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*

«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ» (Б1.Б.19)

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

по специализации

«Информационная безопасность автоматизированных систем на 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 «Управление информационной безопасностью» (Б1.Б.19).

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 принципов и методологии управления информационной безопасностью;
* изучение методов и процесса управления инцидентами информационной безопасности;
* изучение методов и процесса проведения аудита информационной безопасности для оценивания защищенности автоматизированных, информационно-управляющих и распределенных информационных транспортных систем и построения эффективной системы обеспечения информационной безопасности организации.

**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 и/или опыта деятельности.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ:**

* источники и классификацию угроз информационной безопасности;
* основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;
* основные методы управления информационной безопасностью;

**УМЕТЬ:**

* анализировать и оценивать угрозы информационной безопасности объекта;
* разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;
* выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем;
* оценивать информационные риски в автоматизированных системах;
* разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

**ВЛАДЕТЬ:**

* методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем;
* методами управления информационной безопасностью автоматизированных систем;
* методами оценки информационных рисков.

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 профессиональных компетенций (ПК), соответствующих видам профессиональной деятельности, на которые ориентирована программа специалитета:

*научно-исследовательская деятельность:*

* способность проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

*проектно-конструкторская деятельность:*

* способность разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);
* способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

*организационно-управленческая деятельность:*

* способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);
* способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);
* способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

*эксплуатационная деятельность:*

* способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);
* способность управлять информационной безопасностью автоматизированной системы (ПК-28).

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 профессиональной образовательной программы**

Дисциплина «Управление информационной безопасностью» (Б1.Б.19) относится базовой части и является обязательной дисциплиной.

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

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** |
| **9** |
| Контактная работа (по видам учебных занятий)В том числе:* лекции (Л)
* практические занятия (ПЗ)
* лабораторные работы (ЛР)
 | 481632 | 481632 |
| Самостоятельная работа (СРС) (всего) | 51 | 51 |
| Контроль | 45 | 45 |
| Форма контроля знаний | Э | Э |
| Общая трудоемкость: час / з.е. | 144/4 | 144/4 |

**5. Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Методология управления информационной безопасностью | Проблема информационной безопасности и защиты информации.Верификационный и риск-ориентированный подходы к обеспечению и управлению информационной безопасностью.Организационно-правовые аспекты и процессная модель управления информационной безопасностью.Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте. |
| 2 | Управление рисками информационной безопасности | Критерии и процессы управления рисками. Методология оценки рисков информационной безопасности. Примеры методов оценки риска, основанных на использовании таблиц. Методики построения систем защиты информации, включающие этап анализа рисков. Методики и программные продукты для оценки рисков. |
| 3 | Управление инцидентами информационной безопасности | 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. |
| 4 | Аудит информационной безопасности | 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.  |
| 5 | Технические аспекты управления информационной безопасностью | Управление и обеспечение информационной безопасности компьютерных сетей организации - функциональные области, базовые задачи, архитектура, основные характеристики. Управление на основе контроля состояния. Управление аппаратными средствами компьютеров на основе технологии WFM. Управление на основе правил системной политики: стандарты LDAP, DEN, COPS. |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Методология управления информационной безопасностью | 4 |  | 4 | 9 |
| 2 | Управление рисками информационной безопасности | 4 |  | 12 | 16 |
| 3 | Управление инцидентами информационной безопасности | 4 |  | 6 | 10 |
| 4 | Аудит информационной безопасности | 2 |  | 6 | 8 |
| 5 | Технические аспекты управления информационной безопасностью | 2 |  | 2 | 8 |
| **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 | Методология управления информационной безопасностью | 1. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 440 с.2. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. - М.: Горячая линия–Телеком, 2014. - 244 с.3. Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте: учебное пособие. – СПб: ПГУПС, 2016. – 45 с. |
| 2 | Управление рисками информационной безопасности | 1. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 440 с.2. Корниенко А.А., Диасамидзе С.В. Аудит и управление информационной безопасностью (учебное пособие). - СПб.: ПГУПС, 2011. – 83 с.3. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. – М.: Горячая линия–Телеком, 2014. - 130 с. |
| 3 | Управление инцидентами информационной безопасности | 1. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 440 с.2. Корниенко А.А., Диасамидзе С.В. Аудит и управление информационной безопасностью (учебное пособие). - СПб.: ПГУПС, 2011. – 83 с.3. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие – М. : Горячая линия - Телеком, 2012. - 168 с. |
| 4 | Аудит информационной безопасности | 1. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 440 с. 2. Корниенко А.А., Диасамидзе С.В. Аудит и управление информационной безопасностью (учебное пособие). - СПб.: ПГУПС, 2011. – 83 с. |
| 5 | Технические аспекты управления информационной безопасностью | 1. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 448 с.2. Корниенко А.А., Диасамидзе С.В. Аудит и управление информационной безопасностью (учебное пособие). - СПб.: ПГУПС, 2011. – 83 с.3. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие - М.: Горячая линия - Телеком, 2012. - 214 с.  |

**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. 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.: 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. – 440 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. – 448 с.

3. Корниенко А.А., Диасамидзе С.В. Аудит и управление информационной безопасностью (учебное пособие). - СПб.: ПГУПС, 2011. – 83 с.

4. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. - М.: Горячая линия–Телеком, 2014. - 244 с.

5. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. – М.: Горячая линия–Телеком, 2014. - 130 с.

6. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие – М. : Горячая линия - Телеком, 2012. - 168 с.

7. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие - М.: Горячая линия - Телеком, 2012. - 214с.

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.

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. 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 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
5. ГОСТ Р ИСО/МЭК 15408-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3.
6. ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
7. ГОСТ ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
8. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
9. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
10. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения.- М.: Стандартинформ, 2012. -12 с.
11. СТО РЖД 1.18.002-2009 «Управление информационной безопасностью. Общие положения» // ОАО «РЖД», 2009.
12. Основные положения защиты информационной инфраструктуры ОАО «РЖД» // ОАО «РЖД», 2013.
13. Политика информационной безопасности ОАО «РЖД // ОАО «РЖД», 2013.
14. Положение по оценке рисков информационной безопасности ОАО «РЖД» // ОАО «РЖД», 2015.
15. Положение по управлению инцидентами информационной безопасности в ОАО «РЖД» // ОАО «РЖД», 2014.

8.4 Другие издания, необходимые для освоения дисциплины

1. Корниенко А.А., Диасамидзе С.В. Управление информационной безопасностью (методические указания к лабораторным работам). - СПб: ПГУПС, 2016. – 48 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 IT <http://citforum.ru/>
5. Интернет-версия системы «Консультант-Плюс». <http://www.consultant.ru/>
6. Проект «Информационная безопасность». <http://www.itsec.ru/>
7. Проект «Национальный Открытый Университет «ИНТУИТ» http://www.intuit.ru/

**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 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:

* 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.
* Microsoft Security Assessment Tool (MSAT) (бесплатная версия, режим доступа <http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=cd057d9d-86b9-4e35-9733-7acb0b2a3ca1>).
* Microsoft Baseline Security Analyzer (бесплатная версия, режим доступа <https://www.microsoft.com/en-us/download/details.aspx?id=7558>).

**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:

* помещения для проведения лабораторных работ, укомплектованных специальной учебно-лабораторной мебелью, лабораторным оборудованием, лабораторными стендами, специализированными измерительными средствами в соответствии с перечнем лабораторных работ.
* помещения для проведения лекционных и практических (семинарских) занятий, укомплектованных специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (настенным экраном с дистанционным управлением, подвижной маркерной доской, считывающим устройством для передачи информации в компьютер, мультимедийным проектором и другими информационно-демонстрационными средствами).



|  |  |  |
| --- | --- | --- |
| Разработчик программы, заведующий кафедрой, проф. | \_\_\_\_\_\_\_\_\_\_\_\_ | А.А. Корниенко |
| 12.04.2018 г. |  |  |