





**1 Цели и задачи дисциплины**

Рабочая программа составлена в соответствие 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 «Информационная безопасность информационно-управляющих и информационно-логистических систем транспорта» (Б1.Б.36).

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых 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: научно-исследовательская, проектная, контрольно-аналитическая, организационно-управленческая, эксплуатацион­ная и специализацией «Информационная безопасность автоматизированных систем на транспорте».

Для достижения поставленной цели определены следующие задачи изучения дисциплины:

* 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.

При изучении дисциплины решаются следующие конкретные задачи:

* изучение методологии проведения комплексного анализа защищенности и инструментального мониторинга информационно-логистических и информационно-управляющих систем на транспорте;
* изучение принципов проектирования и оценивания надежности результатов разработки программных элементов информационно-логистических и информационно-управляющих систем на транспорте;
* анализ возможностей эксплуатации программно-аппаратных средств защиты информационно-логистических и информационно-управляющих систем с учетом специфики угроз информации в них.

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

Планируемыми результатами обучения по дисциплине являются: приобретение знаний, умений, навыков и/или опыта деятельности.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ:**

* основы комплексного обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта;

**УМЕТЬ:**

* используя современные методы и средства, разрабатывать и оценивать модели и политики безопасности автоматизированных и информационно-управляющих систем на транспорте;
* реализовывать системы защиты информации в распределенных автоматизированных, информационно-управляющих и информационно-логистических системах на транспорте в соответствии со стандартами по оценке защищенных систем;
* анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте, применять автоматизированные средства мониторинга, аудита и анализа защищенности данных систем;

**ВЛАДЕТЬ:**

* навыками анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте;
* навыками анализа угроз и навыками построения политик безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта;
* методами эксплуатации средств защиты информации;
* системным подходом к организации информационных процессов (в том числе систем управления ресурсами предприятия и технологий поддержки жизненного цикла), анализу информационной безопасности распределенных автоматизированных информационно-управляющих и информационно-логистических систем транспорта.

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 *профессионально-специализированных компетенций*:

* способностью участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно логистических систем на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации (ПСК-10.1);
* способностью осуществлять рациональный выбор средств и разрабатывать предложения по обеспечению информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) (ПСК-10.3);
* способностью осуществлять мониторинг и аудит уровня защищенности, оценку соответствия и аттестацию распределенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с учетом нормативных требований по защите информации (ПСК-10.4).

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

Дисциплина «Информационная безопасность информационно-управляющих и информационно-логистических систем транспорта» (Б1.Б.36) относится к базовой части и является обязательной дисциплиной.

**4 Объем дисциплины и виды учебной работы**

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестры** |
| 9 |
| Контактная работа (по видам учебных занятий)В том числе: | 54 | 54 |
| ‑ лекции (Л) | 36 | 36 |
| ‑ практические занятия (ПЗ) |  |  |
| ‑ лабораторные работы (ЛР) | 18 | 18 |
| Самостоятельная работа (СРС) (всего) | 58 | 54 |
| Форма контроля знаний | Зачет | Зачет |
| 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** |
| **Модуль 1** |
| 1 | Информационная безопасность систем управления движением поездов, пассажирскими и грузовыми перевозками | Общая характеристика информационно-управляющих систем как объектов информационной безопасности. Информационные системы сети центров управления перевозками. Структура и основные функции центров управления перевозками (ЦУП). Информационное обеспечение ЦУП. Программно-технический комплекс единого диспетчерского центра управления (ЕДЦУ). Подсистема, методы и средства обеспечения информационной безопасности ЕДЦУ.Защищаемые объекты и угрозы информационной безопасности информаци­онных систем управления движением (системы железнодорожной автоматики и телемеханики, бортовые системы управления, системы диспетчерского управления). Подсистема, методы и средства обеспечения информационной безопасности и защиты информации информационных систем управления движением. |
| **Модуль 2** |
| 2 | Информационная безопасность автоматизированных систем управления грузовыми перевозками и информационно-логистических систем | Общая характеристика сетевой интегрированной корпоративной информаци­онно-управляющей системы «СИРИУС». Подсистема, методы и средства обеспечения информационной безопасности и защиты информации системы «СИРИУС».Общая характеристика, методы и средства обеспечения информационной безопасности и защиты информации автоматизированной системы оперативного управления перевозками (АСОУП), АСУ «Грузовой экспресс», АСУ вагонным и контейнерным парком. Общая характеристика системы «ГИД “Урал-ВНИИЖТ”». Состав и основные компоненты центрального комплекса системы ГИД. Взаимодействие подсистем, АРМов и пользователей ГИД. Подсистемы, методы и средства обеспечения информационной безопасности и защиты информации системы «ГИД “Урал-ВНИИЖТ”».Назначение и структура автоматизиро­ванного комплекса системы фирменного транспортного обслуживания (АКС ФТО). Функции и характеристика программно-аппаратной платформы АС «ЭТРАН». АС «ЭТРАН» как объект информационной безопасности.  |
| 3 | Информационная безопасность автоматизированных систем управления пассажирскими перевозками | Общая характеристика информационно-логистических систем как объектов информационной безопасности. Назначение, состав и основные функциональные подсистемы АСУ «Экспресс-3». Программно - аппаратный комплекс АСУ «Экспресс-3». Угрозы и защищаемые объекты АСУ «Экспресс-3». Система обеспечения информационной безопасности АСУ «Экспресс-3». Средства обеспечения информационной безопасности АСУ «Экспресс-3». |
| **Модуль 3** |
| 4 | Системы защиты информации и обеспечения информационной безопасности корпоративного и дорожного уровней | Назначение и архитектура систем управления доступом. Примеры типовых систем управления доступом. Система учета и регистрации заявок на доступ к информационным ресурсам ОАО «РЖД». Основные принципы и требования к построению системы антивирусной защиты. Система антивирусной защиты ОАО «РЖД». Защищенный сегмент электронной почтовой системы (ЭПС). Принципы построения и функционирования ЭПС ОАО «РЖД». Методы и средства обеспечения информационной безопасности и защиты информации ЭПС. Защищенный электронный технологический документооборот (ЭТД). Принципы построения, функционирования и защиты информации ЭТД ОАО «РЖД».Средства аудита информационной безопасности и защиты информации региона ведения железной дороги. Типовые программно-аппаратные средства защиты информации региона ведения железной дороги. Основные решения и средства обеспечения информационной безопасности, применяемые в СПД и ЛВС подразделений ОАО «РЖД». Сетевые средства защиты информации. |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование разделов дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Информационная безопасность систем управления движением поездов, пассажирскими и грузовыми перевозками | 8 |  | 4 | 12 |
| 2 | Информационная безопасность автоматизированных систем управления грузовыми перевозками и информационно-логистических систем | 10 |  | 6 | 14 |
| 3 | Информационная безопасность автоматизированных систем управления пассажирскими перевозками | 8 |  | 2 | 10 |
| 4 | Системы защиты информации и обеспечения информационной безопасности корпоративного и дорожного уровней | 10 |  | 6 | 18 |

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

|  |  |  |
| --- | --- | --- |
| **№****п/п** | **Наименование раздела** | **Перечень учебно-методического обеспечения** |
| 1 | Информационная безопасность систем управления движением поездов, пассажирскими и грузовыми перевозками | 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. – 439с.
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.
 |
| 2 | Информационная безопасность автоматизированных систем управления грузовыми перевозками и информационно-логистических систем |
| 3 | Информационная безопасность автоматизированных систем управления пассажирскими перевозками |
| 4 | Системы защиты информации и обеспечения информационной безопасности корпоративного и дорожного уровней |

**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 и утвержденным заведующим
кафедрой.

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

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.
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.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Корниенко А.А., Поляничко М.А. Стандарты информационной безопасности (учебное пособие). – СПб.: ПГУПС, 2011. – 72 с.
2. Корниенко А.А., Диасамидзе С.В. Защищенный электронный технологический документооборот на железнодорожном транспорте (учебное пособие). – СПб.: ПГУПС, 2015. – 58 с.
3. А.А. Корниенко, А.П. Глухов, С.В. Диасамидзе, А.А. Сидак. Профили защиты и задания ПО безопасности корпоративных информационных систем и сетей железнодорожного транспорта: учебное пособие. – СПб.: ПГУПС, 2014. – 94 с.
4. Корпоративные информационные системы на железнодорожном транспорте: Учебник / под ред. Э.К. Лецкого и В.В. Яковлева – М.: УМЦО ЖДТ, 2013. – 256 с.
5. Платонов В.В. Программно-аппаратные средства защиты информации. – М.: Академия, 2013. – 336 с.

8.3 Перечень нормативно-правовой документации, необходимой для
освоения дисциплины

1. Стратегия национальной безопасности Российской Федерации до 2020 года, от 12 мая 2009 г. № 537.
2. Федеральные законы:
	* + - «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006;
			- «О коммерческой тайне» № 119-ФЗ от 29.07.2004;
			- «О персональных данных» № 152-ФЗ от 27.07.2006.
3. Сборник Руководящих документов Гостехкомиссии России по защите информации от несанкционированного доступа – М: Гостехкомиссия, 1998. – 120 с.
4. ГОСТ Р ИСО/МЭК 15408-1,-2,-3. Информационная технология. Методы и средства обеспечения безопасности (Часть 1. Введение и общая модель. Часть 2. Функциональные требования безопасности. Часть 3. Требования гарантированности безопасности). – М.: ИПК Издательство стандартов, 2004.
5. ИСО/МЭК 27001. Информационные технологии. Технологии безопасности. Система управления информационной безопасностью. Требования
6. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

8.4 Другие издания, необходимые для освоения дисциплины

1. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. – М.: Горячая линия–Телеком, 2014. – 244 с.
2. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление инцидентами информационной безопасности и непрерывностью бизнеса. – М.: Горячая линия–Телеком, 2012. – 130 с.
3. Милославская Н. Г., Толстой А. И., Сенаторов М. Ю. Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2012. – 214 с.

**9. 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. Официальный портал Росстандарта <http://www.gost.ru/wps/portal/>, портал по стандартизации <http://standard.gost.ru/wps/portal/>
3. Официальный сайт ФСТЭК России <http://www.fstec.ru/>
4. Проект «Информационная безопасность». <http://www.itsec.ru/>
5. Проект «Национальный Открытый Университет «ИНТУИТ» http://www.intuit.ru/

**10. Методические указания для обучающихся по прохождению 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 из разделов 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).

**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:

* + - * персональные компьютеры, локальная вычислительная сеть кафедры, проектор;
			* методы обучения с использованием информационных технологий: компьютерный лабораторный практикум, демонстрация мультимедийных материалов;
			* лабораторное программное обеспечение, разрабатываемое в ходе учебного процесса студентами совместно с преподавателем;
			* Интернет-сервисы и электронные ресурсы: сайты, перечисленные в разделе 9 рабочей программы; электронные учебно-методические материалы, доступные через личный кабинет обучающегося на сайте sdo.pgups.ru; на выбор обучающегося - поисковые системы, профессиональные, тематические чаты и форумы, системы аудио и видео конференций, онлайн-энциклопедии и справочники.

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

* + - * Microsoft Windows 7;
			* Office Standard 2010 Russian OpenLicensePack NoLevel AcademicEdition;
			* Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа <https://get.adobe.com/ru/reader/>);
			* Visual Studio Professional 2010 Russian OLP NL AcademicEdition;
			* Oracle Java SE Development Kit 8 (бесплатное, свободно распространяемое программное обеспечение; режим доступа <http://www.oracle.com/technetwork/java/javase/downloads/index.html>);
			* NetBeans IDE 8.2 (бесплатное, свободно распространяемое программное обеспечение; режим доступа <https://netbeans.org/downloads/>).

**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 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.

