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*

«Комплексное обеспечение информационной безопасности автоматизированных систем»
(Б1.В.ОД.11)

для специальности
10.05.03 «Информационная безопасность автоматизированных систем»
по специализации
«Информационная безопасность автоматизированных систем на транспорте»

форма обучения - очная

Санкт-Петербург

2017



**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 «Комплексное обеспечение информационной безопасности автоматизированных систем».

Целью дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» 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 и эксплуатационная.

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;
* обучение студентов практическому применению технологий создания систем управления информационной безопасностью;
* изучение управления рисками и инцидентами;
* изучение работы с системами обнаружения и предотвращения вторжений.

**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:**

* методики управления рисками и инцидентами;
* архитектуру систем управления информационной безопасности;
* средства администрирования информационной безопасности;
* системы обнаружения вторжения;
* системы предотвращения вторжений;
* системы управления доступом.

**УМЕТЬ:**

* определять состав информационных активов, подлежащих защите;
* составлять требования к разрабатываемой автоматизированной системе;
* разрабатывать политику информационной безопасности;
* определять оптимальный вариант решения задачи при наличии альтернатив.

**ВЛАДЕТЬ:**

* навыками разворачивания и настройки систем управления доступом;
* навыками разворачивания и настройки систем обнаружения вторжений;
* навыками разворачивания и настройки систем предотвращения вторжений.

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 **общепрофессиональных** **компетенций** **(ОПК)**:

* *способность применять нормативные правовые акты в профессиональной деятельности* (ОПК-6).

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

**научно-исследовательская деятельность:**

* *способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности* (ПК-6);
* *способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ* (ПК-7);

**проектно-конструкторская деятельность:**

* *способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем* (ПК-8);
* *способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности* (ПК-9);

**организационно-управленческая деятельность:**

* *способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа* (ПК-23).

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 «Комплексное обеспечение информационной безопасности автоматизированных систем» (Б1.В.ОД.11) относится к вариативной части и является обязательной для изучения.

**4 Объем дисциплины и виды учебной работы**

Общая трудоемкость дисциплины ‑ 4 зачетных единицы.

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестры** |
| **9** |
| Контактная работа (по видам учебных занятий)В том числе: | 50 | 50 |
| ‑ лекции (Л) | 34 | 34 |
| ‑ практические занятия (ПЗ) | - | - |
| ‑ лабораторные работы (ЛР) | 16 | 16 |
| Самостоятельная работа (СРС) (всего) | 22 | 22 |
| Контроль | 36 | 36 |
| Форма контроля знаний | Экзамен, КП | Экзамен, КП |
| Общая трудоемкость: час /з.е. | 108 / 3 | 108 / 3 |

**5 Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№П/П** | **Наименованиераздела дисциплины** | **Содержание раздела** |
| 1 | Система управления информационной безопасностью | Цели и задачи изучения дисциплины " Комплексное обеспечение информационной безопасности автоматизированных систем". Построение систем управления информационной безопасностью. Международные стандарты в области построения систем управления информационной безопасностью. |
| 2 | Методологическое и техническое обеспечение информационной безопасности | Проектирование систем обеспечения информационной безопасности. Архитектура системы обеспечения информационной безопасности. Компоненты системы обеспечения информационной безопасности. |
| 3 | Информационные активы автоматизированной системы | Информационная инфраструктура автоматизированной системы. Оценка информационных активов. Защита информационных активов. Системы предотвращения потери данных. Внутренние угрозы информационным активам. |
| 4 | Управление рисками и инцидентами. Анализ рисков в области защиты информации | Методологии оценки рисков. Выбор шкалы оценки рисков. Оценка стоимости ресурсов, вероятности угроз и величины уязвимости. Определение допустимого уровня остаточных рисков. Подготовка отчета по результатам оценки рисков. Регистрация инцидента информационной безопасности. Расследование инцидента. Реализация действий, предупреждающих повторное возникновение инцидента. |
| 5 | Создание и реализация политик информационной безопасности | Требования стандартов к политике безопасности. Разработка политики безопасности. |
| 6 | Технологии обнаружения вторжений | История разработок в области систем обнаружения и предотвращения вторжений. Принцип работы систем обнаружения и предотвращения вторжений. Архитектура систем обнаружения предотвращения вторжений. Виды систем обнаружения предотвращения вторжений. Внедрение и настройка системы обнаружения и предотвращения вторжений. |
| 7 | Системы управления доступом | История разработок в области систем управления доступом. Технологии, применяемые при реализации систем управления доступом. Виды систем управления доступом. Уязвимые места систем управления доступом. |
| 8 | Управление и администрирование информационной безопасности | Задачи администрирования информационной безопасности. |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№п/п** | **Наименование разделов дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Система управления информационной безопасностью | 4 | - | 0 | 2 |
| 2 | Методологическое и техническое обеспечение информационной безопасности | 4 | - | 0 | 2 |
| 3 | Информационные активы автоматизированной системы | 4 | - | 0 | 2 |
| 4 | Управление рисками и инцидентами. Анализ рисков в области защиты информации | 4 | - | 0 | 2 |
| 5 | Создание и реализация политик информационной безопасности | 4 | - | 0 | 2 |
| 6 | Технологии обнаружения вторжений | 6 | - | 8 | 4 |
| 7 | Системы управления доступом | 4 | - | 8 | 4 |
| 8 | Управление и администрирование информационной безопасности | 4 | - | 0 | 4 |
| **Итого** | 34 | - | 16 | 22 |

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

|  |  |  |
| --- | --- | --- |
| **№п/п** | **Наименование раздела дисциплины** | **Перечень учебно-методического обеспечения** |
| 1 | Система управления информационной безопасностью | Основная литература: [1], [3]Дополнительная литература: [1], [3]Интернет-ресурсы: [1], [3], [4] |
| 2 | Методологическое и техническое обеспечение информационной безопасности | Основная литература: [1], [2]Дополнительная литература: [2], [3]Интернет-ресурсы: [1], [2], [4] |
| 3 | Информационные активы автоматизированной системы | Основная литература [1]Дополнительная литература: [2]Интернет-ресурсы: [1], [3], [5] |
| 4 | Управление рисками и инцидентами. Анализ рисков в области защиты информации | Основная литература [2]Дополнительная литература: [2]Интернет-ресурсы: [1], [2], [3] |
| 5 | Создание и реализация политик информационной безопасности | Основная литература: [3]Нормативно-правовая документация [1], [2], [3]Интернет-ресурсы: [1], [2], [4] |
| 6 | Технологии обнаружения вторжений | Дополнительная литература: [2]Интернет-ресурсы: [1], [3], [5] |
| 7 | Системы управления доступом | Дополнительная литература: [1], [2], [3]Интернет-ресурсы: [1], [2], [3] |
| 8 | Управление и администрирование информационной безопасности | Дополнительная литература: [1], [2], [3]Интернет-ресурсы: [1], [2], [4] |

**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. Афанасьев А., Веденьев Л.Т., Воронцов А.В., Газизова Э.Р., Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов, Горячая линия-Телеком, 2012. – 552 с.
2. Петренко С.А., Симонов С.В., Управление информационными рисками. Экономически оправданная безопасность, ДМК, 2011. – 384 с.
3. Петренко С.А, Курбатов В., Политики безопасности компании при работе в Интернете, ДМК, 2011. – 396 с.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Мельников, В. П. Информационная безопасность и защита информации. / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – 6-е изд., стер. – М.: Академия, 2012. – 336 с.
2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах. / В. Ф. Шаньгин; М.: ФОРУМ-ИНФРА-М, 2010. – 501 с.
3. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. - М.: Горячая линия–Телеком, 2014. - 244 с.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

При освоении данной дисциплины нормативно-правовая документация не используется.

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>.

**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 мультимедийных материалов, компьютерный лабораторный практикум и т.д.);
* 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 обеспечена необходимым комплектом лицензионного программного обеспечения:

* Microsoft Windows 7;
* Microsoft Word 2010;
* Microsoft Excel 2010;
* Microsoft Power Point 2010;
* перечень прикладного программного обеспечения (системы тестирования, профессиональные пакеты прикладных программ, программы-тренажеры, программы-симуляторы) перечень информационных справочных систем.

**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:

* помещение для проведения лабораторных работ (ауд. 2-110), укомплектованное специальной учебно-лабораторной мебелью, лабораторным оборудованием, лабораторными стендами, специализированными измерительными средствами в соответствии с перечнем лабораторных работ;
* помещение для проведения лекционных занятий (ауд. 2-113), укомплектованное 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);
* помещение для проведения групповых и индивидуальных консультаций (ауд. 2-110);
* помещение для проведения текущего контроля и промежуточной аттестации (ауд. 2-110);
* помещения для самостоятельной работы (ауд. 2-110).

