

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
«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»
(Б1.Б.5)
для направления
09.04.02 «Информационные системы и технологии»
по магистерской программе
«Информационные системы и технологии на транспорте»

Форма обучения – очная

Санкт-Петербург
2018

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена и обсуждена на заседании кафедры
«Информатика и информационная безопасность»
Протокол № 10 от «24» апреля 2018 г.

Заведующий кафедрой «Информатика и
информационная безопасность»
«24» апреля 2018 г.



А. А. Корниенко

СОГЛАСОВАНО

Руководитель магистерской программы
«25» апреля 2018 г.



А. Д. Хомоненко

Председатель методической комиссии
факультета «Автоматизация и
интеллектуальные технологии»
«25» апреля 2018 г.



М. Л. Глухарев

1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «30» октября 2014 г., приказ № 1402 по направлению 09.04.02 «Информационные системы и технологии», по дисциплине «Обеспечение безопасности информационных систем».

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других дисциплин в соответствии с требованиями, установленными федеральным государственным образовательным стандартом для формирования у выпускника общекультурных, общепрофессиональных и профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности (проектно-конструкторская, проектно-технологическая, научно-исследовательская) и магистерской программой «Информационные системы и технологии на транспорте».

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 проведению научно-исследовательской работы;
- развитие социально-воспитательного компонента учебного процесса.

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:

- методы и механизмы обеспечения целостности информации в базах данных;
- методы и механизмы идентификации, аутентификации и авторизации в СУБД;
- механизмы криптографической защиты информации в базах данных;
- методы и механизмы обеспечения доступности информации в системах баз данных.

УМЕТЬ:

- применять программные механизмы реализации требований целостности информации в базах данных;

- применять механизмы идентификации, аутентификации и управления доступом пользователей к СУБД и объектам баз данных;
- применять криптографические средства защиты информации в системах баз данных;
- применять механизмы поддержки доступности информации в системах баз данных;
- применять различные средства администрирования баз данных и СУБД.

ВЛАДЕТЬ:

- навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности;
- навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности.

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):**

- *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);*
- *способность к профессиональной эксплуатации современного оборудования и приборов (ОК-7).*

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

- *способность анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности (ОПК-3);*
- *владение методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях (ОПК-5).*

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

проектно-конструкторская деятельность:

- умение разрабатывать стратегии проектирования, определением целей проектирования, критериев эффективности, ограничений применимости (ПК-1);

проектно-технологическая деятельность:

- умение разрабатывать новые технологии проектирования информационных систем (ПК-3);

научно-исследовательская деятельность:

- способность проводить анализ результатов проведения экспериментов, осуществлять выбор оптимальных решений, подготавливать и составлять обзоры, отчеты и научные публикации (ПК-12).

Область профессиональной деятельности обучающихся, освоивших данную дисциплину, приведена в п. 2.1 общей характеристики ОПОП.

Объекты профессиональной деятельности обучающихся, освоивших данную дисциплину, приведены в п. 2.2 общей характеристики ОПОП.

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Обеспечение безопасности информационных систем» (Б1.Б.5) относится к базовой части и является обязательной дисциплиной.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		1
Контактная работа (по видам учебных занятий)	54	54
В том числе:		
– лекции (Л)	18	18
– практические занятия (ПЗ)	18	18
– лабораторные работы (ЛР)	18	18
Самостоятельная работа (СРС) (всего)	72	72
Контроль	54	54
Форма контроля знаний		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	Введение в дисциплину	Основные понятия дисциплины. Аксиомы защищенных автоматизированных информационных систем (АИС). ГОСТ Р 51583-2014 «Порядок создания автоматизированных систем в защищенном исполнении». Безопасность систем баз данных как одна из важнейших составляющих информационной безопасности АИС. Теоретические основы безопасности систем баз данных.
2	Встроенные механизмы управления доступом в реляционных СУБД	Архитектура подсистемы защиты от НСД в СУБД. Управление учетными записями, пользователями баз данных, ролями и привилегиями в реляционных СУБД на примере Microsoft SQL Server. Разграничение доступа на уровне отдельных строк таблиц.
3	Криптографическая защита информации в реляционных СУБД	Обоснование необходимости криптографической защиты информации в системах баз данных. Архитектура криптографической подсистемы Microsoft SQL Server. Шифрование трафика между клиентом и сервером СУБД. Шифрование данных в БД. Шифрование программных модулей в БД.
4	Поддержка электронной цифровой подписи (ЭЦП) в СУБД	Понятие и назначение ЭЦП. Цели использования ЭЦП в системах БД. Способы формирования и проверки ЭЦП в СУБД Microsoft SQL Server.

5	Реализация требований целостности в реляционных БД	Понятие требований целостности. Виды и примеры требований целостности. Применение формальных описателей для логико-алгебраического моделирования требований целостности. Ограничения целостности. Триггеры. Рекомендации по реализации требований целостности.
6	Методы и механизмы обеспечения доступности информации в СУБД	Резервное копирование и восстановление баз данных. Отказоустойчивый кластер как механизм резервирования серверов СУБД.
7	SQL-инъекции и способы их предотвращения	Понятие SQL-инъекции. Уязвимости программного обеспечения, открывающие возможность осуществления SQL-инъекций. Примеры SQL-инъекций. Способы предотвращения SQL-инъекций.
8	Дополнительные механизмы защиты систем баз данных	Мониторинг событий. Автоматизация выполнения административных задач.
9	Вопросы безопасности распределенных БД	Управление распределенными транзакциями. Двухфазный протокол фиксации распределенных транзакций. Проблемы обеспечения целостности и доступности данных в распределенных БД. Теорема CAP. Репликация как механизм обеспечения высокой доступности. Виды и схемы репликации. Управление доступом в СУРБД.

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1	Введение в дисциплину	2	2	2	8

2	Встроенные механизмы управления доступом в реляционных СУБД	2	2	2	8
3	Криптографическая защита информации в реляционных СУБД	2	2	2	8
4	Поддержка электронной цифровой подписи (ЭЦП) в СУБД	2	2	2	8
5	Реализация требований целостности в реляционных БД	2	2	2	8
6	Методы и механизмы обеспечения доступности информации в СУБД	2	2	2	8
7	Дополнительные механизмы защиты систем баз данных	2	2	2	8
8	SQL-инъекции и способы их предотвращения	2	4	2	8
9	Вопросы безопасности распределенных БД	2	-	2	8
Итого		18	18	18	72

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

№ п/п	Наименование раздела дисциплины	Перечень учебно-методического обеспечения
1	Введение в дисциплину	Документы, входящие в состав комплекса методических материалов дисциплин: – конспект лекций; – методические рекомендации по организации самостоятельной работы обучающихся
2	Встроенные механизмы управления доступом в реляционных СУБД	
3	Криптографическая защита информации в реляционных СУБД	
4	Поддержка электронной цифровой подписи (ЭЦП) в СУБД	
5	Реализация требований целостности в реляционных БД	
6	Методы и механизмы обеспечения доступности информации в СУБД	
7	Дополнительные механизмы защиты систем баз данных	
8	SQL-инъекции и способы их предотвращения	
9	Вопросы безопасности распределенных БД	

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: учебник: / А.А. Корниенко и др.; под ред. А.А. Корниенко. – Ч. 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте –М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. – 448 с.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Глухарев М. Л. Методы и механизмы обеспечения информационной безопасности в СУБД «Microsoft SQL Server»: учеб. пособие по дисциплине «Безопасность систем баз данных» / М. Л. Глухарев. – СПб.: Петербургский государственный университет путей сообщения, 2010. – 46 с.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. ГОСТ Р ИСО/МЭК ТО 10032-2007. Эталонная модель управления данными. – М.: Стандартинформ, 2009.

2. Система управления базой данных. Профиль защиты (первая редакция). - Центр безопасности информации, 2002.

8.4 Другие издания, необходимые для освоения дисциплины

Эрик, Р. Семь баз данных за семь недель. Введение в современные базы данных и идеологию NoSQL [Электронный ресурс] / Р. Эрик, Р.У. Джим.. — Электрон. дан. — Москва : ДМК Пресс, 2013. — 384 с. — Режим доступа: <https://e.lanbook.com/book/58690>.

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/> (для доступа к полнотекстовым документам требуется авторизация).

2. Научно-техническая библиотека университета [Электронный ресурс]. – Режим доступа: <http://library.pgups.ru/> (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:

- персональные компьютеры, локальная вычислительная сеть кафедры, проектор;
- методы обучения с использованием информационных технологий: компьютерный лабораторный практикум, демонстрация мультимедийных материалов;
- 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:

- операционная система Windows, MS Office, Антивирус Касперский;
- SQL Server;
- Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа <https://get.adobe.com/ru/reader/>);
- Microsoft® SQL Server® 2008 Express (бесплатное, свободно распространяемое программное обеспечение; режим доступа <https://www.microsoft.com/ru-ru/download/details.aspx%3Fid%3D1695>);
- 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 данному направлению и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит:

– помещения для проведения лекционных занятий, укомплектованные специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории, демонстрационным оборудованием (настенным или переносным экраном с дистанционным управлением, мультимедийным проектором и другими информационно-демонстрационными средствами) и учебно-наглядными (презентациями), обеспечивающие тематические иллюстрации в соответствии с рабочей программой дисциплины;

– помещения для проведения занятий семинарского типа (практических занятий), укомплектованные специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории;

– помещения для проведения лабораторных работ, укомплектованные лабораторным оборудованием и программным обеспечением в соответствии с перечнем лабораторных работ;

– 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.

Разработчик программы, доцент
«19» апреля 2018 г.

 М. Л. Глухарев