ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Петербургский государственный университет путей сообщения

Императора Александра I»

(ФГБОУ ВО ПГУПС)

Кафедра «Информатика и информационная безопасность»

**РАБОЧАЯ ПРОГРАММА**

*дисциплины*

«КРИПТОГРАФИЯ» (Б1.В.ОД.19)

для направления

38.03.05 «Бизнес-информатика»

по профилю

«Архитектура предприятия»

Форма обучения – очная

Санкт-Петербург

2018

**1. Цели и задачи дисциплины**

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «11» августа 2016г., приказ № 1002 по направлению

38.03.05 «Бизнес-информатика» по дисциплине «КРИПТОГРАФИЯ».

Целью изучения дисциплины является формирование у обучающихся компетенций в соответствии с учебным планом за счет освоения теоретических основ криптографической защиты информации в автоматизированных системах.

Для достижения поставленной цели решаются следующие задачи:

* формирование у обучающихся понятийного аппарата в области криптографии и информационной безопасности;
* освоение обучающимися методики определения актуальных угроз для криптографических систем;
* формирование у обучающихся знаний о методах криптографической защиты информации в автоматизированных информационно-управляющих системах.
* формирование у обучающихся начальных навыков построения и использования криптографических методов защиты информации;

**2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы**

Планируемыми результатами обучения по дисциплине являются: приобретение знаний, умений, навыков.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ**:

* функции криптосистем (обеспечение конфиденциальности, целостности, подлинности информации);
* математическую модель системы шифрования (дешифрования);
* безусловно стойкие шифры, способы и условия их реализации;
* классификацию шифров (блоковые, потоковые, с открытым ключом);
* основные методы криптоанализа блоковых шифров (переборный, на основе анализа статистики криптограммы);
* примеры построения блоковых шифров AES, ГОСТ Р 34.12-15;
* принципы построения потоковых шифров;
* модель системы аутентификации сообщений;
* безусловно и вычислительно стойкие системы аутентификации;
* принципы построения хэширующих функций;
* принципы построения криптосистем с открытым ключем;
* аппарат теории чисел, алгебры в части построения и анализа криптосистем с открытым ключем;
* принципы построения криптосистем с открытым ключем Эль-Гамаля, РША;
* модель цифровой подписи сообщения. Виды ЭЦП. Основные схемы ЭЦП, включая ЭЦП на основе эллиптических кривых;
* управления ключами в симметричных криптографических системах;
* этапы жизненного цикла ключа;
* способы распределения ключа с использованием центра распределения ключей.
* модель управления открытыми ключами. Принципы построения PKI. Назначение и порядок использования сертификатов открытых ключей.

**УМЕТЬ**:

- пользоваться методами теории чисел;

- рассчитывать основные характеристики и параметры криптографических алгоритмов защиты информации;

- оценивать (в первом приближении) стойкость основных криптосистем и их элементов;

* шифровать и дешифровать информацию с помощью симметричных и асимметричных криптосистем;
* генерировать и проверять электронную подпись при передаче и получении электронных сообщений и документов;

**ВЛАДЕТЬ**:

* навыками использования типовых криптографических алгоритмов.
* навыками анализа основных характеристик систем с открытыми ключами;
* программной реализации элементов криптосистем с открытым ключем;

Приобретенные знания, умения, навыки, характеризующие формирование компетенций, осваиваемые в данной дисциплине, позволяют решать профессиональные задачи, приведенные в соответствующем перечне по видам профессиональной деятельности в п. 2.4 общей характеристики основной профессиональной образовательной программы (ОПОП).

Изучение дисциплины направлено на формирование следующих **общекультурных компетенций**

* способность к самооорганизации и самообразованию (ОК-7).

Изучение дисциплины направлено на формирование следующих **профессиональных компетенций (ПК)**, соответствующих виду **профессиональной деятельности, на который ориентирована программа** бакалавриата:

*организационно-управленческая деятельность*:

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

Область профессиональной деятельности обучающихся, освоивших данную дисциплину, приведена в п. 2.1 общей характеристики ОПОП.

Объекты профессиональной деятельности обучающихся, освоивших данную дисциплину, приведены в п. 2.2 общей характеристики ОПОП.

**3. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Криптография» (Б1.В.ОД.19) относится к вариативной части и является обязательной для изучения.

**4. Объем дисциплины и виды учебной работы**

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** |
| **III** |
| Контактная работа (по всем видам занятий)В том числе:* лекции (Л)
* практические занятия (ПЗ)
* лабораторные работы (ЛР))
 | 4816032 | 4816032 |
| Самостоятельная работа (СРС) (всего) | 51 | 51 |
| Контроль | 9 | 9 |
| Форма контроля знаний | З | З |
| Общая трудоемкость: час / з.е. | 108 / 3 | 108 / 3 |

**5. Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Введение | Введение в криптографию. Типы криптосистем. Модель системы шифрования. Способы шифрования. Влияние ошибок в криптограмме на дешифрование. |
| 2 | Алгоритмы шифрования информации в симметричных криптосистемах | Необходимые и достаточные условия построения безусловно стойких криптосистем. Понятие расстояния единственности. Принципы построения блочных шифров. Шифры на основе схемы Фейстеля. Подстановочно перестановочные шифры. Методы криптоанализа блочных шифров: тотальный перебор ключей, анализ статистики криптограммы, Модификации блоковых шифров. Стандарты шифрования AES, ГОСТ З 34.12-15. |
| 3 | Аутентификация сообщений | Модель системы аутентификации, классификация, характеристики эффективности. Безусловно стойкие системы аутентификации. Вычислительно-стойкие системы аутентификации. Способы построения ключевых хэш-функций. Системы аутентификации, на основе блочного шифра. |
| 4 | Криптографические системы с открытыми ключами | Аппарат теории чисел, алгебры в части построения и анализа криптосистем с открытым ключем;Принципы построения криптосистем с открытым ключем Эль-Гамаля, РША;Модель цифровой подписи сообщения. Виды ЭЦП. Основные схемы ЭЦП, включая ЭЦП на основе эллиптических кривых;Электронная подпись по алгоритмам RSA и Эль-Гамаля. Стандарт электронной подписи ГОСТ Р 34.10-12. |
| 5 | Управление криптографическими ключами | Модель управления ключами. Этапы жизненного цикла ключа. Распределение ключей на основе ЦРК. Модель управления открытыми ключами. Принципы построения PKI. Назначение и порядок использования сертификатов открытых ключей. |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Введение | 4 | 0 | 4 | 8 |
| 2 | Алгоритмы шифрования информации в симметрич-ных криптосистемах | 4 |  | 10 | 15 |
| 3 | Аутентификация сообщений | 2 | 0 | 4 | 6 |
| 4 | Криптографические системы с открытыми ключами | 4 | 0 | 10 | 16 |
| 5 | Управление криптографии-ческими ключами | 2 |  | 4 | 6 |
|  | Итого | 16 |  | 32 | 51 |

**6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

|  |  |  |
| --- | --- | --- |
| **№****п/п** | **Наименование раздела дисциплины** | **Перечень учебно-методического обеспечения** |
| 1 | Введение | 1.Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. [Электронный ресурс] — Электрон. дан. — М.: УМЦ ЖДТ, 2014. — 440 с. — Режим доступа: http://e.lanbook.com/book/59240.2.Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. [Электронный ресурс] — Электрон. дан. — М.: УМЦ ЖДТ, 2014. — 448 с. — Режим доступа: http://e.lanbook.com/book/59241.3.Основы криптографии: учебное пособие / В.И. Коржик, В.А. Яковлев. - СПб. ИЦ Интермедиа,. 2016г.- 296с. |
| 2 | Алгоритмы шифрования информации в симметричных криптосистемах |
| 3 | Аутентификация сообщений |
| 4 | Криптографические системы с открытыми ключами |
| 5 | Управление криптографическими ключами |

**7. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине**

Фонд оценочных средств по дисциплине является неотъемлемой частью рабочей программы и представлен отдельным документом, рассмотренным на заседании кафедры «Информатика и информационная безопасность» и утвержденным заведующим кафедрой.

**8. Перечень основной и дополнительной учебной литературы, нормативно-правовой документации и других изданий, необходимых для освоения дисциплины**

8.1 Перечень основной учебной литературы, необходимой для освоения дисциплины

1. Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. [Электронный ресурс] — Электрон. дан. — М.: УМЦ ЖДТ, 2014. — 440 с. — Режим доступа: http://e.lanbook.com/book/59240.
2. Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. [Электронный ресурс] — Электрон. дан. — М.: УМЦ ЖДТ, 2014. — 448 с. — Режим доступа: http://e.lanbook.com/book/59241.
3. Основы криптографии: учебное пособие / В.И. Коржик, В.А. Яковлев. - СПб. ИЦ Интермедиа, 2016г.- 296с.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

* + 1. Н.А. Молдовян. Криптография: скоростные шифры. – СПб.: БХВ-Петербург, 2014. – 496 с.
		2. М.В. Адаменко. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК-Пресс, 2012. – 256 с.
		3. Б.Я. Рябко. Криптографические методы защиты информации. – М.: «Горячая линия – Телеком», 2013. – 229 с.
		4. М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. Введение в теоретико-численные методы криптографии. – СПб., М., Краснодар: Лань, 2011. – 394 с.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. Федеральный закон от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации [Электронный ресурс] – Режим доступа: https://rg.ru/2006/07/29/informacia-dok.html.
2. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" [Электронный ресурс] – Режим доступа: https://rg.ru/2011/04/08/podpis-dok.html
3. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Стандартинформ, 2012. – 33 с.
4. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2012. – 38 с.
5. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 25 с.
6. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 42 с.

8.4 Другие издания, необходимые для освоения дисциплины

При изучении данной дисциплины другие издания не используются.

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

1. Личный кабинет обучающегося и электронная информационно-образовательная среда. [Электронный ресурс]. – Режим доступа: http://sdo.pgups.ru/ (для доступа к полнотекстовым документам требуется авторизация).
2. Раздел «Криптография» на сайте www.citforum.ru.
3. Бесплатные курсы по тематике криптографической защиты на портале www.intuit.ru.
4. Информационно-аналитический портал www.anti-malware.ru.
5. Информационно-аналитический портал [www.securitylab.ru](http://www.securitylab.ru).
6. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: (<http://fstec.ru/>).
7. Электронный фонд нормативно-правовой документации. [Электронный ресурс] - Режим доступа: ( <http://docs.cntd.ru/search/intellectual?q=%D0%93%D0%9E%D0%A1%D0%A2+%D0%A0+56205-2014+&itemtype>;
8. Официальный сайт информационной сети ТЕХЭКСПЕРТ [Электронный ресурс] - Режим доступа: *http://www.cntd.ru/*, свободный.
9. Официальный сайт технического комитета по разработке ГОСТов по информационной безопасности - [Электронный ресурс] - Режим доступа: (<http://tk.gost.ru/wps/portal/tk362>).
10. Электронно-библиотечная система ЛАНЬ [Электронный ресурс]. Режим доступа: https://e.lanbook.com — Загл. с экрана.

**10. Методические указания для обучающихся по освоению дисциплины**

Порядок изучения дисциплины следующий:

1. Освоение разделов дисциплины производится в порядке, приведенном в разделе 5 «Содержание и структура дисциплины». Обучающийся должен освоить все разделы дисциплины с помощью учебно-методического обеспечения, приведенного в разделах 6, 8 и 9 рабочей программы.
2. Для формирования компетенций обучающийся должен представить выполненные типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, предусмотренные текущим контролем (см. фонд оценочных средств по дисциплине).
3. По итогам текущего контроля по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. фонд оценочных средств по дисциплине).

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

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине:

* технические средства: компьютерная техника и средства связи**,** персональные компьютеры, проектор;
* методы обучения с использованием информационных технологий**:** демонстрация презентационных материалов;
* Интернет-сервисы и электронные ресурсы: поисковыесистемы, электронная почта, профессиональные, тематические чаты ифорумы, системы аудио и видео конференций, онлайн-энциклопедии исправочники, электронные учебные и учебно-методические материалы; Интернет-сайты, приведенные в разделе 9 настоящей рабочей программы.

