

УТВЕРЖДАЮ

Первый проректор, проректор по
УР

_____ А.Е. Рудин

«30» июня 2020 года

Рабочая программа дисциплины

Б1.В.ДВ.03.02 Лицензирование и сертификация в области защиты информации

Учебный план: ФГОС 3++_2020-2021_09.03.03_ИИТА_ОО_ПИЭ.рлх

Кафедра: **20** Интеллектуальных систем и защиты информации

Направление подготовки:
(специальность) 09.03.03 Прикладная информатика

Профиль подготовки: Прикладная информатика в экономике
(специализация)

Уровень образования: бакалавриат

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)	Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
	Лекции	Практ. занятия				
7	УП	17	73,75	0,25	3	Зачет
	РПД	17	73,75	0,25	3	
Итого	УП	17	73,75	0,25	3	
	РПД	17	73,75	0,25	3	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 Прикладная информатика, утверждённым приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 922

Составитель (и):

кандидат технических наук, Доцент

Штеренберг Станислав
Игоревич

От кафедры составителя:

Заведующий кафедрой интеллектуальных систем и
защиты информации

Макаров Авинир
Геннадьевич

От выпускающей кафедры:

Заведующий кафедрой

Пименов Виктор
Игоревич

Методический отдел:

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: В результате изучения профессионального модуля студент должен освоить вид деятельности лицензирование и сертификация в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции.

1.2 Задачи дисциплины:

Иметь практический опыт:

- установки, настройки программных средств защиты информации в автоматизированной системе;
- обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;
- решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;
- применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;
- учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

1.3 Требования к предварительной подготовке обучающегося:

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

Сертификация информационных систем и технологий

Учебная практика (научно-исследовательская работа (получение первичных навыков научно-исследовательской работы))

Учебная практика (технологическая (проектно-технологическая) практика))

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПКп-4 : Способен составлять технико-экономическое обоснование проектных решений и техническое задание на разработку информационной системы
Знать: Правовые, нормативно-технические и организационные основы лицензирования и сертификации в области защиты информации
Уметь: Использовать правовые акты при проведении лицензирования и сертификации программных продуктов
Владеть: Навыками поиска научно-технической, методической и нормативной информации, необходимой для подачи заявки на лицензирование и сертификацию

3 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Инновац. формы занятий	Форма текущего контроля
		Лек. (часы)	Пр. (часы)			
Раздел 1. Сертификация ФСТЭК и ФСБ	7					О
Тема 1. Прохождение сертификации ФСТЭК		2	2	5	Т	
Тема 2. Прохождение сертификации ФСБ		2	2	5	Т	
Раздел 2. Применение программных и программно-аппаратных средств защиты информации						О,Р
Тема 3. Применение криптографических средств защиты информации		2	2	7	ГД	
Тема 4. Классификация методов и средств программно-аппаратной защиты информации		2	2	10	ИЛ	
Раздел 3. Стандарты безопасности						

Тема 5. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	1	1	1,75	НИ	
Тема 6. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2	1	5	НИ	
Раздел 4. Защищенная автоматизированная система					
Тема 7. Особенности автоматизированных систем в	3	3	20	АС	К,ДЗ
Тема 8. Методология проектирования гарантированно защищенных КС	3	4	20	НИ	
Итого в семестре (на курсе для ЗАО)	17	17	73,75		
Консультации и промежуточная аттестация (Зачет)	0,25				
Всего контактная работа и СР по дисциплине	34,25		73,75		

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1 Описание показателей, критериев и системы оценивания результатов обучения

5.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения	Наименование оценочного средства
ПКп-4	<ul style="list-style-type: none"> -Объясняет принципы защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. -Осуществляет установку и настройку отдельных программных, программно-аппаратных средств защиты информации; обеспечивает защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. -Осуществляет тестирование функций отдельных программных и программно-аппаратных средств защиты информации, осуществляет обработку, хранение и передачу информации ограниченного доступа. -Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств; осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. 	<p>Вопросы для устного собеседования</p> <p>Тестовые задания</p> <p>Практико-ориентированные задания</p>

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа

Зачтено	<p>Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу.</p> <p>Учитываются баллы, накопленные в течение семестра. Критическое и разностороннее рассмотрение вопросов, свидетельствующее о значительной самостоятельной работе с источниками. Качество исполнения всех элементов задания полностью соответствует всем требованиям.</p> <p>Учитываются баллы, накопленные в течение семестра.</p>	
Не зачтено	<p>Попытка списывания или пользования подсказкой другого человека (вне зависимости от успешности такой попытки).</p> <p>Не учитываются баллы, накопленные в течение семестра.</p>	

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

5.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
Семестр 7	
1	Защита информации - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.
2	Средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.
3	Эффективность защиты информации - степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.
4	Контроль эффективности защиты информации - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.
5	Безопасность информации (информационная безопасность) - состояние информации, информационных ресурсов и информационных и телекоммуникационных систем, при котором с требуемой вероятностью обеспечивается защита информации.
6	Требования по безопасности информации - руководящие документы ФАПСИ, регламентирующие качественные и количественные критерии безопасности информации и нормы эффективности ее защиты.
7	Криптографическая защита - защита данных при помощи криптографического преобразования преобразования данных.
8	Криптографическое преобразование - преобразование данных при помощи шифрования и (или) выработки имитовставки.
9	Шифр - совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.
10	Маскиратор - средство защиты информации, реализующее математический алгоритм преобразования информации, не использующее секретного ключа или передающее (хранящее) его вместе с сообщением.
11	Скремблер - шифровальное средство, предназначенное для защиты информации только от непосредственного прослушивания, просмотра или прочтения.
12	Защищенные (закрытые) системы и комплексы телекоммуникаций - системы и комплексы телекоммуникаций, в которых обеспечивается защита информации с использованием шифровальных средств, защищенного оборудования и организационных мер.
13	Техническое средство обработки информации - техническое средство, предназначенное для приема, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи.

5.2.2 Типовые тестовые задания

Виды работ:

- Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах
- Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности
- Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности
- Составление документации по учету, обработке, хранению и передаче конфиденциальной информации
- Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации
- Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.
- Устранение замечаний по результатам проверки
- Анализ и составление нормативных методических документов по обеспечению информационной безопасности программноаппаратными средствами, с учетом нормативных правовых актов.
- Применение математических методов для оценки качества и выбора наилучшего программного средства

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

Виды работ

- Анализ принципов построения систем информационной защиты производственных подразделений.
- Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.
- Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;
- Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении
- Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации
- Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.

5.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

5.3.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная Письменная Компьютерное тестирование Иная

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Учащийся может выполнять следующие действия с использованием корпоративных систем корпоративного класса (Virtual Private Network):

Развёртывание, настройка и проверка работоспособности сети на существующей и вычислительной инфраструктуре.

Администрирование узлов и пользователей.

Внедрение централизованных политик безопасности. Обеспечение защиты рабочих мест.

При выполнении заданий необходимо:

Настроить СУБД и БД

Развернуть структуру защищенной сети согласно схеме с помощью дистрибутивов

Произвести настройку пользователей и узлов защищенной сети

Составить отчет о работе

При работе могут использоваться различные операционные системы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				

Басыня, Е. А.	Системное администрирование и информационная безопасность	Новосибирск: Новосибирский государственный технический университет	2018	http://www.iprbookshop.ru/91423.html
Фомин, Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства	Саратов: Вузовское образование	2018	http://www.iprbookshop.ru/77317.html
Петров, С. В., Кисляков, П. А.	Информационная безопасность	Саратов: Ай Пи Ар Букс	2015	http://www.iprbookshop.ru/33857.html
6.1.2 Дополнительная учебная литература				
Кикин А. Б.	Информационная безопасность	СПб.: СПбГУПТД	2015	http://publish.sutd.ru/tp_ext_inf_publish.php?id=2809
Смышляев, А. Г.	Информационная безопасность. Лабораторный практикум	Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, ЭБС АСВ	2015	http://www.iprbookshop.ru/66655.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

ЭБС iBooks (<https://ibooks.ru>)

ЭБС Лань (<https://e.lanbook.com/>)

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft Windows

MicrosoftOfficeProfessional

1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Продажа по договору с учебными заведениями об использовании в учебном процессе по заявкам

СПС КонсультантПлюс

6.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория	Оснащение
Лекционная аудитория	Мультимедийное оборудование, специализированная мебель, доска
Учебная аудитория	Специализированная мебель, доска