаты освоения (знать, уметь, владеть, понимать) | **Образовательные технологии** |
| **1** | Тема 1. Основы информационной безопасности. | Понятие безопасности. Концепция информацион-ной безопасности России. Принципы и организация защиты информации. Меры, способы и средства защиты информации. | **ОК-9**  **ОПК-1**  **ПК-11** | **Знать:** виды угроз и методы обеспечения информационной безопасности  **Уметь:** выявлять угрозы информационной безопасности  **Знать:** основные требования информационной безопасности при получении, хранении и переработке информации  **Знать:** состояние законодательной базы информационной безопасности | Лекции, лабораторные работы, домашнее практическое задание, самостоятельная работа с литературой, консультации преподавателей |
| **2** | Тема 2. Криптографическая защита информации. Стеганография. | Основные понятия и определения при криптографической защите информации. Симметричные и ассиметричные криптоалгоритмы. Общие сведения об электронной подписи (ЭП). Проверка, передача и обновление ключей. Основные принципы компьютерной стеганографии и области её применения. | **ОК-9**  **ОПК-1**  **ПК-11** | **Владеть:** навыками защиты от вредной информации  **Уметь:** применять методы информационной безопасности при поиске информации, сборе и анализе конфиденциальных сведений в профессиональной деятельности  **Владеть:** современными методами защищенного сбора, обработки и анализа данных  **Знать:** состояние законодательной базы информационной безопасности  **Уметь:** оценивать защищенность информационных ресурсов  **Владеть:** навыками применения стеганографических меток на цифровых объектах интеллектуальной собственности |  |
| **3** | Тема 3. Защита информации в компьютерах. | Угрозы информации в персональном компьютере и обеспечение ее целост-ности. Защита персональ-ного компьютера от несанкционированного доступа. Программно-аппаратные средства защиты информации от несанкционированных действий - визуального съема, модификации, копирования, блокирования, уничтожения. Особенности защиты информации при подготовке текстовых и аналитических материалов. Подготовка и защита документов в MS Word и MS Excel. Архивирование как метод защиты данных. | **ОК-9**  **ПК-9**  **ПК-11** | **Знать:** виды угроз и методы обеспечения информационной безопасности  **Уметь:** выявлять угрозы информационной безопасности  **Владеть:** навыками защиты от вредной информации  **Знать:** техническое и программное обеспечение для решения задач информационной безопасности;  **Уметь:** обосновывать организационно-технические мероприятия по защите информации  **Владеть:** инструментальными средствами защиты информации  **Уметь:** оценивать защищенность информационных ресурсов | Лабораторные работы, мастер-класс, домашнее практическое задание, самостоятельная работа с литературой, консультации преподавателей |
| **4** | Тема 4. Особенности защиты информации в вычислительных сетях. | Цели, функции и задачи защиты информации в вычислительных сетях. Понятие сервисов безопасности. Архитектура механизмов защиты информации в компьютерных сетях. | **ОК-9**  **ПК-9** | **Знать:** виды угроз и методы обеспечения информационной безопасности  **Уметь:** выявлять угрозы информационной безопасности  **Владеть:** навыками защиты от вредной информации  **Знать:** техническое и программное обеспечение для решения задач информационной безопасности;  **Уметь:** обосновывать организационно-технические мероприятия по защите информации  **Владеть:** инструментальными средствами защиты информации | Лабораторные работы, мастер-класс, домашнее практическое задание, самостоятельная работа с литературой, консультации преподавателей |
| **5** | Тема 5. Вредоносные компьютерные программы и защита от них. | Защита компьютерной информации от разрушающих программных воздействий. Классификация компьютерных вредоносных программ и признаки их проявления. Понятие антивирусных программ и их классификация. Методы защиты информации от вредоносных программ. | **ОК-9**  **ПК-9** | **Знать:** виды угроз и методы обеспечения информационной безопасности  **Уметь:** выявлять угрозы информационной безопасности  **Владеть:** навыками защиты от вредной информации  **Знать:** техническое и программное обеспечение для решения задач информационной безопасности;  **Владеть:** инструментальными средствами защиты информации  **Уметь:** оценивать защищенность информационных ресурсов | Лекции, лабораторные работы, мастер-класс, домашнее практическое задание, самостоятельная работа с литературой, консультации преподавателей |

# III. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе освоения дисциплины используются следующие образовательные технологии:

1. **Стандартные методы обучения:**

* лекции;
* лабораторные работы проводятся в компьютерных классах и сочетают выполнение заданий по обработке, анализу, поиску информации в справочных информационно-поисковых системах, хранению и передаче информации с использованием современных программных средств и информационно-коммуникационных технологий;
* письменные домашние задания;
* самостоятельная работа проводится в форме изучения теоретического материала, доступного в библиотечном фонде вуза и в электронном формате на сайте вуза, и выполнения заданий для самостоятельной работы студентов и ответов на контрольные вопросы. Проверка самостоятельной работы студентов производится дистанционно с использованием технологий сети Интернет.

2. **Методы обучения с применением интерактивных форм образовательных технологий:**

* интерактивные лекции;
* обсуждение вопросов, возникающих в процессе решения практических задач, разбор конкретных ситуаций;
* лабораторные занятия в форме мастер-класса.

# IV. УЧЕБНО-МЕТОДИЧЕСКОЕ, ИНФОРМАЦИОННОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

(в соответствии с пунктом 7.3. «Требования к материально-техническому и учебно-методическому обеспечению программы бакалавриата» ФГОС ВО)

## Рекомендуемая литература

**Основная литература:**

1. Информационная безопасность: учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева. – М.: Русайнс, 2016. – 354 с. (ЭБС)
2. Базовые понятия информационной безопасности: учебное пособие / Г.О. Крылов и др. – М.: Русайнс, 2016. – 257 с. (ЭБС)
3. Башлы П.Н. Информационная безопасность и защита информации: Учебник / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. – М.: РИОР, 2013. – 222 с. (ЭБС)

**Дополнительная литература:**

1. Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. – М.: НИЦ ИНФРА-М, 2016. – 118 с. (ЭБС)
2. Информационная безопасность. Практикум (+CD): учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2016. – 131 с. (ЭБС)
3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-e изд., доп. – М.: Форум: НИЦ ИНФРА-М, 2015. – 240 с. (ЭБС)
4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. – 592 с. (ЭБС)
5. Баранова, Е. К. Основы информатики и защиты информации: Учеб. пособие / Е. К. Баранова. – М.: РИОР: ИНФРА-М, 2013. – 183 с. (ЭБС)

## Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

1. http:// www.all-ib.ru/
2. http:// www.pravo.fso.gov.ru/
3. http:// www.fstec.ru/
4. http:// www.iso27000.ru/
5. http:// www.kaspersky.ru/

## Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Перечень информационных технологий, программного обеспечения,**  **информационных справочных систем** | **Номера тем** |
|  | Microsoft Office | 1-5 |
|  | Google Chrome | 1-5 |

## Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

**Тема 1. Основы информационной безопасности.**

**Литература** О – 1, 2; Д – 1, 2, 3, 4, 5

**Вопросы для самопроверки:**

1. Понятие безопасности. Концепция информационной безопасности России.
2. Принципы и организация защиты информации.
3. Меры, способы и средства защиты информации.

**Задания для самостоятельной работы:**

1. Самостоятельное изучение основной и дополнительной литературы.
2. Домашнее практическое задание.

**Тема 2. Криптографическая защита информации. Стеганография.**

**Литература** О – 1, 3; Д – 1, 2, 3, 4, 5.

**Вопросы для самопроверки:**

1. Основные понятия и определения при криптографической защите информации.
2. Симметричные и ассиметричные криптоалгоритмы.
3. Общие сведения об электронной подписи (ЭП). Проверка, передача и обновление ключей.
4. Основные принципы компьютерной стеганографии и области её применения.

**Задания для самостоятельной работы:**

1. Самостоятельное изучение основной и дополнительной литературы.
2. Домашнее практическое задание.

**Тема 3. Защита информации в компьютерах**

**Литература** О – 1, 3; Д – 1, 2, 5.

**Вопросы для самопроверки:**

1. Угрозы информации в персональном компьютере и обеспечение ее целостности. Защита персонального компьютера от несанкционированного доступа.
2. Программно-аппаратные средства защиты информации от несанкционированных действий - визуального съема, модификации, копирования, блокирования, уничтожения.
3. Особенности защиты информации при подготовке текстовых и аналитических материалов. Подготовка и защита документов в MS Word и MS Excel.
4. Архивирование как метод защиты данных.

**Задания для самостоятельной работы:**

1. Самостоятельное изучение основной и дополнительной литературы.
2. Домашнее практическое задание.

**Тема 4 Особенности защиты информации в вычислительных сетях.**

**Литература** О – 1, 3; Д – 1, 3, 4.

**Вопросы для самопроверки:**

1. Цели, функции и задачи защиты информации в вычислительных сетях.
2. Понятие сервисов безопасности.
3. Архитектура механизмов защиты информации в компьютерных сетях.

**Задания для самостоятельной работы:**

1. Самостоятельное изучение основной и дополнительной литературы.
2. Домашнее практическое задание.

**Тема 5 Вредоносные компьютерные программы и защита от них.**

**Литература** О – 1, 3; Д – 2, 3, 4, 5.

**Вопросы для самопроверки:**

1. Защита компьютерной информации от разрушающих программных воздействий.
2. Классификация компьютерных вредоносных программ и признаки их проявления.
3. Понятие антивирусных программ и их классификация.
4. Методы защиты информации от вредоносных программ.

**Задания для самостоятельной работы:**

1. Самостоятельное изучение основной и дополнительной литературы.
2. Домашнее практическое задание.

## Материально-техническое обеспечение дисциплины

Для проведения занятий по дисциплине используются лекционные аудитории, оснащенные необходимым мультимедийным оборудованием.

Лабораторные занятия проводятся в компьютерных аудиториях с достаточным количеством персональных компьютеров и установленным лицензионным программным обеспечением.

Для организации самостоятельной работы студентов им открыт доступ в компьютерные аудитории в свободное от занятий время, имеется оборудование и программное обеспечение для реализации интерактивного доступа студентов к электронным учебно-методическим материалам через сеть Интернет.

# V. ТЕМАТИЧЕСКИЙ ПЛАН ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

***(Содержание дисциплины, структурированное по темам (разделам) с указанием часов и видов занятий)***

**Очная форма обучения**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | **Наименование разделов и тем** | **Контактные часы** | | | | | | | **Самостоятельная работа** | | **Формы текущего/ рубежного контроля** |
| **Аудиторные часы** | | | | | | **Часы в электронной форме обучения** | формы | часы |
| Лекции | Практи- ческие занятия | Лабора-торные работы | Всего ауд. | **в том числе интерактивные** | |
| формы | часы |
| 1 | Тема 1. Основы информационной безопасности. | 4 |  | 6 | 10 | И.л | 2 |  | Лит., ПЗ | 12 | Устный опрос |
| 2 | Тема 2. Криптографическая защита информации. Стеганография. | 4 |  | 8 | 12 | М-к | 4 |  | Лит., ПЗ | 12 | Устный опрос, отчет по практическому заданию |
| 3 | Тема 3. Защита информации в компьютерах. | 4 |  | 6 | 10 | М-к | 2 |  | Лит., ПЗ | 14 | Устный опрос, отчет по практическому заданию |
| 4 | Тема 4. Особенности защиты информации в вычислительных сетях. | 4 |  | 6 | 10 |  |  |  | Лит., ПЗ | 12 | Устный опрос, отчет по практическому заданию |
| 5 | Тема 5. Вредоносные компьютерные программы и защита от них. | 2 |  | 2 | 4 | И.л. | 2 |  | Лит., ПЗ | 12 | Устный опрос, отчет по практическому заданию |
| **Подготовка к экзамену** | |  |  |  |  |  |  |  |  |  | **36** |
| **Итого:** | | **18** |  | **28** | **46** |  | **10** |  |  | **62** | **Экзамен** |
| **Всего по дисциплине** | | **18** |  | **28** | **46** |  | **10** |  |  | **62** |  |

Сокращения, используемые в Тематическом плане изучения дисциплины:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Сокращение** | **Вид работы** |
|  | Лит | Работа с литературой |
|  | И.л. | Интерактивная лекция |
|  | М-к. | Мастер-класс |
|  | ПЗ | Домашнее практическое задание |

# VI. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ [[1]](#footnote-1)

Оценочные средства по дисциплине разработаны в соответствии с Положением о фонде оценочных средств в ФГБОУ ВО «РЭУ им. Г.В.Плеханова».

(***Фонд оценочных средств хранится на кафедре, обеспечивающей преподавание данной дисциплины)***

## Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы (см. таблицу раздела II)

## Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (см. таблицу раздела II и раздел VIII)

## Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Курсовая работа по дисциплине «Информационная безопасность» не предусмотрена.

**Вопросы к экзамену**

1. Основные понятия информационной безопасности.
2. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
3. Классификация угроз информационной безопасности автоматизированных систем.
4. Угрозы нарушения конфиденциальности, целостности данных, отказа служб (угроза отказа в доступе). Особенности и примеры реализации угроз.
5. Понятие политики безопасности информационных систем. Назначение политики безопасности.
6. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
7. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
8. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
9. Критерии оценки безопасности компьютерных систем. Структура требований безопасности. Классы защищенности.
10. Физические средства обеспечения информационной безопасности.
11. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
12. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
13. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
14. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации.
15. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
16. Применение криптографических средств для обеспечения информационной безопасности электронного документа.
17. Симметричные алгоритмы шифрования. Шифрование методом подстановки, перестановки.
18. Использование ассимметричного шифрования для обеспечения защиты информации.
19. Понятие электронной подписи. Процедуры формирования электронной подписи.
20. Методы стеганографии.
21. Средства обеспечения информационной безопасности в Windows. Пользователи и группы в Windows. Разграничение доступа к данным. Шифрование данных.
22. Парольная защита документов MS Word, MS Excel.
23. Приемы скрытия текста и графических объектов в документе.
24. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
25. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
26. Вирусы, их классификация и методы борьбы с ними.
27. Антивирусные программы и пакеты.
28. Программно-аппаратные средства защиты информации
29. Межсетевые экраны, их функции и назначения.
30. Стеганография. Классические и компьютерные методы стеганографии. Область применения.

* ***Тестовые задания***

# Примеры тестов для контроля знаний

1. Государственная тайна – это:

1. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации
2. сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
3. защищаемые государством сведения, несанкционированное распространение которых может нанести ущерб органам государственной власти, государственным предприятиям, учреждениям, организациям или нарушить их функционирование.

2. Служебная тайна – это:

1. информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности;
2. защищаемые сведения, не являющиеся государственной тайной, несанкционированное распространение которых государственным служащим, которому эти сведения были доведены в связи с исполнением им должностных обязанностей, может нанести ущерб органам государственной власти, государственным предприятиям, учреждениям, организациям или нарушить их функционирование;
3. служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами;
4. защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

3. Конфиденциальная информация – это:

1. документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;
2. информация, требующая защиты;
3. информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

4. Как классифицируются угрозы информационным ресурсам

1. по свойству информационных ресурсов;
2. по компонентам информационных систем;
3. по способу осуществления;
4. по расположению источника угроз;
5. по объему наносимого ущерба;
6. по длительности воздействия.

5.Основные носители информации - это:

1. газеты;
2. журналы;
3. телевидение и радио;
4. люди;
5. средства связи;
6. электронные системы данных;
7. разные отслеживаемые факторы;
8. документы

6. Свойства защищаемой информации:

1. доступность;
2. целостность;
3. конфиденциальность;
4. стоимость;
5. неизменность.

7. Антивирусные программы классифицируются:

1. фильтры;
2. мониторы;
3. полифаги;
4. детекторы;
5. вакцины;
6. сканеры.

8. Основные функции системы защиты программ от копирования:

1. идентификация;
2. аутентификация;
3. регистрация санкционированного копирования;
4. регистрация несанкционированного копирования;
5. реагирование на попытки несанкционированного копирования;
6. блокирование работы программы;
7. противодействие изучению алгоритма работы системы защиты.

9. Основные способы реализации вредоносных закладок:

1. аппаратные;
2. программные;
3. технические;
4. физические;
5. организационные.

10. К аппаратным средствам защиты относятся:

1. форматирование диска;
2. физическая блокировка клавиатуры;
3. установка защиты на запись и стирание;
4. запрет и регистрация попыток записи в файлы операционной системы.

11. Механизмы защиты информации включают:

1. идентификация и аутентификация;
2. управление доступом;
3. обеспечение конфиденциальности данных и сообщений;
4. обеспечение целостности данных и сообщений;
5. контроль субъектов взаимодействия;
6. регистрация и наблюдение.

12. Разграничение доступа к защищаемой информации осуществляется:

1. по уровням;
2. по специальным спискам;
3. по допуску;
4. по должности;
5. по матрицам полномочий;
6. по специальным мандатам.

13. Уровни межсетевого взаимодействия:

1. физический;
2. прикладной;
3. канальный;
4. представительный;
5. сетевой;
6. показательный;
7. адресный;
8. транспортный;
9. сеансовый.

14. Угрозы для сетей передачи данных:

1. прослушивание каналов;
2. умышленное искажение или уничтожение сообщений;
3. преднамеренный разрыв линии связи;
4. внедрение сетевых вирусов;
5. присвоение злоумышленником своему узлу чужого имени

15. Основные активные способы несанкционированного доступа:

1. маскировка одного логического объекта под другой;
2. переадресация сообщений;
3. модификация сообщений;
4. блокировка логического объекта.

16. Основные виды средств защиты:

1. нормативно-правовые;
2. морально-этические;
3. физические;
4. организационные;
5. технические.

17. Технические методы защиты информации

1. замки;
2. решетки;
3. аппаратные;
4. аппаратно-программные;
5. системы управления доступом
6. программные.

# VII. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Положение об интерактивных формах обучения (http://www.rea.ru)

Положение об организации самостоятельной работы студентов (http://www.rea.ru)

Положение о курсовых работах (http://www.rea.ru)

Положение об учебно-исследовательской работе студентов в ФГБОУ ВО "РЭУ им. Г.В. Плеханова" (http://www.rea.ru)

Методические указания для обучающихся по освоению дисциплины (модуля) призваны оказать помощь в успешном освоении дисциплины, позволят обучающимся получить необходимые знания, умения и навыки в профессиональной деятельности и на базе их сформировать соответствующие компетенции – планируемые результаты обучения по дисциплине в соответствии с разделом Ι.

В приведенной ниже таблице даны общие рекомендации, при подготовке методических указаний для обучающихся по освоению адаптационной дисциплины для инвалидов и лиц с ограниченными возможностями здоровья «Информационно-коммуникационные технологии».

|  |  |
| --- | --- |
| Вид учебных занятий | Организация самостоятельной работы студента |
| Лекция | В ходе лекционных занятий необходимо вести конспектирование учебного материала: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. |
| Лабораторные работы | Важной составной частью учебного процесса в вузе являются лабораторные работы. Лабораторные работы помогают студентам глубже усвоить учебный материал, приобрести навыки практического использования информационных систем и технологий. |
| Практические задания | Выполняя практическое задание, студенту необходимо ознакомиться с основной и дополнительной литературой. |

# VIII. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

***Формирование балльной оценки по дисциплине «Информационная безопасность»***

В соответствии с «Положением о рейтинговой системе оценки успеваемости и качества знаний студентов в федеральном государственном бюджетном образовательном учреждении высшего образования «Российский экономический университет имени Г.В. Плеханова» распределение баллов, формирующих рейтинговую оценку работы студента, осуществляется следующим образом:

|  |  |
| --- | --- |
| Виды работ | Максимальное количество баллов |
| Посещаемость | 20 |
| Текущий и рубежный контроль | 20 |
| Творческий рейтинг | 20 |
| Промежуточная аттестация (экзамен/ зачет) | 40 |
| ИТОГО | 100 |

**Посещаемость**

В соответствии с утвержденным учебным планом по направлению подготовки 38.03.05 Бизнес-информатика по дисциплине предусмотрено:

* для очной формы обучения в семестре 3 – 9 лекций и 14 лабораторных работ. За посещение 1 занятия студент набирает 0,87 балла;

**Текущий и рубежный контроль**

|  |  |  |  |
| --- | --- | --- | --- |
| **Форма контроля** | **Наименование раздела/ темы, выносимых на контроль** | **Форма проведения контроля** | **Количество баллов, максимально** |
| 1. Текущий и рубежный контроль | Тема 1. Основы информационной безопасности. | Устный опрос | 4 |
| Тема 2. Криптографическая защита информации. Стеганография. | Устный опрос, отчет по практическому заданию | 4 |
| Тема 3. Защита информации в компьютерах. | Устный опрос, отчет по практическому заданию | 4 |
| Тема 4. Особенности защиты информации в вычислительных сетях. | Устный опрос, отчет по практическому заданию | 4 |
|  | Тема 5. Вредоносные компьютерные программы и защита от них. | Устный опрос, отчет по практическому заданию | 4 |
| **Всего** |  |  | **20** |

**Творческий рейтинг**

Распределение баллов осуществляется по решению методической комиссии кафедры и результат распределения баллов за соответствующие виды работ представляются в виде следующей таблицы:

|  |  |  |
| --- | --- | --- |
| **Наименование раздела/ темы, выносимых на контроль** | **Вид работы** | **Количество баллов** |
| Тема 1. Основы информационной безопасности. | Опрос | 4 |
| Тема 2. Криптографическая защита информации. Стеганография. | ПЗ | 4 |
| Тема 3. Защита информации в компьютерах. | ПЗ | 4 |
| Тема 4. Особенности защиты информации в вычислительных сетях. | ПЗ | 4 |
| Тема 5. Вредоносные компьютерные программы и защита от них. | ПЗ | 4 |
| **ИТОГО** |  | **20** |

**Промежуточная аттестация**

Экзамен по результатам изучения дисциплины «Информационная безопасность» в 3 семестре проводится в форме тестирования. **В итоге результаты тестирования оцениваются в баллах:**

|  |  |
| --- | --- |
| Результаты тестирования, % | **Количество баллов** |
| 85 – 100 | 40 |
| 70 – 84 | 30 |
| 50 – 69 | 20 |
| менее 50 | 0 |

**Итоговый балл** формируется суммированием баллов за промежуточную аттестацию и баллов, набранных перед аттестацией. Приведение суммарной балльной оценки к четырехбалльной шкале производится следующим образом:

**Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную**

|  |  |
| --- | --- |
| **100-балльная  система оценки** | **Традиционная четырехбалльная система оценки** |
| 85 – 100 баллов | оценка «отлично»/«зачтено» |
| 70 – 84 баллов | оценка «хорошо»/«зачтено» |
| 50 – 69 баллов | оценка «удовлетворительно»/«зачтено» |
| менее 50 баллов | оценка «неудовлетворительно»/«незачтено» |

**IV. УЧЕБНО-МЕТОДИЧЕСКОЕ, ИНФОРМАЦИОННОЕ И МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

**Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)**

## Рекомендуемая литература

**Основная литература:**

1. Информационная безопасность: учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева. – М.: Русайнс, 2016. – 354 с. (ЭБС)
2. Базовые понятия информационной безопасности: учебное пособие / Г.О. Крылов и др. – М.: Русайнс, 2016. – 257 с. (ЭБС)
3. Башлы П.Н. Информационная безопасность и защита информации: Учебник / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. – М.: РИОР, 2013. – 222 с. (ЭБС)

**Дополнительная литература:**

1. Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. – М.: НИЦ ИНФРА-М, 2016. – 118 с. (ЭБС)
2. Информационная безопасность. Практикум (+CD): учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2016. – 131 с. (ЭБС)
3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-e изд., доп. – М.: Форум: НИЦ ИНФРА-М, 2015. – 240 с. (ЭБС)
4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. – 592 с. (ЭБС)
5. Баранова, Е. К. Основы информатики и защиты информации: Учеб. пособие / Е. К. Баранова. – М.: РИОР: ИНФРА-М, 2013. – 183 с. (ЭБС)

**Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

Перечень электронных ресурсов, к которым обеспечивается доступ обучающихся:

1. http://82.179.36.11/irbis64r\_12 - электронный каталог библиотеки ССЭИ на основе  системы автоматизации библиотек (САБ) «ИРБИС64»
2. http://seun.ru/content/learning/4/science/1/?clear\_cache=Y – учебные пособия и учебно-методические материалы ССЭИ
3. http://znanium.com – электронно-библиотечная система «Знаниум»
4. http://biblioklub.ru - электронно-библиотечная система «Университетская библиотека online»
5. http://www.biblio-online.ru - электронно-библиотечная система «Юрайт»
6. http://book.ru - электронно-библиотечная система «BOOK.ru»
7. http://grebennikon.ru/ -  электронная библиотека Издательского дома "Гребенников"
8. http://search.proquest.com/business - электронно-библиотечная система «ProQuest»
9. http://www.consultant.ru/?utm\_source=sps - справочная правовая система «КонсультантПлюс»
10. http://elibrary.ru/defaultx.asp - Научная электронная библиотека eLIBRARY.RU
11. http://cyberleninka.ru/ - Научная электронная библиотека «КИБЕРЛЕНИНКА»
12. http://www.prlib.ru/Pages/default.aspx - Президентская библиотека имени Б.Н. Ельцина
13. http://www.polpred.com/ - база данных «Polpred.com Обзор СМИ»
14. http://www.ilo.org/global/lang--en/index.htm#a2 – Международный научно-исследовательский институт по вопросам труда
15. https://www.isi-web.org/ - База данных ISI (The International Statistical Institute) Международного статистического института
16. http://www.edu.ru/ - Федеральный портал «Российское образование»
17. http://window.edu.ru/ - Информационная система «Единое окно доступа к образовательным ресурсам»
18. http://school-collection.edu.ru/ - Единая коллекция цифровых образовательных ресурсов
19. http://fcior.edu.ru/ - Федеральный центр информационно-образовательных ресурсов

**Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

|  |  |
| --- | --- |
| **№ п/п** | **Наименование** |
| **Программное обеспечение** | |
|  | Microsoft office suit   1. MS Access 2007 2. MS Access 2007 – 103 ключа выдано 2010 - 3. MS Visual Studio 2008 4. MS FrontPage 2003 5. MS Visual Studio 2010 6. MS Project 2007 |
|  | Программный комплекс «Компьютерная деловая игра «Бизнес-Курс: Максимум. Версия 1» |
|  | 1С: Предприятие версии 8.2. Комплект для студентов и преподавателей |
|  | ПС ГИС «ИнГЕО 4.3» |
|  | «Дело-предприятие» под СУБД MS SQL Server версия учебное заведение  «Архивное дело» под СУБД MS SQL Server версия учебное заведение  «Кадры-предприятие» под СУБД MS SQL Server версия учебное заведение  eDocLib под СУБД MS SQL Server версия учебное заведение |
|  | Система поддержки принятия решений при выдаче потребительских кредитов в коммерческом банке |
|  | Statistica 6 |
|  | Project Expert 7 |
|  | Corel DRAW 10 |
|  | PROMT NET Professional 7/0 ГИгант |
|  | ABBYY FineReader 8.0 Corporate Edition |
|  | Программный комплекс адаптивного компьютерного тестирования "ACT-Тест Plus" версии 4.x.x |
|  | LMS Moodle |
|  | АнтиплагиатВУЗ |
|  | КонсультантПлюс |
| **Свободно распространяемое ПО** | |
|  | Пакет свободно-распространяемого ПО для образовательных учреждений LINUX |
|  | Adobe Reader 10 |
|  | PGP (1GP8.exe) – криптографическая программа |
|  | GPSS World Student Version 4.3.5 |
|  | CLIPS 6.24 |
|  | Visual Prolog 7.1 |
|  | Accembler |
|  | VMWare |
|  | Gretl 1.9.9 |
|  | LISTER 8.8 |
|  | RapidMiner |
|  | Project Euler |
|  | OpenStat |
|  | Maxima |
|  | Google Chrome |
|  | Firefox |
|  | Internet Explorer 8 |
|  | FisPro |
|  | Free Pascal |
|  | Альфа-директ |
|  | BizAgi Process Modeler |
|  | CMS Joomla |
|  | Ramus Educational – моделирование и анализ бизнес-процессов (создания диаграмм в формате IDEF0 и DFD) |
|  | 7-Zip - архиватор |
|  | GIMP – графический редактор |

1. Приведены примеры из ФОС [↑](#footnote-ref-1)