Учреждение образования

«Белорусский государственный университет

информатики и радиоэлектроники»

УТВЕРЖДАЮ

Проректор по учебной работе

и менеджменту качества

\_\_\_\_\_\_\_\_\_\_\_\_ Е.Н.Живицкая

"\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Регистрационный № УД /р

### «КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ»

Учебная программа учреждения высшего образования по учебной дисциплине

#### для специальности

#### 1-58 01 01 Инженерно-психологическое обеспечение информационных технологий

Кафедра инженерной психологии и эргономики

|  |  |
| --- | --- |
| Всего часов по |  |
| дисциплине 108 |  |
| Зачетных единиц 3 |  |

2016 г.

Учебная программа учреждения высшего образования составлена на основе образовательного стандарта ОСВО 1-58 01 01-2013 и учебных планов специальности   
1-58 01 01 «Инженерно-психологическое обеспечение информационных технологий».

Составители:

Д.И.Черемисинов, доцент кафедры инженерной психологии и эргономики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент;

М.М.Меженная, доцент кафедры инженерной психологии и эргономики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук;

К.Д.Яшин, заведующий кафедрой инженерной психологии и эргономики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», кандидат технических наук, доцент.

Рецензенты:

Кафедра «Интеллектуальные системы» учреждения образования «Белорусский национальный технический университет» (протокол № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_);

Л.М. Лыньков, заведующий кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор

Рассмотрена и рекомендована к утверждению:

Кафедрой инженерной психологии и эргономики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 10 от 8.02.2016);

Научно-методическим советомучреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_)

СОГЛАСОВАНО

Эксперт-нормоконтролер

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

**План учебной дисциплины в дневной форме обучения:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код  специальности  (направления специальности) | Название специальности (направления  специальности) | Курс | Семестр | Аудиторных часов  (в соответствии  с учебным планом уво) | | | | Академ. часов на курс. работу (проект) | Типовой расчет | Форма текущей аттестации |
| Всего | Лекции | Лабораторные  занятия | Практические занятия ,семинары |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 4 | 7 | 64 | 32 | - | 32 | - | - | Зачет |

**План учебной дисциплины в заочной форме обучения:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код  специальности  (направления специальности) | Название специальности  (направления  специальности) | Курс | Семестр | Аудиторных часов  (в соответствии  с учебным планом уво) | | | | Академ. часов на курс. работу (проект) | Контрольные работы | Форма текущей аттестации |
| Всего | Лекции | Лабораторные  занятия | Практические занятия ,семинары |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 4 | 7 | 16 | 8 | - | 8 | - | 1 | Зачет |

**План учебной дисциплины в дистанционной форме обучения:**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код  специальности  (направления специальности) | Название специальности  (направления  специальности) | Курс | Семестр | Всего | Количество работ | | | Академ. часов на курс. работа (проект) | Форма текущей аттестации |
| Контрольные работы | Лабораторные  занятия | Индивидуальная практическая работа |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 4 | 7 | 108 | 1 | - | 2 | - | Зачет |

**План учебной дисциплины в вечерней форме обучения**

**для получения высшего образования,**

**интегрированного со средним специальным образованием:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код  специальности  (направления специальности) | Название специальности  (направления  специальности) | Курс | Семестр | Аудиторных часов  (в соответствии  с учебным планом уво) | | | | Академ. часов  на курс. работу (проект) | Типовой расчет | Форма  текущей  аттестации |
| Всего | Лекции | Лабораторные  занятия | Практические занятия, семинары |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 3 | 6 | 40 | 24 | - | 16 | - | - | Зачет |

**План учебной дисциплины в заочной форме обучения**

**для получения высшего образования,**

**интегрированного со средним специальным образованием:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Код  специальности  (направления специальности) | Название специальности  (направления  специальности) | Курс | Семестр | Аудиторных часов  (в соответствии  с учебным планом уво) | | | | Контрольные работы | Академ. часов  на курс. работу (проект) | Форма  текущей  аттестации |
| Всего | Лекции | Лабораторные  занятия | Практические занятия,  семинары |
| 1-58 01 01 | Инженерно-психологическое обеспечение информационных технологий | 3 | 5 | 16 | 8 | - | 8 | 1 | - | Зачет |

**Место учебной дисциплины.**

Дисциплина «Криптографические технологии» формирует знания, умения и навыки специалиста в области анализа и синтеза криптографических протоколов, соответствующих государственным и международным стандартам.

**Цель преподавания учебной дисциплины:** изучение базовых принципов, овладение современными методами использования криптографических протоколов для защиты информации, оценки уязвимости применяемых криптографических протоколов.

**Задачи изучения учебной дисциплины:**

* изучение средств и методов хранения и передачи аутентификационной информации;
* изучение основных протоколов идентификации и аутентификации;
* изучение основных видов симметричных и асимметричных криптографических алгоритмов;
* изучение математических моделей шифров;
* изучение криптографических стандартов;
* изучение алгоритмов проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах.

В результате изучения учебной дисциплины формируются следующие компетенции:

**академические:**

1. умение применять базовые научно-теоретические знания для решения теоретических и практических задач;
2. владение системным и сравнительным анализом;
3. владение исследовательскими навыками;
4. умение работать самостоятельно;
5. владение навыками, связанными с использованием технических устройств, управлением информацией и работой с компьютером;
6. владение навыками устной и письменной коммуникации;
7. умение учиться, повышать свою квалификацию в течение всей жизни.

**социально-личностные:**

1. способность к межличностным коммуникациям;
2. способность к критике и самокритике.

**профессиональные:**

1. умение использовать методы анализа и мониторинга для приведения процессов профессиональной деятельности в соответствие действующим стандартам, инструкциям, правилам и нормам;
2. владение современными методами, языками, технологиями и инструментальными средствами проектирования и разработки программных продуктов;
3. способность устанавливать, испытывать и сопровождать системное и прикладное программное обеспечение;
4. умение использовать современные инновационные педагогические технологии и средства обучения;
5. умение пользоваться глобальными информационными ресурсами;
6. владение современными средствами инфокоммуникаций.

В результате изучения учебной дисциплины обучаемый должен:

***знать:***

* криптографические стандарты;
* типовые криптографические протоколы и основные требования к ним;
* принципы построения криптографических хеш-функций;
* основные схемы цифровой подписи;
* протоколы идентификации;
* протоколы передачи и распределения ключей;
* методы оценки безопасности криптографического протокола.

***уметь:***

* формулировать свойства безопасности криптографических протоколов;
* использовать симметричные и асимметричные шифрсистемы для построения криптографических протоколов;
* проводить сравнительный анализ криптографических протоколов.

***владеть:***

* криптографической терминологией;
* простейшими подходами к анализу безопасности криптографических протоколов.

## Перечень учебных дисциплин, усвоение которых необходимо

**для изучения данной учебной дисциплины.**

|  |  |  |
| --- | --- | --- |
| № п.п. | Название дисциплины | Раздел, темы |
| 1 | «Математика» | Все темы |
| 2 | «Основы защиты информации» | Все темы |

1. **Содержание учебной дисциплины**

|  |  |  |
| --- | --- | --- |
| №  тем | Наименование  разделов, тем | Содержание тем |
| 1 | 2 | 3 |
| 1 | Роль криптографических протоколов в системах защиты информации. | Криптографический протокол. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей.  Классификация криптографических протоколов. Моделирование криптографических протоколов. Уязвимости и атаки на криптографический протокол.  Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Основные подходы к автоматизации анализа протоколов. |
| 2 | Схемы цифровой подписи | Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем. Схемы Эль-Гамаля, Фиата-Фейга-Шамира и Шнорра, их свойства.  Стандарты США, России и Республики Беларусь электронной цифровой подписи.  Одноразовые подписи. Схемы конфиденциальной цифровой подписи и подписи вслепую. Подписи с обнаружением подделки. |
| 3 | Протоколы идентификации | Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования. Протоколы интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото. Связь между протоколами цифровой подписи и протоколами идентификации. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов. |
| 4 | Инфраструктура открытых ключей | Управление открытыми ключами. Организация и компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509.  Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа. |
| 5 | Протоколы распределения ключей | Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем. Двух и трех сторонние протоколы передачи и распределения ключей. Функции доверенной третьей стороны и выполняемые ею роли.  Схемы предварительного распределения ключей. Неравенство Блома. Схемы предварительного распределения ключей Блома и на основе пересечений множеств. Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине». Аутентифицированные протоколы открытого распределения ключей. Групповые протоколы. Протоколы разделения секрета и распределения ключей для телеконференции. |
| 6 | Прикладные протоколы | Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей. Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации. |
| 7 | Протоколы открытых сделок | Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и “игры в покер” по телефону. Забывающая передача информации. Протокол подписания контракта. Протокол сертифицированной электронной почты. Протоколы электронного голосования. Свойства неотслеживаемости и несвязывемости. Протоколы электронных платежей и цифровых денег. |
| 8 | Технологии взлома механизмов защиты. Методы защиты от исследования программ | Взлом механизмов, основанных на ключевом сравнении. Уязвимость криптографических систем защиты. Надежность цифровой подписи. Атака полным перебором. Эмуляция ключевых дисков.  Средства исследования программ. Защита программ от дизассемблирования. Защита программ от работы под контролем отладчика. |

**2. Информационно-методический раздел**

**2.1 Литература**

**2.1.1 Основная**

1. Алферов, А.П. Основы криптографии. Учебное пособие. 3е изд., доп. / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: АРВ Гелиос, 2005. – 450 с.
2. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости. Учебное пособие. / А.В. Черемушкин. – М.: Изд. центр «Академия», 2009. –   
   272 с.
3. Харин, Ю.С. Математические основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Мн: БГУ, 2003.
4. Гашков, С. Б. Криптографические методы защиты информации: учеб. пособие / С.Б. Гашков, Э.А. Применко, М.А. Черепнёв. – М.: Изд. центр «Академия», 2010. – 304 с.

**2.1.2 Дополнительная**

1. Погорелов, Б.А. Словарь криптографических терминов / Б.А. Погорелов, В.Н. Сачков. – М.: МЦНМО, 2006.
2. Введение в криптографию под общ. ред. В.В.Ященко, 3-е изд. - М.: МЦНМО - ЧеРо, 2000.
3. Столлингс, В., Криптография и защита сетей: принципы и практика, 2-е издание / В. Столлингс. – М.: издательский дом “Вильямс”, 2001.
4. Столлингс, В., Основы защиты сетей. Приложения и стандарты / В. Столлингс. – М.: ИД «Вильямс», 2002. – 429 с.
5. Анохин, М.И. Криптография в банковском деле / М.И. Анохин, Н.П. Варновский, В.М. Сидельников, В.В. Ященко. – Московский государственный инженерно-физический институт (технический университет), Москва, 1997.
6. Чмора, А. Современная прикладная криптография / А. Чмора. – М.: Гелиос АРВ, 2001.
7. Саломаа, А. Криптография с открытым ключом / А. Саломаа. – М.: Мир, 1995.
8. Мао, В. Современная криптография: теория и практика / В. Мао. – М.: Вильямс, 2005, 768 с.
9. Stinson, D.R. Cryptography, theory and practice / D.R. Stinson. – London etc., CRC Press, 1995.
10. Menezes, A.J. Handbook of Applied Cryptography / A.J. Menezes, P.C. Oorcshot, S.A. Vanstone. – CRC Press, 1997. – 780 pp.

**2.2 Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения**

1. Компьютер с программным обеспечением Microsoft Office

**2.3. Перечень тем практических занятий, их название**

Основная цель проведения практических занятий состоит в закреплении теоретического материала курса, приобретении навыков выполнения задач по основам криптографических технологий, анализа результатов, грамотного оформления отчетов.

|  |  |  |  |
| --- | --- | --- | --- |
| № темы по п.1 | Название  практического  занятия | Содержание | Обеспеченность  по пункту 2.2 |
| 1 | 2 | 3 | 4 |
| 1 | Криптоанализ классических шифров | Шифры перестановки, шифры замены. Примеры шифрования и дешифрования. | 2.2.1 |
| 2 | Маршрутные и подстановочные шифры | Примеры шифрования и дешифрования, вскрытие ключа. | 2.2.1 |
| 3 | Шифрование, дешифрование информации с применением криптографических алгоритмов гаммирования | Примеры шифрования и дешифрования. | 2.2.1 |
| 4 | Исследование ассиметричных алгоритмов шифрования | Создание ключей в системе PGP, передача подписанных и защищенных сообщений. | 2.2.1 |
| 5 | Исследование методов идентификация и аутентификация пользователя. Протоколы «рукопожатия» и идентификации типа «запрос-ответ». | Парольная идентификация и аутентификация, разграничение доступа к ресурсам. | 2.2.1 |
| 6 | Цифровые подписи DSA и ГОСТ. | Конфигурирование почтового клиента. | 2.2.1 |
| 8 | Сертификаты инфрастуктуры открытых ключей и их структура. Функции удостоверяющего центра. | Установка цифрового сертификата для почтового клиента. | 2.2.1 |
| 8 | Примеры прикладных протоколов (протоколы заключения сделок, платежных систем, сертифицированная электронная почта, голосования и др.). | Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. | 2.2.1 |

**2.4 Контрольная работа, ее характеристика**

Основная цель выполнения контрольной работы состоит в закреплении теоретического материала курса, приобретении практических навыков решения задач по основам криптографических технологий, анализа результатов, грамотного оформления отчетов.

| № темы по п.1 | Наименование  контрольной работы | Содержание | Обеспеченность  по пункту 2.2 |
| --- | --- | --- | --- |
| 3 | Исследование методов идентификация и аутентификация пользователя | Авторизация, аутентификация, атаки на систему аутентификации, механизмы подтверждения подлинности пользователя | 2.2.1 |

**2.5 Индивидуальная практическая работа**

| № темы по п.1 | Наименование  индивидуальной практической работы | Содержание | Обеспеченность  по пункту 2.2 |
| --- | --- | --- | --- |
| 1 | Изучение криптосистемы [PGP](http://www.pgpru.com/soft/#pgp) | Использование системы PGP для защищенного хранения файлов. | 2.2.1 |
| 2 | Цифровые подписи | Назначение, правовой статус, стандарты и алгоритмы построения электронно-цифровой подписи. | 2.2.1 |

**3. 1 Учебно-методическая карта учебной дисциплины в дневной форме обучения**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Номер раздела, темы по п.1 | Название раздела, темы | Количество аудиторных часов | | | Самостоятельная работа, часы | Форма контроля знаний студентов |
| ЛК | ПЗ | Лаб. зан. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Роль криптографических протоколов в системах защиты информации. | 4 | 4 |  | 6 | Отчет по практической работе |
| 2 | Схемы цифровой подписи | 4 | 4 |  | 6 | Отчет по практической работе |
| 3 | Протоколы идентификации | 4 | 4 |  | 6 | Отчет по практической работе |
| 4 | Инфраструктура открытых ключей | 4 | 4 |  | 6 | Отчет по практической работе |
| 5 | Протоколы распределения ключей | 4 | 4 |  | 6 | Отчет по практической работе |
| 6 | Прикладные протоколы | 4 | 4 |  | 6 | Отчет по практической работе |
| 7 | Протоколы открытых сделок | 4 |  |  | 2 | Устный опрос |
| 8 | Технологии взлома механизмов защиты. Методы защиты от исследования программ | 4 | 8 |  | 6 | Отчет по практической работе |
|  | Текущая аттестация |  |  |  |  | Зачет |
|  | Итого | 32 | 32 |  | 44 |  |

**3. 2 Учебно-методическая карта учебной дисциплины в заочной форме обучения,**

**в том числе в заочной форме обучения для получения высшего образования,**

**интегрированного со средним специальным образованием**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Номер раздела, темы по п.1 | Название раздела, темы | Количество аудиторных часов | | | Само-стоя-тельная работа, часы | Форма контроля знаний студентов |
| ЛК | ПЗ | Лаб. зан. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Роль криптографических протоколов в системах защиты информации. | 1 |  |  | 11 | Устный опрос |
| 2 | Схемы цифровой подписи | 1 | 2 |  | 12 | Устный опрос |
| 3 | Протоколы идентификации | 1 | 2 |  | 12 | Защита  контрольной  работы |
| 4 | Инфраструктура открытых ключей | 1 |  |  | 11 | Устный опрос |
| 5 | Протоколы распределения ключей | 1 |  |  | 11 | Устный опрос |
| 6 | Прикладные протоколы | 1 | 2 |  | 12 | Устный опрос |
| 7 | Протоколы открытых сделок | 1 |  |  | 11 | Устный опрос |
| 8 | Технологии взлома механизмов защиты. Методы защиты от исследования программ | 1 | 2 |  | 12 | Устный опрос |
|  | Текущая аттестация |  |  |  |  | Зачет |
|  | Итого | 8 | 8 |  | 92 |  |

**3.3 Учебно-методическая карта учебной дисциплины**

**в дистанционной форме обучения**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Номер раздела, темы по п.1 | Название раздела, темы | Количество работ | | | Само-стоя-тельная работа, часы | Форма контроля знаний студентов |
| КР | ИПР | Лаб. зан. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Роль криптографических протоколов в системах защиты информации. |  | ИПР1 |  | 13 | Контроль  выполнения  индивидуального  задания |
| 2 | Схемы цифровой подписи |  | ИПР2 |  | 14 | Контроль  выполнения  индивидуального  задания |
| 3 | Протоколы идентификации | КР |  |  | 14 | Защита  контрольной  работы |
| 4 | Инфраструктура открытых ключей |  |  |  | 13 |  |
| 5 | Протоколы распределения ключей |  |  |  | 13 |  |
| 6 | Прикладные протоколы |  |  |  | 14 |  |
| 7 | Протоколы открытых сделок |  |  |  | 13 |  |
| 8 | Технологии взлома механизмов защиты. Методы защиты от исследования программ |  |  |  | 14 |  |
|  | Текущая аттестация |  |  |  |  | Зачет |
|  | Итого | 1 | 2 |  | 108 |  |

**3.4 Учебно-методическая карта учебной дисциплины в вечерней форме обучения для получения высшего образования, интегрированного со средним специальным образованием**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Номер раздела, темы по п.1 | Название раздела, темы | Количество аудиторных часов | | | Само-стоя-тельная работа, часы | Форма контроля знаний студентов |
| ЛК | ПЗ | Лаб. зан. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Роль криптографических протоколов в системах защиты информации. | 2 |  |  | 8 | Устный опрос |
| 2 | Схемы цифровой подписи | 4 | 4 |  | 9 | Отчет по  практической работе |
| 3 | Протоколы идентификации | 4 | 4 |  | 9 | Отчет по  практической работе |
| 4 | Инфраструктура открытых ключей | 2 | 2 |  | 9 | Отчет по  практической работе |
| 5 | Протоколы распределения ключей | 2 | 2 |  | 8 | Отчет по  практической работе |
| 6 | Прикладные протоколы | 4 |  |  | 8 | Устный опрос |
| 7 | Протоколы открытых сделок | 2 |  |  | 8 | Устный опрос |
| 8 | Технологии взлома механизмов защиты. Методы защиты от исследования программ | 4 | 4 |  | 9 | Отчет по  практической работе |
|  | Текущая аттестация |  |  |  |  | Зачет |
|  | Итого | 24 | 16 |  | 68 |  |

УТВЕРЖДАЮ

Проректор по учебной работе

и информатизации

\_\_\_\_\_\_\_\_\_\_\_\_\_Б.В. Никульшин

Учебно-методическая карта изучения учебной дисциплины с использованием

дистанционных образовательных технологий

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Номер раздела, темы по п.1 | Название раздела, темы | Количество работ | | | Само-стоя-тельная работа, часы | Форма контроля знаний студентов |
| КР | ИПР | Лаб. зан. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Роль криптографических протоколов в системах защиты информации. |  | ИПР1 |  | 13 | Контроль  выполнения  индивидуального  задания |
| 2 | Схемы цифровой подписи |  | ИПР2 |  | 14 | Контроль  выполнения  индивидуального  задания |
| 3 | Протоколы идентификации | КР |  |  | 14 | Защита  контрольной  работы |
| 4 | Инфраструктура открытых ключей |  |  |  | 13 |  |
| 5 | Протоколы распределения ключей |  |  |  | 13 |  |
| 6 | Прикладные протоколы |  |  |  | 14 |  |
| 7 | Протоколы открытых сделок |  |  |  | 13 |  |
| 8 | Технологии взлома механизмов защиты. Методы защиты от исследования программ |  |  |  | 14 |  |
|  | Текущая аттестация |  |  |  |  | Зачет |
|  | Итого | 1 | 2 |  | 108 |  |

Рассмотрена и рекомендована к утверждению на заседании кафедры инженерной психологии и эргономики, протокол № 10 от 8.02.2016г.

Заведующий кафедрой

инженерной психологии и эргономики К.Д.Яшин

**4. Рейтинг-план**

|  |  |
| --- | --- |
| Рейтинг-план дисциплины КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ  для студентов дневной формы обучения  Специальность:  1-58 01 01 Инженерно-психологическое обеспечение информационных технологий  курс 4, семестр 7  Количество часов по учебному плану 108, в т.ч. аудиторная работа 64, самостоятельная работа 44.  Преподаватель Черемисинов Дмитрий Иванович, к.т.н., кафедра ИПиЭ | Рекомендовано на заседании кафедры ИПиЭ  Протокол № 10 от 8.02.2016  Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_/ К.Д.Яшин /  Преподаватель \_\_\_\_\_\_\_\_\_\_\_\_/Д.И.Черемисинов/ |

Выставление отметки по текущей аттестации допускается по результатам итогового рейтинга студента.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Виды учебной деятельности студентов | Модуль 1  (весовой коэффициент  вк1 = 0,4) | | Модуль 2  (весовой коэффициент  вк2 = 0,3) | | Модуль 3  (весовой коэффициент  вк3 =0,3) | | Итоговый  контроль  по всем  модулям |
| Календар­ные сроки сдачи | Весовой коэффици­ент отметки | Календар­ные сроки сдачи | Весовой коэффици­ент отметки | Календар­ные сроки сдачи | Весовой коэффици­ент отметки |  |
| 1. Практические занятия |  | К11=1 |  | К12=1 |  | К13=1 |  |
| 1-3 | 15 октября |  |  |  |  |  |  |
| 4-6 |  |  | 15 ноября |  |  |  |  |
| 7-8 |  |  |  |  | 15 декабря |  |  |
| Модульный контроль |  | МР1 |  | МР2 |  | МР3 | ИР |

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

|  |  |  |  |
| --- | --- | --- | --- |
| Код и наименование специальности  (направления  специальности) | Выпускающая кафедра | Предложения  об изменениях  в содержании  по изучаемой  учебной дисциплине | Подпись заведующего выпускающей кафедрой  с указанием номера  протокола и  даты заседания кафедры |
| 1 | 2 | 3 | 4 |
| 1-58 01 01 Инженерно-психологическое обеспечение информационных технологий | Кафедра  инженерной  психологии и  эргономики | - | Протокол № 10  от 8.02.2016г.  Зав. кафедрой ИПиЭ  \_\_\_\_\_\_\_\_\_\_\_\_/К.Д.Яшин/ |

Заведующий кафедрой

инженерной психологии и эргономики К.Д.Яшин