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.ДВ.5.2)

для направления

38.03.02 «Менеджмент»

по профилю

«Производственный менеджмент»

Форма обучения – очная

Санкт-Петербург
2018

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена, 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

Председатель методической комиссии факультета «Экономика и менеджмент»
«25» апреля 2018 г. _____ Н. Е. Коклева

Руководитель ОПОП
«24» апреля 2018 г. _____ Н. А. Журавлева

1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «12» января 2016 г., приказ № 7 по направлению 38.03.02 «Менеджмент», по дисциплине «Информационная безопасность».

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 общепрофессиональных и профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности (организационно-управленческая, информационно-аналитическая, предпринимательская) и профилем «Производственный менеджмент».

Для достижения поставленной цели решаются следующие задачи:

- подготовка студента по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
- 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 является приобретение знаний, умений и навыков.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

- основные понятия в области информационной безопасности и кибербезопасности;
- 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, сведения о современных криптографических средствах защиты информации;
- сведения о программно-аппаратных средствах обеспечения информационной безопасности в операционных системах, системах управления базами данных, компьютерных сетях.

УМЕТЬ:

- идентифицировать угрозы информационной безопасности, действующие на информационные системы;
- идентифицировать уязвимости информационных систем;
- оценивать состояние защищенности объектов информатизации на железнодорожном транспорте;
- эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах.

ВЛАДЕТЬ:

- технологией построения моделей угроз информационных систем;
- навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем.

Приобретенные знания, умения и навыки, характеризующие формирование компетенций, осваиваемые в данной дисциплине, позволяют решать профессиональные задачи, приведенные в соответствующем перечне по видам профессиональной деятельности в п. 2.4 общей характеристики основной профессиональной образовательной программы (ОПОП).

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

- *владение навыками поиска, анализа и использования нормативных и правовых документов в своей профессиональной деятельности* (ОПК-1).

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

информационно-аналитическая деятельность:

– способность оценивать воздействие макроэкономической среды на функционирование организаций и органов государственного и муниципального управления, выявлять и анализировать рыночные и специфические риски, а также анализировать поведение потребителей экономических благ и формирование спроса на основе знания экономических основ поведения организаций, структур рынков и конкурентной среды отрасли (ПК-9).

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 «Информационная безопасность» (Б1.В.ДВ.5.2) относится к вариативной части и является дисциплиной по выбору обучающегося.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		7
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ)	64 32 32	64 32 32
Самостоятельная работа (СРС) (всего)	31	31
Контроль	9	9
Форма контроля знаний	зачет	зачет
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	Введение в дисциплину	Основные понятия и определения дисциплины. Цели и задачи обеспечения информационной безопасности на железнодорожном транспорте.
2	Правовые методы обеспечения информационной безопасности	Государственная система защиты информации в Российской Федерации. Организационная структура государственной системы защиты информации в Российской Федерации (ОАО РЖД). Функции и задачи Федеральной службы по техническому и экспортному контролю. Информационная

		безопасность в системе национальной безопасности. Обзор и краткое содержание законов и национальных стандартов Российской Федерации и международных стандартов в области информационной безопасности.
3	Угрозы информационной безопасности на железнодорожном транспорте	Активы организации. Уязвимости информационных систем. Источники угроз. Классификация угроз. Модель нарушителя информационной безопасности.
4	Менеджмент информационной безопасности	Политика безопасности: порядок разработки, реализация, пересмотр. Построение модели угроз информационной безопасности объекта информатизации. Правила разграничения доступа к ресурсам системы. Управление информационной безопасностью в ОАО РЖД. Меры по обеспечению безопасности государственных информационных систем.
5	Криптографические методы защиты информации	Основные термины и определения криптографии. Классификация криптосистем. Симметричные криптосистемы. Асимметричные криптосистемы. Инфраструктура открытых ключей.
6	Программно-аппаратные методы и средства защиты информации в автоматизированных информационных системах	Средства идентификации и аутентификации. Механизмы управления доступом. Проблема повторного использования объектов и способы ее решения. Средства обеспечения целостности и доступности информации в автоматизированных информационных системах.
7	Безопасность компьютерных сетей	Межсетевое экранирование. Виртуальные защищенные сети.
8	Методы и механизмы обеспечения информационной безопасности в системах баз данных	Средства управления транзакциями. Механизмы обеспечения целостности информации в базах данных. Механизмы управления доступом. Средства криптографической защиты информации. Средства резервирования.
9	Заключение	Анализ перспектив развития методов и средств обеспечения информационной безопасности.

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1	2	3	4	5	6
1	Введение в дисциплину	4	-		8
2	Правовые методы обеспечения информационной безопасности	4	4		8
3	Угрозы информационной безопасности на железнодорожном транспорте	2	4		8
4	Менеджмент информационной безопасности	2	4		8
5	Криптографические методы защиты информации	4	8		8
6	Программно-аппаратные методы и средства защиты информации в автоматизированных информационных системах	4	4		8
7	Безопасность компьютерных сетей	4	4		8
8	Методы и механизмы обеспечения информационной безопасности в системах баз данных	4	4		8
9	Заключение	4	-		7
Итого		32	32	-	71

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

№ п/п	Наименование раздела	Перечень учебно-методического обеспечения
1	Введение в дисциплину	1. Информационная безопасность и защита информации на железнодорожном транспорте: учебник: / С.Е. Ададуров и др.; под ред. А.А. Корниенко. – Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте –
2	Правовые методы обеспечения информационной	

	безопасности	М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. – 440 с. 2. 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. 3. Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс]: Учебные пособия — Электрон. дан. — М.: ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/book/50578.
3	Угрозы информационной безопасности на железнодорожном транспорте	
4	Менеджмент информационной безопасности	
5	Криптографические методы защиты информации	
6	Программно-аппаратные методы и средства защиты информации в автоматизированных информационных системах	
7	Безопасность компьютерных сетей	
8	Методы и механизмы обеспечения информационной безопасности в системах баз данных	
9	Заключение	

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-х частях. Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. [Электронный ресурс] — Электрон.дан. — М.: УМЦ ЖДТ, 2014. — 440 с. — Режим доступа: http://e.lanbook.com/book/59240.

2. Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. [Электронный ресурс] — Электрон.дан. — М.: УМЦ ЖДТ, 2014. — 448 с. — Режим доступа: http://e.lanbook.com/book/59241.

3. Шаньгин В.Ф. Информационная безопасность. [Электронный ресурс] — Электрон.дан. — М.: ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/book/50578.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Яковлев В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта. [Электронный ресурс] / В.В. Яковлев, А.А. Корниенко. — Электрон.дан. — М.: УМЦ ЖДТ, 2002. — 328 с. — Режим доступа: http://e.lanbook.com/book/59172.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М.: Стандартинформ, 2012. – 33 с.

2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. – М.: Стандартинформ, 2012. – 38 с.

3. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 25 с.

4. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 42 с.

8.4 Другие издания, необходимые для освоения дисциплины

При изучении 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/ (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.

4. Официальный сайт электронной библиотечной системы «Лань» [Электронный ресурс]. – Режим доступа: http://e.lanbook.com (для доступа к полнотекстовым документам требуется авторизация).

5. Электронная библиотека «Единое окно к образовательным ресурсам». Режим доступа: http://window.edu.ru. – свободный.

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 и навыков, 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);
- методы обучения с использованием информационных технологий (демонстрация мультимедийных материалов, компьютерный лабораторный практикум);
- Интернет-сервисы и электронные ресурсы, перечисленные в разделе 9, в том числе личный кабинет обучающегося и электронная информационно-образовательная среда (Режим доступа: http://sdo.pgups.ru/).

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

- операционная система Windows, MS Office, Антивирус Касперский;
- Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://get.adobe.com/ru/reader/);
- Oracle Java SE Development Kit 8 (бесплатное, свободно распространяемое программное обеспечение; режим доступа http://www.oracle.com/technetwork/java/javase/downloads/index.html)

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.

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 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