

**1 Цели и задачи дисциплины**

Рабочая программа составлена в соответствии с ФГОС, утвержденным 30.10.2014 № 1402 по направлению 09.04.02 «Информационные системы и технологии», по дисциплине «Информационная безопасность и защита информации на транспорте».

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 «Информационные системы и технологии на транспорте».

Для достижения поставленной цели решаются следующие задачи:

* изучение принципов и методологии управления информационной безопасностью;
* изучение методов и процесса управления инцидентами информационной безопасности;
* изучение методологии проведения комплексного анализа защищенности и ин­ст­ру­мен­таль­ного мо­ни­то­рин­га автоматизированных транспортных систем.

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

Планируемыми результатами обучения по дисциплине являются:

* приобретение знаний об основных подходах к управлению информационной безопасностью;
* приобретение умений по применению принципов и методов управления инцидентами информационной безопасности;
* приобретение навыков по проведения комплексного анализа защищенности и ин­ст­ру­мен­таль­ного мо­ни­то­рин­га информационных транспортных систем.

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 информационных транспортных систем;
* выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных транспортных систем;
* оценивать информационные риски в информационных транспортных системах;
* разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных транспортных систем;

**ВЛАДЕТЬ:**

* методами мониторинга и аудита, выявления угроз информационной безопасности информационных транспортных систем;
* методами управления информационной безопасностью информационных транспортных 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 **общекультурных компетенций (ОК)**:

* умение свободно пользоваться русским и иностранным языком как средством делового общения (ОК-3);
* способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности (ОК-6);

Изучение дисциплины направлено на формирование следующих **общепрофессиональных компетенций (ОПК)**:

* способность анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями (ОПК-6);

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

*проектно-конструкторская деятельность:*

умение разрабатывать новые методы и средства проектирования информационных систем (ПК-2);

*научно-исследовательская деятельность:*

умение проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция, бизнес, предпринимательство, коммерция, менеджмент, банковские системы, безопасность информационных систем, управление технологическими процессами, механика, техническая физика, энергетика, ядерная энергетика, силовая электроника, металлургия, строительство, транспорт, железнодорожный транспорт, связь, телекоммуникации, управление инфокоммуникациями, почтовая связь, химическая промышленность, сельское хозяйство, текстильная и легкая промышленность, пищевая промышленность, медицинские и биотехнологии, горное дело, обеспечение безопасности подземных предприятий и производств, геология, нефтегазовая отрасль, геодезия и картография, геоинформационные системы, лесной комплекс, химико-лесной комплекс, экология, сфера сервиса, системы массовой информации, дизайн, медиаиндустрия, а также предприятия различного профиля и все виды деятельности в условиях экономики информационного общества (ПК-8);

умение проводить разработку и исследование методик анализа, синтеза, оптимизации и прогнозирования качества процессов функционирования информационных систем и технологий (ПК-9).

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 профессиональной программы**

Дисциплина «Информационная безопасность и защита информации на транспорте» относится к вариативной части и является дисциплиной по выбору.

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

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** |
| **1** |
| Контактная работа (по видам учебных занятий) | 36 | 36 |
| В том числе: |  |  |
| * лекции (Л) |  |  |
| * практические занятия (ПЗ) | 18 | 18 |
| * лабораторные работы (ЛР) | 18 | 18 |
| Самостоятельная работа (СРС) (всего) | 90 | 90 |
| Контроль | 54 | 54 |
| Форма контроля знаний | Э | Э |
| Общая трудоемкость: час / з.е. | 180/ 5 | 180/ 5 |

**5 Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Организационно-правовые аспекты и процессная модель управления информационной безопасностью | Основные понятия и определения. Система управления информационной безопасностью (СУИБ). Организационно-правовые аспекты построения и функционирования СУИБ. Технические аспекты построения СУИБ. Подходы к построению системы управления информационной безопасностью корпорации и корпоративных информационных систем и сетей. Процесс управления информационной безопасностью. Задание требований к системе управления информационной безопасностью. |
| 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 | Информационная безопасность ERP-систем | Система управления ресурсами предприятия (ERP-система). Понятие, назначение и функции ERP-систем. Общие принципы построения ERP-системы. Реализация ERP-системы на программно-аппаратной платформе SAPR/3.  Функции и состав Единой корпоративной автоматизированной системы управления финансами и ресурсами (ЕК АСУФР/ТР) Характеристика программно-аппаратного комплекса ЕК АСУФР/ТР. Характеристика угроз информационной безопасности ЕК АСУФР/ТР.  Подсистема, методы и средства обеспечения информационной безопасности ERP-систем. Характеристика объектов защиты и мер обеспечения информационной безопасности ЕК АСУФР/ТР. Система требований к информационной безопасности ЕК АСУФР/ТР. |
| 6 | Информационная безопасность автоматизированных систем управления грузовыми перевозками и информационно-логистических систем | 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. |
| 7 | 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». |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** | **Всего** |
| 1 | Организационно-правовые аспекты и процессная модель управления информационной безопасностью |  |  | 4 | 12 | 16 |
| 2 | Управление рисками информационной безопасности |  |  | 6 | 12 | 16 |
| 3 | Управление инцидентами информационной безопасности |  |  | 4 | 12 | 16 |
| 4 | Аудит информационной безопасности |  |  | 4 | 12 | 18 |
| 5 | Информационная безопасность ERP-систем |  | 6 |  | 14 | 20 |
| 6 | Информационная безопасность автоматизированных систем управления грузовыми перевозками и информационно-логистических систем |  | 6 |  | 14 | 20 |
| 7 | Информационная безопасность автоматизированных систем управления пассажирскими перевозками |  | 6 |  | 14 | 20 |
|  | **Итого** |  | **18** | **18** | **90** | **126** |

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

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Наименование раздела** | **Перечень учебно-методического обеспечения** |
| 1 | Организационно-правовые аспекты и процессная модель 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.: УМЦ ЖДТ, 2014. – 439 с. |
| 2 | Управление рисками информационной безопасности | * 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.: УМЦ ЖДТ, 2014. – 439 с. |
| 3 | Управление инцидентами информационной безопасности | * 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.: УМЦ ЖДТ, 2014. – 439 с. |
| 4 | Аудит информационной безопасности | * 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.: УМЦ ЖДТ, 2014. – 439 с. |
| 5 | Информационная безопасность ERP-систем | * 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.: УМЦ ЖДТ, 2014. – 439 с. * 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.: УМЦ ЖДТ, 2014. – 447 с. * 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. |
| 6 | Информационная безопасность автоматизированных систем управления грузовыми перевозками и информационно-логистических систем | * 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.: УМЦ ЖДТ, 2014. – 439 с. * 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.: УМЦ ЖДТ, 2014. – 447 с. * Корниенко А.А., Диасамидзе С.В. Защищенный электронный технологический документооборот на железнодорожном транспорте (учебное пособие). - СПб.: ПГУПС, 2015. – 58 с. |
| 7 | Информационная безопасность автоматизированных систем управления пассажирскими перевозками | * 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.: УМЦ ЖДТ, 2014. – 439 с. * 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.: УМЦ ЖДТ, 2014. – 447 с. * 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. |

**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 на транспорте» 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 1,2)
3. Корниенко А.А., Диасамидзе С.В. Защищенный электронный технологический документооборот на железнодорожном транспорте (учебное пособие). - СПб.: ПГУПС, 2015. – 58 с. (40 экз., ККО 2,0)
4. 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. (30 экз., ККО 1,5)

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 0,6)
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 0,6)
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 0,6)
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 0,6)
5. Корпоративные информационные системы на железнодорожном транспорте: Учебник / под ред. Э.К. Лецкого и В.В. Яковлева – М.: УМЦО ЖДТ, 2013.- 256 с. (19 экз., ККО 0,95)

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. Указ Президента РФ «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. Интернет-университет информационных технологий. <http://www.intuit.ru>
2. Проект «Информационная безопасность и защита информации». <http://www.itsec.ru/>
3. Интернет-версия системы «Консультант-Плюс». <http://www.consultant.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 «Информационная безопасность и защита информации на транспорте»:

* технические средства (компьютерная техника и средства связи (персональные компьютеры, проектор);
* методы обучения с использованием информационных технологий (демонстрация мультимедийных материалов, компьютерный лабораторный практикум);
* перечень Интернет-сервисов и электронных ресурсов (поисковые системы, электронная почта, профессиональные, тематические чаты и форумы, системы аудио и видео конференций, онлайн-энциклопедии и справочники, электронные учебные и учебно-методические материалы).

Кафедра «Информатика и информационная безопасность» обеспечена необходимым комплектом лицензионного программного обеспечения:

* Microsoft Windows 7;
* Microsoft Word 2010;
* Microsoft Excel 2010;
* Microsoft Visual Studio 2010.

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



ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа по дисциплине «Информационная безопасность и защита информации на транспорте» (Б1.В.ДВ.2.2) на 2016/2017 учебный год актуализирована без изменений.