

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное учреждение  
высшего профессионального образования  
"Казанский (Приволжский) федеральный университет"  
Институт вычислительной математики и информационных технологий



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Таюрский Д.А.



\_\_\_\_\_ 20\_\_ г.

*подписано электронно-цифровой подписью*

### Программа дисциплины

Программно-аппаратные методы защиты информации БЗ.ДВ.4

Направление подготовки: 010400.62 - Прикладная математика и информатика

Профиль подготовки: Математическое и программное обеспечение вычислительных машин и сетей

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

**Автор(ы):**

Кугураков В.С.

**Рецензент(ы):**

Ишмухаметов Ш.Т.

**СОГЛАСОВАНО:**

Заведующий(ая) кафедрой: Аблаев Ф. М.

Протокол заседания кафедры No \_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 201\_\_ г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:

Протокол заседания УМК No \_\_\_\_ от " \_\_\_\_ " \_\_\_\_\_ 201\_\_ г

Регистрационный No 976915

Казань

2015

## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Кугураков В.С. кафедра теоретической кибернетики отделение фундаментальной информатики и информационных технологий , Vladimir.Kugurakov@kpfu.ru

### 1. Цели освоения дисциплины

Цель дисциплины – ознакомить студентов с современными средствами защиты информации в компьютерных системах, овладение методами решения профессиональных задач.

### 2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " Б3.ДВ.4 Профессиональный" основной образовательной программы 010400.62 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 4 курсе 8 семестр для студентов, обучающихся по направлению "Прикладная математика и информатика".

### 3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-8 (профессиональные компетенции)	
ПК-7 (профессиональные компетенции)	

В результате освоения дисциплины студент:

#### 1. должен знать:

принципы обеспечения информационной безопасности в условиях информационного общества;

принципы функционирования и обеспечения защиты программно-аппаратных средств информационной безопасности.

#### 2. должен уметь:

создавать необходимые условия использования программно-аппаратных средств для обеспечения информационной безопасности современных информационных технологий;

#### 3. должен владеть:

навыками работы со средствами защиты информации (на основе учебных имитационных программ);создавать и эксплуатировать автоматизированные системы, используя программно-аппаратные;

#### 4. должен демонстрировать способность и готовность:

применять в различных проектах программно-аппаратные средства обеспечения информационной безопасности.

### 4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 8 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

#### **4.1 Структура и содержание аудиторной работы по дисциплине/ модулю** **Тематический план дисциплины/модуля**

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение в проблематику программно-аппаратных средств защиты информации Информация, информатизация и информационная безопасность. Определение назначения программно-аппаратных средств защиты информации для информационной технологии коммерческой организации. Терминология. Основные понятия информатики применительно к программно-аппаратным средствам защиты информации, термины и положения теории информационных систем. Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Информационные риски и статистика угроз для информации.	8	1-3	0	0	12	научный доклад дискуссия

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Пакет программ Криптон	8	4-7	0	0	14	научный доклад дискуссия
3.	Тема 3. Сертифицированное программное средство СКЗИ ?ВЕРБА?/ ?ВЕРБА-О?.	8	8-10	0	0	14	домашнее задание отчет
	Тема . Итоговая форма контроля	8		0	0	0	зачет
	Итого			0	0	40	

#### 4.2 Содержание дисциплины

**Тема 1. Введение в проблематику программно-аппаратных средств защиты информации**  
**Информация, информатизация и информационная безопасность. Определение назначения программно-аппаратных средств защиты информации для информационной технологии коммерческой организации. Терминология. Основные понятия информатики применительно к программно-аппаратным средствам защиты информации, термины и положения теории информационных систем. Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Информационные риски и статистика угроз для информации.**

##### **лабораторная работа (12 часа(ов)):**

Введение в проблематику программно-аппаратных средств защиты информации  
 Информация, информатизация и информационная безопасность. Определение назначения программно-аппаратных средств защиты информации для информационной технологии коммерческой организации. Терминология. Основные понятия информатики применительно к программно-аппаратным средствам защиты информации, термины и положения теории информационных систем. Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной

##### **Тема 2. Пакет программ Криптон**

##### **лабораторная работа (14 часа(ов)):**

Лабораторные работы по изучению Пакета программ Криптон.

##### **Тема 3. Сертифицированное программное средство СКЗИ ?ВЕРБА?/ ?ВЕРБА-О?.**

##### **лабораторная работа (14 часа(ов)):**

Лабораторные работы по изучению Сертифицированного программного средства СКЗИ ?ВЕРБА/ ?ВЕРБА

#### 4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	<p>Тема 1. Введение в проблематику программно-аппаратных средств защиты информации. Информация, информатизация и информационная безопасность. Определение назначения программно-аппаратных средств защиты информации для информационной технологии коммерческой организации. Терминология. Основные понятия информатики применительно к программно-аппаратным средствам защиты информации, термины и положения теории информационных систем. Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Информационные риски и статистика угроз для информации.</p>	8	1-3	подготовка к дискуссии	4	дискуссия
				подготовка к научному докладу	6	научный доклад
2.	Тема 2. Пакет программ Криптон	8	4-7	подготовка к дискуссии	4	дискуссия
				подготовка к научному докладу	8	научный доклад

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
3.	Тема 3. Сертифицированное программное средство СКЗИ ?ВЕРБА?/ ?ВЕРБА-О?.	8	8-10	подготовка домашнего задания	6	домашнее задание
				подготовка к отчету	4	отчет
	Итого				32	

## 5. Образовательные технологии, включая интерактивные формы обучения

технологии Обучение происходит в форме лабораторных занятий, а также самостоятельной работы студентов.

## 6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

**Тема 1. Введение в проблематику программно-аппаратных средств защиты информации**  
**Информация, информатизация и информационная безопасность. Определение назначения программно-аппаратных средств защиты информации для информационной технологии коммерческой организации. Терминология. Основные понятия информатики применительно к программно-аппаратным средствам защиты информации, термины и положения теории информационных систем. Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Информационные риски и статистика угроз для информации.**

дискуссия , примерные вопросы:

Введение в проблематику программно-аппаратных средств защиты информации  
Информация, информатизация и информационная безопасность. Определение назначения программно-аппаратных средств защиты информации для информационной технологии коммерческой организации. Терминология. Основные понятия информатики применительно к программно-аппаратным средствам защиты информации, термины и положения теории информационных систем. Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Информационные риски и статистика угроз для информации.

научный доклад , примерные вопросы:

Определение назначения программно-аппаратных средств защиты информации для информационной технологии коммерческой организации. Терминология. Основные понятия информатики применительно к программно-аппаратным средствам защиты информации, термины и положения теории информационных систем. Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий. Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Информационные риски и статистика угроз для информации.

### Тема 2. Пакет программ Криптон

дискуссия , примерные вопросы:

Концептуальные подходы к защите информации в компьютерных системах и сетях. Пакет программ Криптон



научный доклад , примерные вопросы:

Отечественные программно-аппаратные средства криптографической защиты компьютерной информации серии КРИПТОН/Cripton. Системы защиты информации от несанкционированного доступа. Абонентское шифрование (АШ) и электронная цифровая подпись (ЭЦП). Пакет программ АШ и ЭЦП для MS DOS. Пакет программ АШ и ЭЦП для Windows 95/98/NT.

### **Тема 3. Сертифицированное программное средство СКЗИ ?ВЕРБА?/ ?ВЕРБА-О?.**

домашнее задание , примерные вопросы:

Сертифицированное программное средство СКЗИ ?ВЕРБА/ ?ВЕРБА-О.

отчет , примерные вопросы:

Изучение Сертифицированных программных средств СКЗИ ВЕРБА/ ВЕРБА-О.

### **Тема . Итоговая форма контроля**

Примерные вопросы к зачету:

По данной дисциплине предусмотрено проведение зачета.

Вопросы к зачету:

1. Основная задача защиты информации.
2. Атаки.
3. Угрозы.
4. Аутентификация.
5. Вредоносное программное обеспечение.
6. Виды вредоносного программного обеспечения.
7. Антивирусные техники.
8. Модель безопасности Харрисона-Руззо-Ульмана.
9. Матрица доступов (модель ХРУ).
10. Прimitивные операторы (модель ХРУ).
11. Команды (модель ХРУ).
12. Утечка права (модель ХРУ).
13. Модель распространения прав доступа Take-Grant.
14. Граф доступов в модели Take-Grant.
15. Де-юре правила (правила преобразования графа доступов) в модели Take-Grant.
16. Предикат "возможен доступ" (модель Take-Grant).
17. Предикат "возможно похищение" (модель Take-Grant).
18. Остров, мост, начальный пролет моста, конечный пролет моста (модель Take-Grant).
19. Вирусное множество (абстрактная теория компьютерных вирусов).
20. Теорема об определении утечки права для монооперациональных систем защиты информации.
21. Теорема об определении утечки права для произвольной системы защиты информации.
22. Необходимое и достаточное условие истинности предиката "возможен доступ" в случае, когда граф доступов состоит только из субъектов (модель Take-Grant).
23. Необходимое и достаточное условие истинности предиката "возможен доступ" (модель Take-Grant).
24. Необходимое и достаточное условие истинности предиката "возможно похищение".
25. Теорема о невозможности создания универсального антивируса.

Типовой билет:

1. Формулировка теоремы о необходимом и достаточном условии истинности предиката "возможно похищение".
2. Предикат "возможен доступ" (модель Take-Grant).

### **7.1. Основная литература:**

1. Расторгуев, С. П. Основы информационной безопасности: учебное пособие / С.П. Расторгуев. - Москва: Академия, 2007. - 186 с.
2. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие, 2012. - URL: <http://kpfu.ru/docs/F366166681/mzi.pdf>
3. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: <http://www.znanium.com/bookread.php?book=420047>
4. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. URL: <http://www.znanium.com/bookread.php?book=405000>
5. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: <http://znanium.com/bookread.php?book=335362>

### **7.2. Дополнительная литература:**

1. М.Р. Биктимиров, А.Ю. Щербаков. Избранные главы компьютерной безопасности. - Казань: Изд - во КМО, 2004. - 371 с.
2. Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. <http://znanium.com/catalog.php?bookinfo=441493>

### **7.3. Интернет-ресурсы:**

Википедия - <http://ru.wikipedia.org>  
Интернет журнал по ИТ - <http://www.rsdn.ru>  
Интернет портал математических ресурсов - <http://www.math.ru/>  
Интернет портал образовательных ресурсов - <http://algolist.manual.ru/>  
Интернет портал образовательных ресурсов по ИТ - <http://www.intuit.ru>

### **8. Материально-техническое обеспечение дисциплины(модуля)**

Освоение дисциплины "Программно-аппаратные методы защиты информации" предполагает использование следующего материально-технического обеспечения:

занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером), а так же в специализированных компьютерных кабинетах.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010400.62 "Прикладная математика и информатика" и профилю подготовки Математическое и программное обеспечение вычислительных машин и сетей .

Автор(ы):

Кугураков В.С. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.

Рецензент(ы):

Ишмухаметов Ш.Т. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.