Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет»

**Зязин А.В.**

# КОНЦЕПЦИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ И СИСТЕМ»

# ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

**Цель обучения** – формирование компетенций, необходимых для выполнения нового вида профессиональной деятельности в области информационной безопасности

**Требования к квалификации поступающих на обучение** – высшее образование физико-математического, информационно-технологического профиля, либо в области ИБ

**Продолжительность обучения** – 526 часов, 30 недель

**Форма обучения** – очно-заочная

**Документ, выдаваемый слушателям после освоения программы профессиональной переподготовки** – диплом о профессиональной переподготовке образца РТУ МИРЭА, предоставляющий право на ведение нового вида профессиональной деятельности в области информационной безопасности

# ПРИОБРЕТАЕМЫЕ ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ

| **Профессиональные компетенции** | | **Трудовые функции (обобщенные трудовые функции), квалификационные характеристики** |
|---|---|---|
| Код | Наименование | Шифр и наименование |
| ПК –1 | Способность ориентироваться в современных и перспективных математических методах защиты информации, оценивать возможность и эффективность их применения в конкретных задачах защиты информации | C/03.7<br>Проведение анализа безопасности компьютерных систем |
| ПК –2 | Способность разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации | D/03.8<br>Разработка и тестирование средств защиты информации компьютерных систем и сетей |
| ПК –3 | Способность проводить сравнительный анализ и осуществлять обоснованный выбор программно- аппаратных средств защиты информации с учетом современных и перспективных методов защиты информации | B/03.6<br>Администрирование средств защиты информации прикладного и системного программного обеспечения |

# СМЫСЛОВОЕ ЯДРО ЗАНЯТИЙ

**ЛЕКЦИИ: Изучение документов национальной, межгосударственной системы стандартизации в области криптографической защиты информации (стандарты БШ, ХФ, ЭП, рекомендации ТК26). Порядок проведения тематических исследований СКЗИ, устранение типовых ошибок программных реализаций.**

**ПРАКТИЧЕСКИЕ ЗАНЯТИЯ: использование API-интерфейса зарубежных и российских производителей при реализации рекомендованных или стандартизованных в РФ криптографических функций и протоколов**

**ЛАБОРАТОРНЫЕ РАБОТЫ: изучение криптографических протоколов (S/MIME, TLS, IPsec) и построение сред доверия с использованием средств ИОК российских производителей**

**ИТОГОВАЯ АТТЕСТАЦИОННАЯ РАБОТА (СКВОЗНОЙ ПРОЕКТ): реализация функционала СКЗИ для защищенного доступа к корпоративному порталу в построенной среде доверия на основе ИОК, включая подготовку правил пользования и материалов тематических исследований**

# КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК ПРОГРАММЫ

| | недели обучения | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| **Модуль 1** | **Защита информации криптографическими методами** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Лекции | 8 | 4 | 4 | 4 | | | | | | | | | | | | | | | | | | | | | | | | | |
| Практика | 6 | 10 | 10 | 10 | | | | | | | | | | | | | | | | | | | | | | | | | |
| Сам.работа | 4 | 4 | 4 | 4 | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Модуль 2** | **Криптографические алгоритмы** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Лекции | | | | | 8 | 4 | 4 | 4 | 0 | 0 | 4 | 4 | | | | | | | | | | | | | | | | | |
| Практика | | | | | 6 | 10 | 10 | 10 | 0 | 0 | 10 | 10 | | | | | | | | | | | | | | | | | |
| Сам.работа | | | | | 4 | 4 | 4 | 4 | 18 | 18 | 4 | 4 | | | | | | | | | | | | | | | | | |
| **Модуль 3** | **Криптографические протоколы** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Лекции | | | | | | | | | | | | | 8 | 4 | 4 | 4 | 0 | 0 | 4 | 4 | | | | | | | | | |
| Практика | | | | | | | | | | | | | 6 | 10 | 10 | 10 | 0 | 0 | 10 | 10 | | | | | | | | | |
| Сам.работа | | | | | | | | | | | | | 4 | 4 | 4 | 4 | 18 | 18 | 4 | 4 | | | | | | | | | |
| **Модуль 4** | **Средства криптографической защиты информации** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Лекции | | | | | | | | | | | | | | | | | | | | | 8 | 4 | 4 | 4 | 0 | 0 | 4 | 4 | |
| Практика | | | | | | | | | | | | | | | | | | | | | 6 | 10 | 10 | 10 | 0 | 0 | 10 | 10 | |
| Сам.работа | | | | | | | | | | | | | | | | | | | | | 4 | 4 | 4 | 4 | 18 | 18 | 4 | 4 | |
| **Итоговая аттестация** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | 18 | 4 |
| **Итого** | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 18 | 4 |

# МОДУЛИ ПРОГРАММЫ

| № | Наименование дисциплин (модулей) | Всего, час. | в том числе (час.) | | | Форма промежу – точной аттестации, час. |
|---|---|---|---|---|---|---|
| | | | Лекции | Практические занятия, в том числе лабораторные работы | Самостоятельная работа обучающихся | |
| **Модуль 1. Защита информации криптографическими методами** | | | | | | |
| **1** | **Защита информации криптографическими методами** | 72 | 20 | 34 | 16 | зачет, 2 |
| **Модуль 2. Криптографические алгоритмы** | | | | | | |
| **2** | **Криптографические алгоритмы** | 144 | 28 | 54 | 60 | зачет, 2 |
| **Модуль 3. Криптографические протоколы** | | | | | | |
| **3** | **Криптографические протоколы** | 144 | 28 | 54 | 60 | зачет, 2 |
| **Модуль 4. Средства криптографической защиты информации** | | | | | | |
| **4** | **Средства криптографической защиты информации** | 144 | 28 | 54 | 60 | зачет, 2 |
| | **Итоговая аттестация** | 4 | - | - | 18 | защита ИАР*, 4 |
| | **ИТОГО** | **526** | **104** | **196** | **214** | **12** |

***ИАР – итоговая аттестационная работа**

# КРАТКОЕ СОДЕРЖАНИЕ МОДУЛЕЙ

**Модуль 1. Защита информации криптографическими методами**

1.Регулирование вопросов защиты информации криптографическими методами
2.Математические структуры криптоалгоритмов
**Часть I ИАР: «Реализация механизмов выработки псевдослучайных последовательностей и их тестирование»**

**Модуль 2. Криптографические алгоритмы**

1.Российские стандарты блочного шифрования и сопутствующие криптомеханизмы
2.Российский стандарт функции хэширования и сопутствующие криптомеханизмы
3.Особенности программных реализаций алгоритмов и типовые ошибки
**Часть II ИАР: «Реализация российских криптографических алгоритмов и механизмов»**

**Модуль 3. Криптографические протоколы**

1.Протоколы электронной подписи и сопутствующие криптомеханизмы
2.Криптопротокол TLS
3.Криптопротокол IPsec
**Часть III ИАР: «Реализация TLS-взаимодействия на основе реализованных российских криптографических алгоритмов»**

**Модуль 4. Средства криптографической защиты информации**

1.Средства криптографической защиты информации (СКЗИ) для построения среды доверия
2.Использование СКЗИ российских производителей для построения единой среды доверия
3.Принципы разработки СКЗИ в соответствии с законодательством Российской Федерации
**Часть IV ИАР: «Реализация функционала СКЗИ в области ИОК для решения задачи защищенного доступа к корпоративному порталу в построенной среде доверия»**

# НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ И РЕКОМЕНДАЦИИ ТК 26 (МОДУЛЬ 1,2)

| | | |
|---|---|---|
| **Модуль 1. Защита информации криптографическими методами** | | |
| 1. | **63-ФЗ (2011)** | Об электронной подписи |
| | **152-ФЗ (2020)** | О персональных данных |
| | **Р 1323565.1.006-2017** | Механизмы выработки псевдослучайных последовательностей |
| | **ТС 26.4.001-2019** | Физические генераторы случайных чисел для применения в СКЗИ, не содержащих сведения, составляющие ГТ |
| 2. | **МР 26.2.003-2013** | Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89 *(для примера)* |
| | **Р 1323565.1.024-2019** *RFC7836-2016* | Параметры эллиптических кривых для криптографических алгоритмов и протоколов *(в канонической форме Вейерштрасса, в форме скрученных кривых Эдвардса)* |
| **Модуль 2. Криптографические алгоритмы** | | |
| 1. | **ГОСТ Р 34.12-2015** **ГОСТ 34.12-2018** | Блочные шифры *(“Магма”, “Кузнечик”)* |
| | **ГОСТ Р 34.13-2015** **ГОСТ 34.13-2018** | Режимы работы блочных шифров |
| | **Р 1323565.1.017-2018** | Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования *(режимы с функцией ACPKM, функции экспорта/импорта ключей)* |
| | **Р 1323565.1.005-2017** | Допустимые объёмы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015 |
| | **Р 1323565.1.026-2019** | Режимы работы блочных шифров, реализующих аутентифицированное шифрование *(режим MGM)* |
| 2. | **ГОСТ Р 34.11-2012** **ГОСТ 34.11-2018** | Функция хэширования *(“Стрибог”)* |
| | **Р 50.1.113-2016** *RFC7836-2016* | Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования *(HMAC, PRF_TLS, PRF_IPsec, KDF_TREE, KDF_GOST)* |
| | **Р 1323565.1.022-2018** | Функции выработки производного ключа |
| | **Р 50.1.111-2016** | Парольная защита ключевой информации |
| 3. | - | - |

# НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ И РЕКОМЕНДАЦИИ ТК 26 (МОДУЛЬ 3)

| Модуль 3. Криптографические протоколы | | |
|---|---|---|
| 1. | **ГОСТ Р 34.10-2012**<br>**ГОСТ 34.10-2018** | Процессы формирования и проверки электронной цифровой подписи |
| | **Р 1323565.1.025-2019** | Форматы сообщений, защищенных криптографическими методами *(CMS-форматы)* |
| | **МР 26.2.002-2019** | Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML |
| | **Р 50.1.115-2016** | Протокол выработки общего ключа с аутентификацией на основе пароля |
| | **Р 50.1.113-2016**<br>*RFC7836-2016* | Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования *(протокол VKO_GOST)* |
| | **Р 1323565.1.004-2017** | Схемы выработки общего ключа с аутентификацией на основе открытого ключа *(протоколы “Эхинацея”, “Лимонник”)* |
| | **Р 50.1.112-2016** | Транспортный ключевой контейнер |
| 2. | **МР 26.2.001-2013** | Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS) |
| | **Р 1323565.1.020-2018** | Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2) |
| | **Р 1323565.1.030-2020** | Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3) |
| 3. | **ТС 26.2.002-2013** | Использование ГОСТ Р 34.11-94 при обеспечении целостности в протоколах IPSEC и ESP |
| | **ТС 26.2.002-2014** | Использование ГОСТ 28147-89 при шифровании вложений в протоколах IPSEC ESP |
| | **ТС 26.2.001-2015** | Использование ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 в протоколах обмена ключами IKE и ISAKMP |
| | проект | *Использование российских криптографических алгоритмов в протоколе защиты информации ESP* |
| | проект | *Использование российских криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 (IKEv2)* |

# НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ И РЕКОМЕНДАЦИИ ТК 26 (МОДУЛЬ 4)

## Модуль 4. Средства криптографической защиты информации

| | | |
|---|---|---|
| 1. | **Приказ №795 (2011)** | Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи |
| | **Р 1323565.1.023-2018** | Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509 |
| | **МР 26.2.007-2017**<br><br>**Р 50.1.110-2016** | Расширение PKCS#11 для использования российских стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012<br><br>Контейнер хранения ключей |
| | проект | *Инфраструктура открытых ключей X.509 Интернет. Протокол проверки статуса сертификата в режиме реального времени (OCSP)* |
| | проект | *Использование алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 при взаимодействии со службой штампов времени (TSP)* |
| 2. | **-** | Документация по установке, правила пользования, регламенты работы УЦ СКЗИ российских производителей |
| 3. | **Положение ПКЗ-2005** | Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации |
| | **Р 1323565.1.012-2017** | Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации |
| | **Приказ №796 (2011)** | Об утверждении требований к средствам электронной подписи и Требований к средствам удостоверяющего центра |

# СПАСИБО ЗА ВНИМАНИЕ