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
38.03.05 «Бизнес-информатика»
по профилю
«Архитектура предприятия»

Форма обучения – очная

Санкт-Петербург
2018

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена и обсуждена на заседании кафедры А.А. Корниенко
«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 «Промышленное и гражданское строительство»
«25» апреля 2018 г. Р.С. Кударов

Руководитель ОПОП
«25» апреля 2018 г. В.А. Ходаковский

1. Цели и задачи дисциплины

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «11» августа 2016 г., приказ № 1002 по направлению 38.03.05 «Бизнес-информатика», по дисциплине «Информационная безопасность».

Целью изучения дисциплины является формирование у обучающегося компетенций в соответствии с учебным планом за счет освоения теоретических основ информационной безопасности автоматизированных систем.

Для достижения поставленной цели решаются следующие задачи:

– формирование у обучающихся понятийного аппарата в области защиты информации и информационной безопасности;

– освоение обучающимисяметодики определения актуальных угроз информационной безопасности;

– формирование у обучающихся начальных навыков построения модели угроз безопасности и неформальной модели нарушителя;

– формирование у обучающихся представлений о методах защиты информации в автоматизированных информационно-управляющих системах.

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.

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ:

- сущность и понятие информации, информационной безопасности и кибербезопасности, свойства защищенности информации;
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;
- цели и задачи в области обеспечения информационной безопасности на железнодорожном транспорте;
- 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;

- программно-аппаратные средства обеспечения информационной безопасности в автоматизированных информационных системах, системах управления базами данных, компьютерных сетях.

УМЕТЬ:

- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- выявлять актуальные угрозы информационной безопасности;
- планировать мероприятия по обеспечению информационной безопасности в организации;
- применять средства обеспечения безопасности данных.

ВЛАДЕТЬ:

- навыками своевременного и точного выявления актуальных угроз информационной безопасности объекта информатизации.

Приобретенные знания, умения, 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 **профессиональных компетенций (ОПК)**:

- способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1).

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

организационно-управленческая деятельность:

- организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия (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.ОД.9) относится к вариативной части образовательной программы и является обязательнойдля изучения.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		2
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	50 16 34	50 16 34
Самостоятельная работа (СРС) (всего)	85	85
Контроль	9	9
Форма контроля знаний		зачет, курсовой проект
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	Общие сведения об информационной безопасности и кибербезопасности	1.1 Ключевые термины и определения Информация как объект защиты. Понятие информационной безопасности корпоративных информационных систем и сетей. Конфиденциальность, целостность и доступность информации как аспекты информационной безопасности. 1.2. Понятие кибербезопасности. Общие факторы кибербезопасности. 1.3. Информационная

		безопасность современного общества. Нормативно-правовые аспекты информационной безопасности. 1.4. Цели и задачи обеспечения информационной безопасности на железнодорожном транспорте.
2	Уязвимости информационных систем и угрозы информационной безопасности	Понятия угрозы и уязвимости. Окно опасности. 2.1. Виды уязвимостей АИС 2.2. Классификация угроз и их источников. 2.3. Методика определения актуальных угроз безопасности. 2.4. Модель угроз и модель нарушителя.
3	Обзор криптографических методов защиты информации	3.1. Виды криптографического преобразования информации 3.2. Модель симметричной криптосистемы. Подклассы симметричных криптосистем. 3.3. Системы открытого шифрования. 3.4. Системы цифровой подписи.
4	Обеспечение информационной безопасности информационных систем	4.1. Средства идентификации и аутентификации. 4.2. Модели доступа и механизмы управления доступом. 4.3. Средства обеспечения целостности и доступности информации в операционных системах.
5	Методы и механизмы обеспечения информационной безопасности в системах баз данных	5.1. Методы предотвращения конфликтов транзакций в многопользовательском режиме. 5.2. Механизмы обеспечения целостности информации в базах данных. 5.3. Реализация ролевой модели доступа в СУБД на примере SQLServer. 5.4. Криптографическая защита информации. 5.5. Средства резервирования.

6	Безопасность компьютерных сетей	6.1. Межсетевое экранирование. 6.2. Виртуальные защищенные сети. 6.3. Системы обнаружения вторжений
7	Защита от разрушающих программных воздействий	7.1. Понятие разрушающего программного воздействия (РПВ). Классификация вредоносного программного обеспечения. 7.2. Методы и средства антивирусной защиты. 7.3. Методы и средства выявления программных закладок. 7.4. Запуск доверенных приложений под политикой безопасности.

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС
1	Общие сведения об информационной безопасности и кибербезопасности	2	4	-	7
2	Уязвимости информационных систем и угрозы информационной безопасности	4	10	-	52
3	Обзор криптографических методов защиты информации	2	4	-	7
4	Обеспечение информационной безопасности информационных систем	2	4	-	7
5	Методы и механизмы обеспечения информационной безопасности в системах баз данных	2	4	-	7
6	Безопасность компьютерных сетей	2	4	-	7
7	Защита от разрушающих программных воздействий	2	4	-	7
Итого		16	34	-	94

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

№ п/п	Наименование раздела дисциплины	Перечень учебно-методического обеспечения
1	Общие сведения об информационной безопасности и кибербезопасности	1. Основная и дополнительная литература, нормативные документы – см. раздел 8. 2. Ресурсы ИТКС «Интернет» - см. раздел 9. 3. Электронные методические материалы, доступные обучающимся через личный кабинет на сайте Университета
2	Уязвимости информационных систем и угрозы информационной безопасности	
3	Обзор криптографических методов защиты информации	
4	Обеспечение информационной безопасности информационных систем	
5	Методы и механизмы обеспечения информационной безопасности в системах баз данных	
6	Безопасность компьютерных сетей	
7	Защита от разрушающих программных воздействий	

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. Конституция Российской Федерации [Электронный ресурс] –Режим доступа: http://www.constitution.ru.

2. Доктрина информационной безопасности Российской Федерации[Электронный ресурс] –Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

3. Федеральный закон от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации[Электронный ресурс] –Режим доступа: https://rg.ru/2006/07/29/informacia-dok.html.

4. Закон о государственной тайне [Электронный ресурс] –Режим доступа:http://www.consultant.ru/document/cons_doc_LAW_2481/

5. Федеральный закон от 29 июля 2004 г. N 98-ФЗ О коммерческой тайне[Электронный ресурс] –Режим доступа: https://rg.ru/2004/08/05/taina-doc.html

6. Федеральный закон от 27 июля 2006 г. N 152-ФЗ О персональных данных[Электронный ресурс] –Режим доступа: https://rg.ru/2006/07/29/personaljnye-dannye-dok.html

7. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"[Электронный ресурс] –Режим доступа: https://rg.ru/2011/04/08/podpis-dok.html

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

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

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

11. 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. Раздел «Безопасность» на сайте www.citforum.ru.
2. Бесплатные курсы по тематике информационной безопасности на портале www.intuit.ru.
3. Информационно-аналитический портал www.anti-malware.ru.
4. Информационно-аналитический портал www.securitylab.ru.
5. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: (http://fstec.ru/).
6. Электронный фонд нормативно-правовой документации. [Электронный ресурс] - Режим доступа: (http://docs.cntd.ru/search/intellectual?q=%D0%93%D0%9E%D0%A1%D0%A2+%D0%A0+56205-2014+&itemtype;
7. Официальный сайт информационной сети ТЕХЭКСПЕРТ [Электронный ресурс] - Режим доступа: *http://www.cntd.ru/*, свободный.
8. Официальный сайт технического комитета по разработке ГОСТов по информационной безопасности - [Электронный ресурс] - Режим доступа: (http://tk.gost.ru/wps/portal/tk362).
9. 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, 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:

- Интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, онлайн-энциклопедии и справочники, электронные учебные и учебно-методические материалы).
- электронная информационно-образовательная среда Петербургского государственного университета путей сообщения Императора Александра I [Электронный ресурс]. Режим доступа: http://sdo.pgups.ru.

Дисциплина обеспечена необходимым комплектом лицензионного программного обеспечения, установленного на технических средствах, размещенных в специальных помещениях и помещениях для самостоятельной работы: операционная система Windows, MS Office, AdobeAcrobatReaderDC (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://get.adobe.com/ru/reader/).

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—направлению 38.03.05 и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит специальные помещения - учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения на семестр учебного года выделяются в соответствии с расписанием занятий.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (мультимедийным проектором, экраном, либо свободным участком стены ровного светлого тона размером не менее 2х1.5 метра, стандартной доской для работы с маркером). В случае отсутствия стационарной установки аудитория оснащена розетками электропитания для подключения переносного комплекта мультимедийной аппаратуры и экраном (либо свободным участком стены ровного светлого тона размером не менее 2х1.5 метра).

Для проведения занятий лекционного типа предлагаются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации, соответствующие рабочей учебной программе дисциплины.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Разработчик программы, доцент М. Л. Глухарев

«20» апреля 2018 г.