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*

«ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ» (Б1.В.ОД.9)

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 «Теоретические основы компьютерной безопасности» (Б1.В.ОД.9).

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 компьютерной системы как объектно-субъектной модели,
* изучение основных теоретических положений, используемых при разработке механизма идентификации и аутентификации,
* изучение основных теоретических положений, используемых при разработке механизма авторизации,
* изучение алгоритмов реализации аудита и регистрации событий, используемых при разработке механизма идентификации и аутентификации и анализа матрицы доступа,
* изучение средств антивирусной защиты.

**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:**

* угрозы компьютерной безопасности;
* уязвимости и изъяны системы защиты;
* классификацию атак на защищённые компьютерные системы;
* требования, предъявляемые к защищённым компьютерным системам и архитектуру защищенных компьютерных систем;
* теоретические основы построения механизмов защиты компьютерных систем;
* формальные и неформальные модели разграничения доступа субъектов к объектам компьютерной системы;
* модели разграничения доступа в распределённых компьютерных системах;
* классификацию вирусов и средства антивирусной защиты;
* критерии безопасности.

**УМЕТЬ:**

* разрабатывать модели механизма идентификации и аутентификации;
* разрабатывать модели политик разграничения доступа субъектов к объектам компьютерной системы;
* разрабатывать алгоритмы, реализующие политики аудита и регистрации событий.

**ВЛАДЕТЬ:**

* теоретическими знаниями, позволяющими применять математический аппарат, языки и инструментальные средства программирования, для решения профессиональных задач, связанных с разработкой механизмов защиты компьютерных систем.

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 корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);
* способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3).

Изучение дисциплины направлено на формирование следующих профессиональных компетенций (ПК), соответствующих видам профессиональной деятельности, на которые ориентирована программа специалитета:

*научно-исследовательская деятельность:*

* способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

*проектно-конструкторская деятельность:*

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

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 «Теоретические основы компьютерной безопасности» (Б1.В.ОД.9) относится вариативной части и является обязательной дисциплиной.

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

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** |
| **6** |
| Контактная работа (по видам учебных занятий)В том числе:* лекции (Л)
* практические занятия (ПЗ)
* лабораторные работы (ЛР)
 | 683434 | 683434 |
| Самостоятельная работа (СРС) (всего) | 40 | 40 |
| Контроль | 36 | 36 |
| Форма контроля знаний | Э, КП | Э, КП |
| 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 | Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем | Сущность, субъект, доступ, информационный поток. Классическая классификация угроз безопасности информации. Виды информационных потоков. Виды политик управления доступом и информационными потоками. Утечка права доступа и нарушение безопасности КСОсновные виды формальных моделей безопасности. Проблема адекватности реализации модели безопасности в реальной компьютерной системе |
| 2 | Модели компьютерных систем с дискреционным управлением доступом | Модель матрицы доступов Харрисона–Руззо–Ульмана. Описание модели. Анализ безопасности систем ХРУ Модель типизированной матрицы доступов |
| 3 | Модели компьютерных систем с мандатным управлением доступом | Модель Белла–ЛаПадулы. Классическая модель Белла–ЛаПадулы. Пример некорректного определения свойств безопасности. Политика low-watermark в модели Белла–ЛаПадулы. Примеры реализации запрещенных информационных потоков. Безопасность переходов |
| 4 | Модели компьютерных систем с ролевым управлением доступом | Понятие ролевого управления доступом. Базовая модель ролевого управления доступом. Модель администрирования ролевого управления доступом. Основные положения. Администрирование множеств авторизованных ролей пользователей. Администрирование множеств прав доступа. Администрирование иерархии ролей. Модель мандатного ролевого управления доступом. Защита от угрозы конфиденциальности информации. Защита от угроз конфиденциальности и целостности информации |
| 5 | Общие сведения о компьютерных вирусах | Что такое компьютерный вирус. Какие бывают вирусы. Кто и зачем пишет вирусы. Общие сведения о методах борьбы с компьютерными вирусами.Классификация компьютерных вирусов. Загрузочные вирусы. Файловые вирусы. Макровирусы. Сетевые и почтовые вирусы и черви. Распространение вирусов. |
| 6 | Борьба с компьютерными вирусами | Обнаружение вирусов. Анализ косвенных признаков. Контрольные суммы. Использование сигнатур для детектирования полиморфных вирусов. Метаморфные вирусы и их детектирование. Эвристические методы детектирования вирусов. Концепция современного антивирусного средства.Борьба с вирусами без использования антивирусов.  |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем | 4 |  | 34 | 2 |
| 2 | Модели компьютерных систем с дискреционным управлением доступом | 4 |  |  | 6 |
| 3 | Модели компьютерных систем с мандатным управлением доступом | 4 |  |  | 8 |
| 4 | Модели компьютерных систем с ролевым управлением доступом | 6 |  |  | 8 |
| 5 | Общие сведения о компьютерных вирусах | 6 |  |  | 8 |
| 6 | Борьба с компьютерными вирусами | 10 |  |  | 8 |
| **Итого** | 34 |  | 34 | 40 |

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

|  |  |  |
| --- | --- | --- |
| **№****п/п** | **Наименование раздела дисциплины** | **Перечень учебно-методического обеспечения** |
| 1 | Основные понятия и определения, используемые при описании моделей безопасности компьютерных систем | Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2013. — 338 с. |
| 2 | Модели компьютерных систем с дискреционным управлением доступом | Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2013. — 338 с. |
| 3 | Модели компьютерных систем с мандатным управлением доступом | Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2013. — 338 с. |
| 4 | Модели компьютерных систем с ролевым управлением доступом | Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2013. — 338 с. |
| 5 | Общие сведения о компьютерных вирусах | Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. — М. : ДМК Пресс, 2013. — 656 с.  |
| 6 | Борьба с компьютерными вирусами | Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. — М. : ДМК Пресс, 2013. — 656 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. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — М. : Горячая линия-Телеком, 2013. — 338 с. — Режим доступа: http://e.lanbook.com/book/63235.

2. Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. — М. : ДМК Пресс, 2013. — 656 с. — Режим доступа: http://e.lanbook.com/book/63192.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

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.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

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

2. ГОСТ Р 51188-98 Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

3. Методические документы. Утверждены ФСТЭК России 14 июня 2012 г. Профили защиты средств антивирусной защиты

8.4 Другие издания, необходимые для освоения дисциплины

1. Моделирование механизма идентификации и аутентификации пользователей компьютерной системы: методические указания к выполнению лабораторных работ по дисциплине "Теоретические основы компьютерной безопасности" / СПб : ФГБОУ ВПО ПГУПС, 2014. - 24 с.

**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 PowerPoint 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 (требования к помещениям в соответствии с ФГОС).
* 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) (требования к помещениям в соответствии с ФГОС).
* помещение для проведения групповых и индивидуальных консультаций (ауд. 2-110) (требования к помещениям в соответствии с ФГОС).
* помещение для проведения текущего контроля и промежуточной аттестации (ауд. 2-110) (требования к помещениям в соответствии с ФГОС).
* помещения для самостоятельной работы (ауд. 2-110) (требования к помещениям в соответствии с ФГОС).



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

|  |
| --- |
| 12.01.2017 г. |

 |  |  |