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

«Информационная безопасность» (Б1.В.ОД.9)

для направления

21.03.02 «Землеустройство и кадастры»

профиль «Кадастр недвижимости»

Форма обучения – очная

Санкт-Петербург
2018

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена, обсуждена на заседании кафедры «Информатика и информационная безопасность»
Протокол № 10 от « 24» 04 2018 г.

Заведующий кафедрой «Информатика и информационная безопасность»
«24» 04 2018 г. _____ А.А. Корниенко

СОГЛАСОВАНО

Руководитель ОПОП
«24» 04 2018 г. _____ М.Я. Брынь

Председатель методической комиссии факультета «Транспортное строительство»
«24» 04 2018 г. _____ О.Б. Суровцева

1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «01» октября 2015 г., приказ № 1084 по направлению 21.03.02 «Землеустройство и кадастры», по дисциплине «Информационная безопасность».

Целью изучения дисциплины является ознакомление студентов с теорией защиты информации, а также с современными методами и средствами защиты информации в компьютерных системах и сетях.

Для достижения поставленной цели решаются следующие задачи:

– знакомство с нормативно-правовыми актами международного, федерального и ведомственного уровня, определяющих организационные и правовые аспекты в области информационной безопасности (ИБ);

– изучение основных понятий и принципов защиты информации;

– изучение криптографических методов защиты информации;

– изучение программных и программно-аппаратных средств защиты операционных систем, компьютерных сетей и баз данных;

– изучение методов и инструментов защиты программного обеспечения от разрушающих программных воздействий.

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:

– основы российской правовой системы и законодательства;

– характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ;

– сущность и понятие информации, информационной

– безопасности и характеристику ее составляющих;

– место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;

– правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;

– источники и классификацию угроз информационной безопасности;

– основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

– основные задачи и понятия криптографии;

– требования к шифрам и основные характеристики шифров;

– типовые поточные и блочные шифры;

– частотные характеристики открытых текстов и способы их применения к анализу простейших шифров замены и перестановки;

– типовые шифры с открытыми ключами;

– программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях.

УМЕТЬ:

– использовать в практической деятельности правовые знания;

– анализировать правовые акты и осуществлять правовую оценку информации;

– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

– классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;

– эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах;

– применять средства обеспечения безопасности данных.

ВЛАДЕТЬ:

– навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;

– навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;

– навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности;

– навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;

– навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей;

– навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

Изучение дисциплины направлено на формирование следующих

общепрофессиональных компетенций (ОПК):

– способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий (ОПК-1);

производственно-технологическая деятельность (ПК):

– способность использовать знание современных технологий сбора, систематизации, обработки и учёта информации об объектах недвижимости современных геофизических и земельно-информационных системах (ПК-8).

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 «Информационная безопасность» (Б1.В.ОД.9) относится к вариативной части и является обязательной дисциплиной обучающегося.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		5
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	32 16 16	32 16 16
Самостоятельная работа (СРС) (всего)	31	31
Контроль	9	9
Форма контроля знаний	З	З
Общая трудоемкость: час / з.е.	72/2	72/2

Примечание: «Форма контроля знаний» – зачет.

5. Содержание и структура дисциплины

5.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Введение в дисциплину	Понятие информации; свойства; классификация; единицы измерения информации; обобщённая структурно-функциональная схема информационной системы; понятие информационной безопасности
2	Законодательство Российской Федерации в области информационной безопасности	Правовые акты общего назначения, затрагивающие вопросы информационной безопасности; Федеральные законы: «О государственной тайне», «Об информации, информационных технологиях и о защите информации»; зарубежное законодательство в области информационной безопасности

3	Угрозы безопасности информации в информационных системах	Случайные угрозы; преднамеренные угроз; классификация злоумышленников
4	Защита информации в информационных системах от случайных угроз	Дублирование информации; повышение надёжности информационных систем; создание отказоустойчивых информационных систем; блокировка ошибочных операций; оптимизация взаимодействия пользователей и обслуживающего персонала с информационной системой; минимизация ущерба от аварий и стихийных бедствий
5	Методы и средства защиты информации в информационных системах от традиционного шпионажа и диверсий	Система охраны объекта с информационной системой; организация работ с конфиденциальными информационными ресурсами на объектах с информационной системой; противодействие наблюдению в оптическом диапазоне; противодействие подслушиванию; средства борьбы с закладными подслушивающими устройствами; защита от злоумышленных действий обслуживающего персонала и пользователей
6	Защита информации в информационных системах от несанкционированного доступа	Система разграничения доступа к информации в информационной системе; система защиты программных средств от копирования и исследования
7	Методы защиты от несанкционированного изменения структур информационных систем	Общие требования к защищённости информационной системы от несанкционированного изменения структур; защита от закладок при разработке программ; защита от внедрения аппаратных закладок на этапе разработки и производства; защита от несанкционированного изменения структур информационных систем в процессе эксплуатации
8	Меры и средства защиты информации в информационных системах от утечки по техническим каналам	Пассивные меры защиты информации в информационных системах от утечки по техническим каналам Активные меры защиты информации в информационных системах от утечки по техническим каналам

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1	Введение в дисциплину	2	-	-	3

2	Законодательство Российской Федерации в области информационной безопасности	2	-	4	4
3	Угрозы безопасности информации в информационных системах	2	-	-	4
4	Защита информации в информационных системах от случайных угроз	2	-	4	4
5	Методы и средства защиты информации в информационных системах от традиционного шпионажа и диверсий	2	-	4	4
6	Защита информации в информационных системах от несанкционированного доступа	2	-	4	4
7	Методы защиты от несанкционированного изменения структур информационных систем	2	-	-	4
8	Меры и средства защиты информации в информационных системах от утечки по техническим каналам	2	-	-	4
Итого		16	-	16	31

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

№ п/п	Наименование раздела дисциплины	Перечень учебно-методического обеспечения
1	Введение в дисциплину	В.А. Тихонов, В.В. Райх Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие / В.А. Тихонов. – М.: Гелиос АРВ, 2012 – 528 с. Н.В. Иванова Информационная безопасность систем электронного документооборота / Н.В. Иванова. – СПб.: ПГУПС, 2011. – 282с.
2	Законодательство Российской Федерации в области информационной безопасности	Правовой сервер КонсультантПлюс [Электронный ресурс]. – М.: ЗАО «КонсультантПлюс», 2003. – Режим доступа : http://consultant.ru, свободный. – Загл. с экрана. А.А. Корниенко, М.А. Поляничко Стандарты информационной безопасности / А.А. Корниенко. – СПб.: ПГУПС, 2012. – 93 с.
3	Угрозы безопасности информации в информационных системах	А.А. Бирюков Информационная без-

4	Защита информации в информационных системах от случайных угроз	опасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. – М.: ДМК Пресс, 2012. ISBN 978-5-94074-647-8 М.М. Глухов [и др.] Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учеб. пособие / М.М. Глухов [и др.]. – М. : Лань, 2011. – 394 с. А.М. Перепеченов Основы проектирования защищенных информационных систем / А.М. Перепеченов. – СПб.: ПГУПС, 2013. – 59 с. В.И. Васильев Интеллектуальные системы защиты информации [Электронный ресурс] / В. И. Васильев. – М. : Машиностроение, 2013. – 171 с. О.Ю. Коробулина Риск-модели информационной безопасности / Коробулина О.Ю. – СПб.: ПГУПС, 2014. – 26 с.
5	Методы и средства защиты информации в информационных системах от традиционного шпионажа и диверсий	
6	Защита информации в информационных системах от несанкционированного доступа	
7	Методы защиты от несанкционированного изменения структур информационных систем	
8	Меры и средства защиты информации в информационных системах от утечки по техническим каналам	

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. – 439 с. (24 экз., ККО 1,26) id=59240 «Лань»
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 1,26) id=59241 «Лань»

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Н.В. Иванова Информационная безопасность систем электронного документооборота / Н.В. Иванова. – СПб: ПГУПС, 2011. – 282с.;
2. В.И. Васильев Интеллектуальные системы защиты информации [Электронный ресурс] / В. И. Васильев. – М.: Машиностроение, 2013. – 171 с.; id=5792 «Лань»
3. А.М. Перепеченов Основы проектирования защищенных информационных систем / А.М. Перепеченов. – СПб: ПГУПС, 2013. – 59 с. id=41119 «Лань»

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»
2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования.
3. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

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/
4. Личный кабинет обучающегося и электронная информационно-образовательная среда. [Электронный ресурс]. – Режим доступа: http://sdo.pgups.ru/ (для доступа к полнотекстовым документам требуется авторизация).
5. Электронно-библиотечная система ЛАНЬ [Электронный ресурс]. Режим доступа: https://e.lanbook.com — Загл. с экрана.

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;

– лабораторное программное обеспечение, разрабатываемое в ходе учебного процесса студентами совместно с преподавателем;

– 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.

– электронная информационно-образовательная среда Петербургского государственного университета путей сообщения Императора Александра I [Электронный ресурс]. – Режим доступа: http://sdo/pgups.ru.

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

– Microsoft Windows 7;

– Office Standard 2010 Russian OpenLicensePack NoLevel AcademicEdition;

– Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://get.adobe.com/ru/reader/);

– Visual Studio Professional 2010 Russian OLP NL AcademicEdition;

– 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 данной специальности, и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит специальные помещения, укомплектованных специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Материально-техническая база дисциплины включает:

– помещения для проведения лекционных занятий, укомплектованные наборами демонстрационного оборудования (стационарными или переносными персональными компьютерами, настенными или переносными экранами, мультимедийными проекторами с дистанционным управлением и другими информационно-демонстрационными средствами) и учебно-наглядными пособиями (презентациями), обеспечивающими тематические иллюстрации в соответствии с рабочей программой дисциплины;

– лабораторию информационной безопасности информационно-коммуникационных систем (ауд. 2-104), оснащенную программно-аппаратными средствами защиты информации в соответствии с требованиями ФГОС ВО; лаборатория также оборудована современной вычислительной техникой, комплектом проекционного оборудования для преподавателя;

– помещения для выполнения курсовой работы, оснащенные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых для выполнения индивидуального задания программных средств (см. раздел 11), а также комплектом оборудования для печати;

– 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 _____ А.М. Перепеченов

«24» апреля 2018 г.