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*

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» (Б1.Б.11)

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

по специализации

«Информационная безопасность автоматизированных системна транспорте»

Форма обучения – очная

Санкт-Петербург

2018



1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным от 01.12.2016, приказ № 1509 по специальности 10.05.03 «Информационная безопасность автоматизированных систем» по специализации «Информационная безопасность автоматизированных систем на транспорте» по дисциплине «Основы информационной безопасности».

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых дисциплин первого блока в соответствии с требованиями, установленными федеральным государственным образовательным стандартом (приказ Минобрнауки России от 01.12.2016 № 1509) для формирования у выпускника общекультурных и профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: научно-исследовательская, проектная, контрольно-аналитическая, организационно-управленческая, эксплуатационная и специализацией «Информационная безопасность автоматизированных сетей и систем на транспорте»

Для достижения поставленной цели решаются следующие задачи:

* подготовка студента по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
* подготовка студента к изучению дисциплин, определённых учебным планом в соответствии с указанными компетенциями;
* развитие социально-воспитательного компонента учебного процесса.
1. 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 и/или опыта деятельности.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

* основы обеспечения информационной безопасности информационных систем;
* нормативные документы РФ в области защиты информации;
* правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
* основные угрозы безопасности информации и модели нарушителя в информационных системах;
* основные меры по защите информации в информационных системах (организационные, правовые, программно-аппаратные, криптографические, технические);
* основные методы управления информационной безопасностью.

УМЕТЬ:

* классифицировать защищаемую информацию по видам информации ограниченного доступа;
* классифицировать и оценивать информационные угрозы для объекта информатизации;
* пользоваться нормативными документами по защите информации;
* анализировать и оценивать информационные угрозы объекта информатизации;
* определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите.

ВЛАДЕТЬ:

* профессиональной терминологией в области информационной безопасности;
* навыками безопасного использования технических средств в профессиональной деятельности;
* навыками работы с нормативными правовыми актами.

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

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

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5).

Изучение дисциплины направлено на формирование следующих профессиональных компетенций (ПК), соответствующих видам

профессиональной деятельности, на которые ориентирована программа специалитета:

* научно-исследовательская деятельность:

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4).

* проектно-конструкторская деятельность:

способностью участвовать в разработке защищенных

автоматизированных систем в сфере профессиональной деятельности (ПК-9);

способностью разрабатывать политику информационной безопасности автоматизированной системы (ПК-11).

* контрольно-аналитическая деятельность:

способностью участвовать в проведении экспериментально­-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16).

- организационно-управленческая деятельность:

Способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22).

* эксплуатационная деятельность:
* способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
* способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);
* способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27).

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.

1. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Основы информационной безопасности» (Б1.Б.11) относится к базовой части и является обязательной дисциплиной.

1. Объем дисциплины и виды учебной работы

|  |  |  |
| --- | --- | --- |
| Вид учебной работы | Всего часов | Семестр |
| IV |
| Контактная работа (по видам учебных занятий) | 68 | 68 |
| В том числе:- лекции (Л) | 34 | 34 |
| - практические занятия (ПЗ) | 34 | 34 |
| - лабораторные работы (ЛР) | - | - |
| Самостоятельная работа (СРС) (всего) | 31 | 31 |
| Контроль | 9 | 9 |
| Форма контроля знаний | 3 | 3 |
| Общая трудоемкость: час / з.е. | 108/3 | 108/3 |

1. Содержание и структура дисциплины

**5.1 Содержание дисциплины**

|  |  |  |
| --- | --- | --- |
| №п/п | Наименование раздела дисциплины | Содержание раздела |
| 1. | Введение в информационную безопасность | Информация. Понятие, свойства, количество информации. Защищаемая информация.Основные понятия, основные принципы обеспечения информационной безопасности. Нормативно-правовая база обеспечения информационной безопасности РФ. Организационная структура обеспечения информационной безопасности РФ.Угрозы информационной безопасности, их классификация. Основные механизмы защиты информации. |
| 2. | Введение в правила разграничения доступа | Основные понятия. Идентификация и аутентификация: способы, формы, системность.Основные положения системы правил разграничения доступа. |
| 3. | Введение в криптографические методы защиты информации. | Основные понятия. Стенографические методы защиты.Методы подстановки. Методы перестановки.Гаммирование. Симметричные и ассиметричные криптосистемы. Хеширование. |
| 4. | Принципы построения системы защиты информации | Нормативно-правовая составляющая системы защиты информации.Организационная составляющая системы защиты информации.Техническая составляющая системы защиты информации.Подходы к построению системы защиты информации от угроз конфиденциальности, целостности, доступности. |

**5.2 Разделы дисциплины и виды занятий**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №п/п | Наименование раздела дисциплины | Л | ПЗ | ЛР | СРС |
| 1. | Введение в информационную безопасность | 10 | 10 | - | 8 |
| 2. | Введение в правила разграничения доступа | 8 | 8 | - | 7 |
| 3. | Введение в криптографические методы защиты информации. | 8 | 8 | - | 8 |
| 4. | Принципы построения системы защиты информации | 8 | 8 | - | 8 |
| Итого | 34 | 34 | - | 31 |

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

|  |  |  |
| --- | --- | --- |
| №п/п | Наименование раздела дисциплины | Перечень учебно-методического обеспечения |
| 1. | Введение в информационную безопасность | 1. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. - Ч. 1 : Методология и система обеспечения информационной безопасности на железнодорожном транспорте / С. Е. Ададуров [и др.]. - 440 с.
2. Диасамидзе С. В. Гуманитарные основы информационной безопасности: учебное пособие. – СПб: ПГУПС, 2018. – 48 с.
 |
| 2 | Введение в правила разграничения доступа | Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. - Ч. 1 : Методология и система обеспечения информационной безопасности на железнодорожном транспорте / С. Е. Ададуров [и др.]. - 440 с. Диасамидзе С. В. Гуманитарные основы информационной безопасности: учебное пособие. – СПб: ПГУПС, 2018. – 48 с. |
| 3 | Введение в криптографические методы защиты информации. | Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. - Ч. 1 : Методология и система обеспечения информационной безопасности на железнодорожном транспорте / С. Е. Ададуров [и др.]. - 440 с.  |
| 4 | Принципы построения системы защиты информации | Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. - Ч. 1 : Методология и система обеспечения информационной безопасности на железнодорожном транспорте / С. Е. Ададуров [и др.]. - 440 с.  |

1. 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 и утвержденным заведующим кафедрой.

1. 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 ч.: / под ред. А. А. Корниенко. – М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. - Ч. 1 : Методология и система обеспечения информационной безопасности на железнодорожном транспорте / С. Е. Ададуров [и др.]. - 440 с.
2. Диасамидзе С. В. Гуманитарные основы информационной безопасности: учебное пособие. – СПб: ПГУПС, 2018. – 48 с.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : , 2016. — 266 с. — Режим доступа: <https://e.lanbook.com/book/100295>
2. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2010. - 544 с. <https://e.lanbook.com/book/1122>

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646);

2. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы

3. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ;

8.4 Другие издания, необходимые для освоения дисциплины

При освоении данной дисциплины другие издания не используются.

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

1. Сайт научно-технической библиотеки университета: http://library.pgups.ru/jirbis/index.php?option=com\_irbis&Itemid=300

2. Интернет-университет информационных технологий. http://www.intuit.ru

3. Университетская библиотека онлайн. http://www.biblioclub.ru/

4. Проект «Информационная безопасность». http://www.itsec.ru/

5. Интернет-версия системы «Консультант-Плюс». http://www.consultant.ru/

1. 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 и (или) опыта деятельности, 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).
4. 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, интерактивная доска,видеокамеры, акустическая система и т.д.);

методы обучения с использованием информационных технологий(компьютерное тестирование, демонстрация мультимедийныхматериалов, компьютерный лабораторный практикум и т.д.);

перечень Интернет-сервисов и электронных ресурсов (поисковыесистемы, электронная почта, профессиональные, тематические чаты ифорумы, системы аудио и видео конференций, онлайн-энциклопедии исправочники, электронные учебные и учебно-методические материалы).

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

Microsoft Windows 7;

Microsoft Word 2010;

MicrosoftExcel 2010;

MicrosoftPowerPoint 2010;

перечень прикладного программного обеспечения (системы тестирования, профессиональные пакеты прикладных программ, программы-тренажеры, программы-симуляторы) перечень информационных справочных систем.

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

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

Она содержит специальные помещения, укомплектованных специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Материально-техническая база дисциплины включает:

* + - * помещения для проведения лекционных занятий, укомплектованные наборами демонстрационного оборудования (стационарными или переносными персональными компьютерами, настенными или переносными экранами, мультимедийными проекторами с дистанционным управлением и другими информационно-демонстрационными средствами) и учебно-наглядными пособиями (презентациями), обеспечивающими тематические иллюстрации в соответствии с рабочей программой дисциплины;
			* лабораторию информационной безопасности информационно-коммуникационных систем (ауд. 2-104), оснащенную программно-аппаратными средствами защиты информации в соответствии с требованиями ФГОС ВО; лаборатория также оборудована современной вычислительной техникой, комплектом проекционного оборудования для преподавателя;
			* помещения для выполнения курсовой работы, оснащенные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых для выполнения индивидуального задания программных средств (см. раздел 11), а также комплектом оборудования для печати;
			* помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации;
			* помещения для проведения групповых и индивидуальных консультаций, укомплектованные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых программных средств (см. раздел 11);
			* помещения для проведения текущего контроля и промежуточной аттестации.



|  |  |  |
| --- | --- | --- |
| Разработчик программы, доцент | \_\_\_\_\_\_\_\_\_\_\_\_ | С.В. Диасамидзе |
|

|  |
| --- |
| 12.04.2018 г. |

 |  |  |