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*

«Информационная безопасность и защита

информации 2» (Б1.Б.7)

для направления

27.04.03 «СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ»

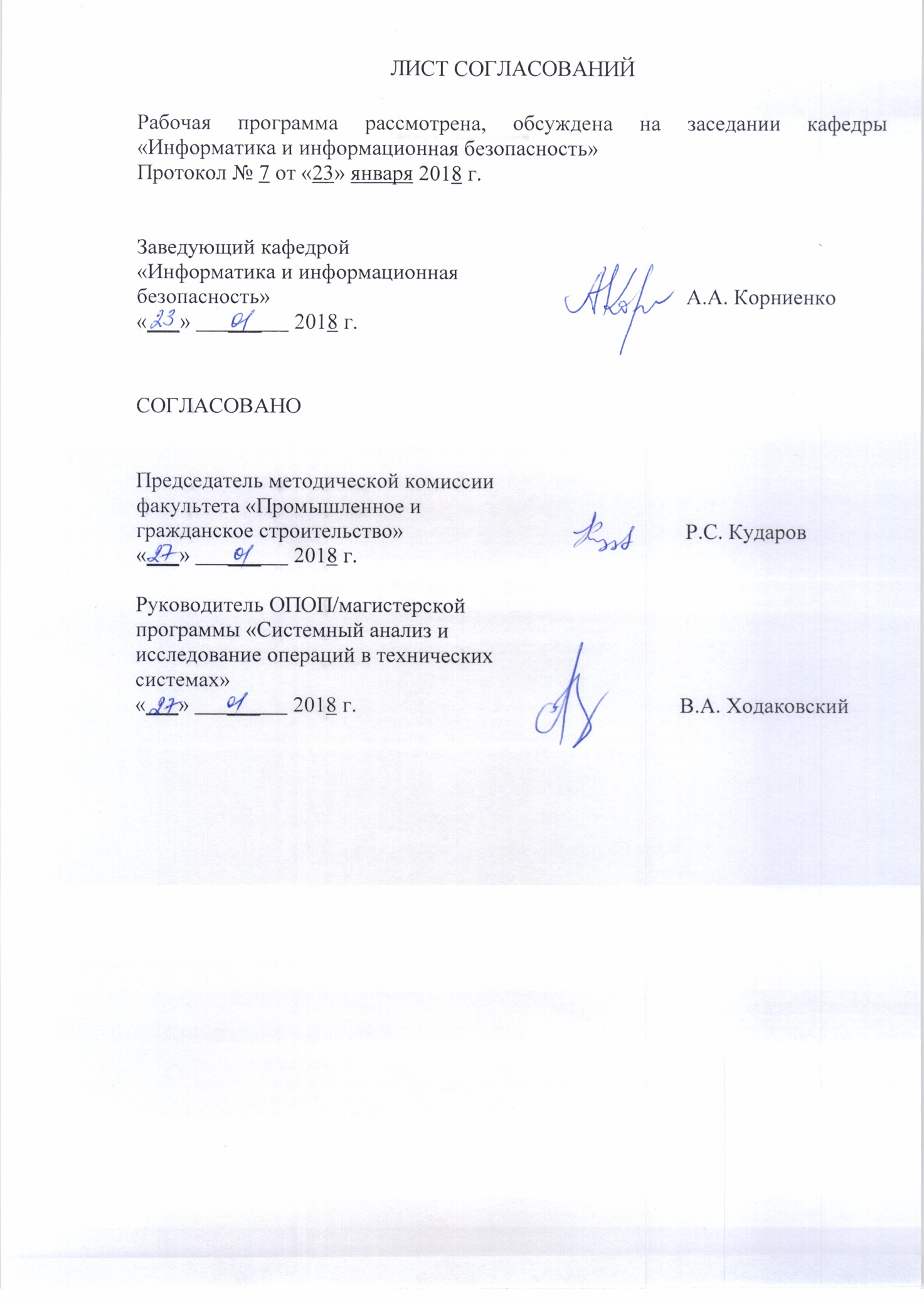
магистерская программа

«Системный анализ и исследование операций в технических системах»

Форма обучения – очная, заочная

Санкт-Петербург

2018



**1 Цели и задачи дисциплины**

Рабочая программа составлена в соответствии с ФГОС, утвержденным 30.10.2014 № 1413 по направлению 27.04.03 «Системный анализ и управление», по дисциплине «Информационная безопасность и защита информации 2».

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других дисциплин профессионального цикла в соответствии с требованиями, установленными федеральным государственным образовательным стандартом для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: организационно-управленческая, аналитическая, научно-исследовательская, педагогическая и специализацией «Системный анализ и исследование операций в технических системах».

Для достижения поставленной цели решаются следующие задачи:

* изучение принципов и методологии управления информационной безопасностью;
* изучение методов и подходов к проектированию, внедрению и эксплуатации систем электронного документооборота;
* изучение подходов к процедурам верификации и методов проведения испытаний программных средств;
* проведение анализа информационной безопасности информационных систем.

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

Планируемыми результатами обучения по дисциплине являются:

* приобретение знаний об основных подходах к управлению информационной безопасностью;
* приобретение знаний о принципах и методах оценки качества и уровня защиты информации в информационных системах;
* приобретение умений по логическому построению системы электронного документооборота на основе инфраструктуры открытых ключей;
* приобретение навыков по оценке рисков информационной безопасности и проведению аудита информационной безопасности информационных систем.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ**:

* методы обработки знаний;
* основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
* основные методы управления информационной безопасностью;
* основные свойства схем шифрования, электронной цифровой подписи и аутентификации при решении задач защиты технологического электронного документооборота и документоведения;
* организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;

**УМЕТЬ**:

* применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
* анализировать и оценивать угрозы информационной безопасности объекта;
* разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;
* оценивать информационные риски в автоматизированных системах;
* разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;
* решать практические задачи информационной безопасности на основе инфраструктуры открытых ключей;

**ВЛАДЕТЬ**:

* методами управления знаниями;
* навыками работы с технической документацией на ЭВМ и вычислительные системы;
* навыками работы с нормативными правовыми актами;
* методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
* методами управления информационной безопасностью автоматизированных систем, в том числе оценки информационных рисков;
* системным подходом к организации защищённого электронного технологического документооборота.

Изучение дисциплины направлено на формирование следующих **общекультурных компетенций (ОК)**:

* готовность действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (ОК-2).

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

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

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

Дисциплина «Информационная безопасность и защита информации 2» (Б1.Б.7) относится к базовой части и является обязательной дисциплиной.

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

Для очной формы обучения:

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** |
| **1** |
| Контактная работа (по видам учебных занятий) | 36 | 36 |
| В том числе: |  |  |
| * лекции (Л) | 18 | 18 |
| * практические занятия (ПЗ) | 18 | 18 |
| * лабораторные работы (ЛР) |  |  |
| Самостоятельная работа (СРС) (всего) | 36 | 36 |
| Контроль |  |  |
| Форма контроля знаний | З | З |
| Общая трудоемкость: час / з.е. | 72 / 2 | 72 / 2 |

Для заочной формы обучения:

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Курс** |
| **1** |
| Контактная работа (по видам учебных занятий) | 16 | 16 |
| В том числе: |  |  |
| * лекции (Л) | 8 | 8 |
| * практические занятия (ПЗ) | 8 | 8 |
| * лабораторные работы (ЛР) |  |  |
| Самостоятельная работа (СРС) (всего) | 52 | 52 |
| Контроль | 4 | 4 |
| Форма контроля знаний | З | З |
| Общая трудоемкость: час / з.е. | 72 / 2 | 72 / 2 |

**5 Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Организационное и правовое обеспечение информационной безопасности Российской Федерации | Организационная основа обеспечения информационной безопасности Российской Федерации  Правовое обеспечение информационной безопасности Российской Федерации  Стандарты и руководящие документы в области информационной безопасности  Методические аспекты защиты персональных данных |
| 2 | Методология управления информационной безопасностью | Основные понятия и определения. Система управления информационной безопасностью (СУИБ). Организационно-правовые аспекты построения и функционирования СУИБ. Технические аспекты построения СУИБ. Процесс управления информационной безопасностью. Задание требований к системе управления информационной безопасностью.  Критерии и процессы управления рисками. Методология оценки рисков информационной безопасности. Примеры методов оценки риска, основанных на использовании таблиц. Методики и программные продукты для оценки рисков.  Основные категории инцидентов. Процесс управления инцидентами. Нормативные документы по управлению инцидентами. Процедура управления инцидентами. Модель управления инцидентами. Формальное описание процесса управления инцидентами. Эффект от внедрения процесса управления инцидентами. Средства автоматизации процесса управления инцидентами.  Понятие аудита информационной безопасности. Концепция аудита информационной безопасности систем информационных технологий и организаций. Цель и задачи аудита информационной безопасности. Формы аудита информационной безопасности. Принципы аудита информационной безопасности. Виды аудита информационной безопасности. Основные этапы проведения аудита информационной безопасности. |
| 3 | Защита электронного документооборота | Нормативные правовые документы в области применения электронного документооборота и электронной подписи. Электронный документооборот: виды, методы организации и применение.  Схемы электронной подписи: виды и применение в электронном документообороте.  Инфраструктура открытых ключей: назначение, архитектура, реализация, сервисы, применение. Логистическая схема инфраструктуры открытых ключей транспортной системы (корпорации).  Специальные схемы электронной подписи: классификация, анализ схем электронной подписи, разработка электронной подписи на основе открытого коллективного ключа (ЭП ОКК).  Применение ЭП ОКК в электронном юридически значимом и защищённом документообороте и техническом документоведении. |
| 4 | Подтверждение соответствия, сертификация, анализ безопасности программного обеспечения | Принципы технического регулирования и подтверждения соответствия. Система сертификации средств защиты информации по требованиям безопасности информации.  Правовая база деятельности и организационная структура Системы сертификации средств защиты информации. Порядок проведения сертификации средств защиты информации.  Нормативные документы по сертификации средств защиты. Требования к испытательным лабораториям. Виды сертификационных испытаний. Задачи и порядок проведения сертификации и испытаний автоматизированных систем. Задачи и порядок проведения сертификации и испытаний средств вычислительной техники. Аттестация объектов информатизации по требованиям безопасности информации. Лицензионная деятельность в области технической защиты информации. |

5.2 Разделы дисциплины и виды занятий

Для очной формы обучения:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** | **Всего** |
| 1 | Организационное и правовое обеспечение информационной безопасности Российской Федерации | 2 |  |  | 6 | 8 |
| 2 | Методология управления информационной безопасностью | 8 | 8 |  | 10 | 26 |
| 3 | Защита электронного документооборота | 6 | 6 |  | 10 | 22 |
| 4 | Подтверждение соответствия, сертификация, анализ безопасности программного обеспечения | 2 | 4 |  | 10 | 16 |
|  | **Итого** | **18** | **18** |  | **36** | **72** |

Для заочной формы обучения:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** | **Всего** |
| 1 | Организационное и правовое обеспечение информационной безопасности Российской Федерации | 2 |  |  | 6 | 8 |
| 2 | Методология управления информационной безопасностью | 2 | 4 |  | 18 | 24 |
| 3 | Защита электронного документооборота | 2 | 2 |  | 18 | 22 |
| 4 | Подтверждение соответствия, сертификация, анализ безопасности программного обеспечения | 2 | 2 |  | 10 | 14 |
|  | **Итого** | **8** | **8** |  | **52** | **68** |

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

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Наименование раздела** | **Перечень учебно-методического обеспечения** |
| 1 | Организационное и правовое обеспечение информационной безопасности Российской Федерации | * Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» * Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 439 с. |
| 2 | Методология управления информационной безопасностью | * Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 439 с. |
| 3 | Защита электронного документооборота | * ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи * Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 447 с. |
| 4 | Подтверждение соответствия, сертификация, анализ безопасности программного обеспечения | * Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 439 с. |

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

Фонд оценочных средств по дисциплине «Информационная безопасность и защита информации 2» является неотъемлемой частью рабочей программы и представлен отдельным документом, рассмотренным на заседании кафедры «Информатика и информационная безопасность» и утвержденным заведующим кафедрой.

**8 Учебно-методическое и информационное обеспечение дисциплины**

Все обучающиеся имеют доступ к электронным учебно-методическим комплексам (ЭУМК) по изучаемой дисциплине согласно персональным логинам и паролям.

Каждый обучающийся обеспечен доступом к электронно-библиотечной системе (ЭБС) через сайт Научно-технической библиотеки Университета http://library.pgups.ru/, содержащей основные издания по изучаемой дисциплине.

ЭБС обеспечивает возможность индивидуального доступа для каждого обучающегося из любой точки, в которой имеется доступ к сети Интернет.

8.1 Перечень основной учебной литературы, необходимой для освоения дисциплины

1. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 439 с.(24 экз., ККО 1,26)
2. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 447 с.(24 экз., ККО 1,26)

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Основы управления информационной безопасностью: учебное пособие / А. П. Курило [и др.]. - Москва : Горячая линия - Телеком, 2012. - 243 с. (12 экз., ККО 0,63)
2. Управление рисками информационной безопасности: учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва : Горячая линия - Телеком, 2012. - 130 с.(12 экз., ККО 0,63)
3. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва : Горячая линия - Телеком, 2012. - 168 с. (12 экз., ККО 0,63)
4. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва : Горячая линия - Телеком, 2012. - 214 с.(12 экз., ККО 0,63)

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»
2. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

8.4 Другие издания, необходимые для освоения дисциплины

При освоении 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/](https://clck.yandex.ru/redir/nWO_r1F33ck?data=NnBZTWRhdFZKOHQxUjhzSWFYVGhXU3JfTEdTY2JPeVRZR0xKdjAzQkRCSko1NlJTd2UxVnRZOWJ3NkhNSG5nRGFZbGdOVmE4T194clZwME1VcDhFOU5VcjlaUDk0MWF3QWMzZU9idjVRajA&b64e=2&sign=5a9122886b8d18119545f9ca08079cfb&keyno=17) (для доступа к полнотекстовым документам требуется авторизация).

2. Научно-техническая библиотека университета [Электронный ресурс]. – Режим доступа: [http://library.pgups.ru/](https://clck.yandex.ru/redir/nWO_r1F33ck?data=NnBZTWRhdFZKOHQxUjhzSWFYVGhXZDVCOHVPSVNvZHd3VEZ4ZVFxVlJnRm1UVG9fYjAzVWJ2S1NkUlQ1Tld6ZjFCRFZ6dDFvd2FLU2k0Unh3T0ZkYmFtcXE5X2prQmdiRlgyaGVtejFSUmNldVBOc3ZjdnFfcktNb3haSDJNZlRJYzA1bEE0NS1fWVlSRlBoeU53dVFPeDNXN3drUE9WWDVHYUFKNkctQ29aOXZwYkxFNEQwM1E&b64e=2&sign=70e725131d005c182709ee9e58f210d4&keyno=17) (свободный доступ).

3. Гарант Информационно-правовой портал [Электронный ресурс]– Режим доступа: <http://www.garant.ru>;

4. 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 «Информационная безопасность и защита информации 2»:

* технические средства (компьютерная техника и средства связи (персональные компьютеры, проектор);
* методы обучения с использованием информационных технологий (демонстрация мультимедийных материалов, компьютерный лабораторный практикум);
* Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, онлайн-энциклопедии и справочники, электронные учебные и учебно-методические материалы).
* электронная информационно-образовательная среда Петербургского государственного университета путей сообщения Императора Александра I [Электронный ресурс]. Режим доступа: http://sdo.pgups.ru.

Дисциплина обеспечена необходимым комплектом лицензионного программного обеспечения, установленного на технических средствах, размещенных в специальных помещениях и помещениях для самостоятельной работы: операционная система Windows, MS Office.

**12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Материально-техническая база обеспечивает проведение всех видов учебных занятий, предусмотренных учебным планом по направлению 27.04.03 и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит специальные помещения - учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения на семестр учебного года выделяются в соответствии с расписанием занятий.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (мультимедийным проектором, экраном, либо свободным участком стены ровного светлого тона размером не менее 2х1.5 метра, стандартной доской для работы с маркером). В случае отсутствия стационарной установки аудитория оснащена розетками электропитания для подключения переносного комплекта мультимедийной аппаратуры и экраном (либо свободным участком стены ровного светлого тона размером не менее 2х1.5 метра).

Для проведения занятий лекционного типа предлагаются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации, соответствующие рабочей учебной программе дисциплины.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.



|  |  |  |
| --- | --- | --- |
| Разработчик программы  доцент |  | С.В. Диасамидзе |
| «\_23\_» января 2018 г. |  |  |