МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Тверской государственный технический университет»
(ТвГТУ)

УТВЕРЖДАЮ
Проректор по учебной работе
_____М.А. Смирнов
« ___ » _____ 20__ г.

РАБОЧАЯ ПРОГРАММА

Дисциплины общепрофессионального цикла
Основы информационной безопасности

Форма обучения – очная
Специальность: 09.02.12 Техническая эксплуатация и сопровождение информационных систем

Кафедра «Информационные системы»

Тверь 202__

Рабочая программа дисциплины предназначена для подготовки студентов среднего профессионального образования и соответствует ОХОП подготовки специалистов среднего звена на базе основного общего образования в части требований к результатам обучения по профессии учебному плану.

Разработчик программы:
доцент кафедры ИС В.В. Алексеев

Программа рассмотрена и одобрена на заседании кафедры ИС
«____» _____ 20__г., протокол № ____.

Заведующий кафедрой Б.В. Палюх

Согласовано:
Начальник учебно-методического
отдела УМУ Е.Э. Наумова

Начальник отдела
комплектования
зональной научной библиотеки О.Ф. Жмыхова

1. Общая характеристика рабочей программы дисциплины общепрофессионального цикла

1.1 Место дисциплины в структуре основной образовательной программы СПО

Дисциплина общепрофессионального цикла ОП.06 Основы информационной безопасности является обязательной частью профессионального цикла образовательной программы СПО в соответствии с ФГОС по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем, срок обучения – 2 года 10 месяцев.

1.2. Цели и планируемые результаты освоения дисциплины

Задачами дисциплины являются:

Формирование системы знаний и умений по основным положениям теории информационной безопасности информационных систем и основных технологий построения защищенных информационных систем;

овладение навыками применения основных моделей безопасности и построения защищенных информационных систем.

Цель дисциплины ОП.06 Основы информационной безопасности: изучение теоретических и практических основ обеспечения безопасности информации в современных информационных системах.

Планируемые результаты освоения общеобразовательной дисциплины в соответствии с ФГОС СПО и на основе ФГОС СОО. Особое значение дисциплина имеет при формировании и развитии ОК 1, ОК 2, ПК 1.1, ПК 1.4, ПК 1.5, ПК 1.6, ПК 1.7, ПК 4.2, ПК 4.4, ПК 4.5.

Планируемые результаты освоения дисциплины в соответствии с ФГОС СПО.

Таблица 1. Планируемые результаты освоения дисциплины

Код и наименование формируемых компетенций	Практический опыт	Умения	Знания
ОК 1, ОК 2, ПК 1.1, ПК 1.4, ПК 1.5, ПК 1.6, ПК 1.7, ПК 4.2, ПК 4.4, ПК 4.5	Распознавания инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Передачи информации об инцидентах в	распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части; определять этапы решения задачи, составлять план действия,	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; основные источники информации и ресурсы для

	службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Информирования заинтересованных лиц заказчика и в своей организации об инцидентах ИБ, связанных с работой ИС, для принятия управленческих решений, минимизирующих ущерб от инцидента ИБ, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Временного блокирования доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Распознавания инцидентов ИБ при работе с БД; Формирования перечня инцидентов ИБ; Передачи информации об инцидентах в службу ИБ организации; Временного блокирования	реализовывать составленный план, определять необходимые ресурсы; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; владеть актуальными методами работы в профессиональной и смежных сферах; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска; оценивать практическую значимость результатов поиска; применять средства информационных технологий для решения профессиональных	решения задач и/или проблем в профессиональном и/или социальном контексте; методы работы в профессиональной и смежных сферах; порядок оценки результатов решения задач профессиональной деятельности номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации, порядок их применения; программное обеспечение в профессиональной деятельности, в том числе цифровые средства; Основы ИБ; Основы ИБ организации; Модель угроз информационной безопасности ИС организации заказчика; Процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика; Методы предотвращения потери данных; Понятие и классификация инцидентов ИБ; Типичные угрозы ИБ при работе с БД; Процедуры и регламенты передачи информации об инцидентах в службу ИБ

	доступа пользователей к элементам БД при обнаружении инцидентов ИБ (при необходимости); Поддержания баз антивирусных программ в актуальном состоянии	задач; использовать современное программное обеспечение в профессиональной деятельности; использовать различные цифровые средства для решения профессиональных задач Идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; Идентифицировать инциденты ИБ при работе с БД; Осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации); Управлять доступом пользователей к элементам БД при обнаружении инцидентов ИБ; Устанавливать и сопровождать антивирусное ПО	организации; Основы работы со средствами антивирусной защиты;

2. Структура и содержание общеобразовательной дисциплины

2.1. Объем учебной дисциплины и виду учебной работы

Таблица 2. Распределение трудоемкости дисциплины по видам учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы дисциплины	**124**
Основное содержание	**102**
В том числе:	
Теоретическое обучение (ТО)	34
Практические занятия (ПЗ)	Не предусмотрено
Лабораторные занятия (ЛР)	68
Самостоятельная работа	**22**
В том числе:	
Курсовая работа	Не предусмотрено
Другие виды самостоятельной работы	Не предусмотрено
Промежуточная аттестация	
Зачет	2
Дифференцированный зачет	2
Экзамен	Не предусмотрено
ИТОГО	124

2. Тематический план и содержание дисциплины

2.2.1. Тематический план

Таблица 3. Содержание учебного материала

№	Наименование разделов и тем	Объем часов	ТО	ПЗ	ЛР	СР	Формируемые компетенции
1	Раздел 1. Информационная безопасность и уровни ее обеспечения	**56**	**16**		**32**	**8**	
	Тема 1.1 Основные понятия информационной безопасности	4	4				ПК-1.1 ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7
	Тема 1.2 Основные угрозы информации	16	4		20		ОК-1, ПК-1.1 ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.5
	Тема 1.3 Основные методы несанкционированного доступа к информации	8	4			4	ПК-1.1 ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.5
	Тема 1.4 Положения теории информационной безопасности информационных систем	16	4		12	4	ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7
	Промежуточная аттестация	2				2	
2	Раздел 2. Обеспечение информационной безопасности	**52**	**12**		**30**	**10**	
	Тема 2.1 Стандарты информационной безопасности	4	4				ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-

							1.7, ПК-4.5
	Тема 2.2 Административный уровень обеспечения информационной безопасности	4	2			2	ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.5
	Тема 2.3 Методы обеспечения информационной безопасности	44	6		30	8	ОК-2 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.2, ПК-4.4, ПК-4.5
3	Раздел 3. Вопросы правового обеспечения защиты информации в информационных системах	**14**	**6**		**6**	**2**	
	Тема 3.1 Отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации.	10	2		6	2	ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7
	Тема 3.2 Международные правовые и нормативные акты обеспечения ИБ процессов переработки информации.	2	2				ОК-1
	Тема 3.3 Ответственность за правонарушения в сфере информации.	2	2				ОК-1 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7
	Промежуточная аттестация	**2**				**2**	
Всего на дисциплину		**124**	**34**		**68**	**22**	

2.2.2. Содержание дисциплины

РАЗДЕЛ 1 «Информационная безопасность и уровни ее обеспечения»

Тема 1.1 «Основные понятия информационной безопасности». Понятие информации. Понятия информационной безопасности и защиты информации. Актуальность информационной безопасности. Конфиденциальность информации. Классификация информации по признаку конфиденциальности. Доступность информации. Целостность информации.

Тема 1.2 «Основные угрозы информации». Международные стандарты обмена информацией. Уязвимость информации. Понятие угрозы. Классификация угроз. Причины нарушения целостности информации. Физические угрозы безопасности информации. Аппаратные угрозы безопасности информации. Программные угрозы безопасности информации.

Тема 1.3 «Основные методы несанкционированного доступа к информации». Методы снижения эффективности работы сети на уровне транспортных и коммуникационных протоколов. Методы несанкционированного доступа к электронной почте. Методы несанкционированного доступа к распределенным системам, построенным на основе архитектуры «клиент-сервер». Методы несанкционированного доступа к клиентскому программному обеспечению WWW. Особенности каналов утечки и несанкционированного доступа к информации в помещениях с информационными системами. Аппаратная реализация современных

методов несанкционированного доступа к информации. Программная реализация несанкционированного доступа к информации на основе использования программных закладок. Использование компьютерных вирусов для организации каналов утечки и несанкционированного доступа к информации. Ботнеты. Darknet.

Тема 1.4 «Положения теории информационной безопасности информационных систем» Функции и задачи защиты информации. Основные положения теории информационной безопасности информационных систем. Понятие политики безопасности. Модели безопасности и их применение: модель Адепт-50; модель конечных автоматов; модель безопасности с полным перекрытием; модель Bell-LaPadula; модель Biba; модель Clark-Wilson; модель информационных потоков; модель невлияния; сетчатая модель; модель Brewer and Nesh; модель Graham-Denning; модель Harrison-Ruzzo-Ullman.

РАЗДЕЛ 2 «Обеспечение информационной безопасности»

Тема 2.1 «Стандарты информационной безопасности». Основные действующие стандарты по направлению "Информационная безопасность". Отраслевые стандарты в области информационной безопасности. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ.

Тема 2.2 «Административный уровень обеспечения информационной безопасности». Цели, задачи и содержание административного уровня обеспечения информационной безопасности. Понятие политики информационной безопасности. Основные компоненты политики информационной безопасности.

Тема 2.3 «Методы обеспечения информационной безопасности». Идентификация и аутентификация. Методы управления доступом к информации. Аудит, контроль целостности. Туннелирование. Криптографические методы защиты информации. Аппаратные и технические средства обеспечения безопасности информации. Программные средства обеспечения безопасности информации. Анализ мер обеспечения безопасности персонального компьютера. Анализ мер обеспечения безопасности файлового сервера. Анализ мер обеспечения безопасности сервера приложений. Методы и средства обеспечения безопасности в каналах информационно-вычислительных сетей и телекоммуникаций. Проектирование информационного обеспечения с учетом требований информационной безопасности. Программные средства обеспечения безопасности информации. Организационное обеспечение информационной безопасности. Основные методы управления проектами защищенных информационных систем.

РАЗДЕЛ 3 «Вопросы правового обеспечения защиты информации в информационных системах»

Тема 3.1 «Отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации». Понятие государственной информационной политики. Виды юридических документов, посвященных защите информации. Содержание законов, касающихся охраны секретных материалов. Закон "Об информации, информатизации и защите информации"

Тема 3.2 «Международные правовые и нормативные акты обеспечения ИБ процессов переработки информации». «Оранжевая книга». «Зелёная книга». Законодательство развитых стран в сфере информационной безопасности.

Тема 3.3 «Ответственность за правонарушения в сфере информации». Административная ответственность за правонарушения в сфере информации - гражданский кодекс РФ. Уголовная ответственность за правонарушения в сфере информации - уголовный кодекс кодекс РФ.

Таблица 4. Тематика лабораторных занятий

№ Темы	Тематика лабораторного занятия	Объем, акад. ч.	Формируемые компетенции
1	Анализ угроз безопасности информации хранящейся в локальном компьютере	10	ОК-1, ПК-1.1 ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.5
2	Анализ угроз безопасности информации хранящейся в компьютере подключенном к локальной сети	10	ОК-1, ПК-1.1 ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.5
3	Построение модели безопасности с полным перекрытием для компьютера подключенного к локальной сети	12	ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7
4	Шифры на основе метода подстановок	4	ОК-2 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.2, ПК-4.4, ПК-4.5
5	Шифрование с помощью датчика псевдослучайных чисел	4	ОК-2 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.2, ПК-4.4, ПК-4.5
6	Изучение стандарта RSA	4	ОК-2 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.2, ПК-4.4, ПК-4.5
7	Разработка комплекса мер по защите информации в офисе фирмы	4	ОК-2 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.2, ПК-4.4, ПК-4.5
8	Анализ законодательства в сфере обеспечения информационной безопасности	4	ОК-1 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7
9	Защита и восстановление данных на компьютере, используя систему архивации	4	ОК-2 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.2, ПК-4.4, ПК-4.5
10	Использование антивирусных программ	6	ОК-2 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.2, ПК-4.4, ПК-4.5
11	Выполнение настройки параметров резервного копирования дисков в соответствии с разработанным планом. Выполнение резервного копирования и восстановления данных.	6	ОК-2 ПК-1.1, ПК-1.4, ПК-1.5, ПК-1.6, ПК-1.7, ПК-4.2, ПК-4.4, ПК-4.5

3. Самостоятельная работа обучающихся и текущий контроль успеваемости

Основными целями самостоятельной работы студентов является формирование способностей к самостоятельному познанию и обучению, поиску литературы, обобщению, оформлению и представлению полученных результатов, их критическому анализу, поиску новых, рациональных и неординарных решений, аргументированному отстаиванию своих предложений, умений подготовки выступлений и ведения дискуссий.

Самостоятельная работа заключается в изучении отдельных тем курса по заданию преподавателя по рекомендуемой им учебной литературе, в подготовке к лабораторным и практическим занятиям; к текущему контролю успеваемости; подготовке к промежуточной аттестации.

После вводных лекций, в которых обозначается содержание дисциплины, ее проблематика и практическая значимость, студентам выдаются задания на самостоятельную работу. Студенты выполняют задания в часы СРС в течение семестра в соответствии с освоением учебных разделов. Защита выполненных заданий производится поэтапно в часы лабораторных/практических занятий. Оценивание осуществляется по содержанию и качеству выполненного задания. Форма оценивания – зачет.

Критерии оценивания:

«зачтено» выставляется студенту за задание, выполненное полностью. Допускаются минимальные неточности в расчетах.

«не зачтено» выставляется студенту за не полностью выполненное задание и/или при наличии грубых ошибок.

Не зачтенные задания студент должен исправить в часы, отведенные на СРС, и сдать на проверку снова.

4. Условия реализации общепрофессиональной дисциплины

4.1. Материально-техническое обеспечение

Для реализации программы предусмотрены следующие специальные помещения: кабинет информационной безопасности оснащенный в соответствии с ОП СПО по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

Помещение для самостоятельной работы: библиотека с читальным залом, оснащенная в соответствии с Приложением 3 ОХОП-П, библиотечный фонд.

4.2. Учебно-методическое обеспечение

4.2.1 Основная литература по дисциплине

1. Середкин, С.П. Основы информационной безопасности : учебно-методическое пособие / С.П. Середкин; Иркутский государственный университет, Физический факультет. - Иркутск : Иркутский государственный университет, 2024. - 103 с. - Текст : непосредственный. - ISBN 978-5-0624-2252-7 : 0-00. - (ID=161585-1)

2. Капгер, И.В. Управление информационной безопасностью : учебное пособие / И.В. Капгер, А.С. Шабуров; Пермский национальный исследовательский политехнический университет. - Пермь : Пермский национальный исследовательский политехнический университет, 2023. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 01.03.2024. - ЭБС Лань. - ISBN 978-5-398-02866-9. - (ID=159231-0)URL: https://e.lanbook.com/book/328889

3. Мошак, Н.Н. Основы управления информационной безопасностью : учебное пособие / Н.Н. Мошак; Санкт-Петербургский государственный университет аэрокосмического приборостроения ; под редакцией В.В. Овчинникова. - Санкт-Петербург : Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2022. - 143 с. : ил. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 01.03.2024. - ЭБС Лань. - ISBN 978-5-8088-1711-1. - (ID=159229-0)URL: https://e.lanbook.com/book/340967

4. Правовые нормы защиты информации в автоматизированных системах : учебное пособие / Н.В. Киреева [и др.]; Поволжский государственный университет телекоммуникаций и информатики . Кафедра информационной безопасности. - Самара : Поволжский государственный университет телекоммуникаций и информатики, 2020. - 60 с. - Текст : непосредственный. - ISBN 978-5-907336-43-8 : 0-00. - (ID=161654-1)

4.2.2 Дополнительная литература по дисциплине

1. Козырь, Н.С.Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н.С. Козырь, Л.Л. Оганесян. - Москва : Юрайт, 2024. - 131 с. - (Высшее образование). - Текст : электронный. - Режим доступа: по подписке. - Образовательная платформа Юрайт. - ISBN 978-5-534-17863-0. - (ID=161935-0)URL: https://urait.ru/bcode/545066

2. Леонтьев, А.С. Защита информации : учебное пособие / А.С. Леонтьев; МИРЭА - Российский технологический университет. - Москва : МИРЭА - Российский технологический университет, 2021. - Текст : электронный. - Режим доступа: по подписке. - Дата обращения: 07.07.2022. - ЭБС Лань. - (ID=145965-0)URL:

4.3. Программное обеспечение по дисциплине

- ОС "Альт Образование" 8
- Учебный комплект программного обеспечения КОМПАС-3D v18 для преподавателя

Программное обеспечение КОМПАС-3D v18

- МойОфис Стандартный
- WPS Office
- Libre Office
- Lotus Notes!Domino,
- LMS Moodle

- Marc-SQL
- МегаПро,
- Office для дома и учебы 2013
- 7zip,
- «Консультант Плюс»
- «Гарант»
- ОС РЕД ОС
- 1С:Предприятие 8.
- ПО PIX.

4.4. Специализированные базы данных, справочные системы, электронно-библиотечные системы, профессиональные порталы в Интернет

ЭБС и лицензионные ресурсы ТвГТУ размещены:

1. Ресурсы: https://lib.tstu.tver.ru/header/obr-res
2. ЭК ТвГТУ: https://elib.tstu.tver.ru/MegaPro/Web
3. ЭБС "Лань": https://e.lanbook.com/
4. ЭБС "Университетская библиотека онлайн": https://www.biblioclub.ru/
5. ЭБС «IPRBooks»: https://www.iprbookshop.ru/
6. Электронная образовательная платформа "Юрайт" (ЭБС «Юрайт»): https://urait.ru/
7. Научная электронная библиотека eLIBRARY: https://elibrary.ru/
8. Информационная система "ТЕХНОРМАТИВ".Конфигурация "МАКСИМУМ": сетевая версия (годовое обновление): [нормативно-технические, нормативно-правовые и руководящие документы (ГОСТы, РД, СНиПы и др.]. Диск 1, 2, 3, 4. - М.:Технорматив, 2014. - (Документация для профессионалов). - CD. - Текст: электронный. - 119600 р. – (105501-1)

5. Контроль и оценка результатов освоения общепрофессиональной дисциплины

Результаты обучения должны быть ориентированы на получение компетенций для последующей профессиональной деятельности как в рамках данной предметной области, так и в смежных с ней областях. Они включают в себя результаты освоения общеобразовательной дисциплины в соответствии с ФГОС СПО и на основе ФГОС СОО.

Таблица 6. Оценочные мероприятия освоения дисциплины

Результаты обучения	**Критерии оценки**	**Методы оценки**
- знать		
актуальный профессиональный и социальный контекст, в котором приходится работать и жить структура плана для решения задач, алгоритмы выполнения работ в	Демонстрация знания способов решения задач профессиональной деятельности применительно к	

профессиональной и смежных областях основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте методы работы в профессиональной и смежных сферах порядок оценки результатов решения задач профессиональной деятельности	различным контекстам	Устный опрос; Оценка результатов лабораторной работы; Оценка результатов текущего контроля; Самооценка своего знания, осуществляемая обучающимися; Промежуточная аттестация
номенклатура информационных источников, применяемых в профессиональной деятельности приемы структурирования информации формат оформления результатов поиска информации современные средства и устройства информатизации, порядок их применения и программное обеспечение в профессиональной деятельности, в том числе цифровые средства	Демонстрация знания современных средств поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	
Основы ИБ; Основы ИБ организации; Модель угроз информационной безопасности ИС организации заказчика; Процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика; Методы предотвращения потери данных; Понятие и классификация инцидентов ИБ; Типичные угрозы ИБ при работе с БД; Процедуры и регламенты передачи информации об инцидентах в службу ИБ организации; Основы работы со средствами антивирусной защиты;	Знание основ информационной безопасности, знание методов обеспечения информационной безопасности	
- уметь		
распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы выявлять и эффективно искать информацию, необходимую для	Умение выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	

решения задачи и/или проблемы владеть актуальными методами работы в профессиональной и смежных сферах оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)		
определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска оценивать практическую значимость результатов поиска применять средства информационных технологий для решения профессиональных задач использовать современное программное обеспечение в профессиональной деятельности использовать различные цифровые средства для решения профессиональных задач	Умение использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	
Идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	Умение обнаруживать инциденты информационной безопасности, связанные с работой информационных систем.	
Идентифицировать инциденты ИБ при работе с БД Осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации) Управлять доступом пользователей к элементам БД при обнаружении инцидентов ИБ Устанавливать и сопровождать антивирусное ПО	Умение выявлять инциденты информационной безопасности при обеспечении функционирования баз данных.	

4.1. Оценочные средства для проведения текущей и промежуточной аттестации

Фонды оценочных средств (далее ФОС) предназначены для контроля и оценки образовательных достижений студентов, освоивших программу учебной дисциплины «Основы информационной безопасности».

ФОС включают контрольные материалы для проведения итоговой аттестации в форме дифференцированного зачета.

ФОС разработаны на основании основной профессиональной образовательной программы по направлению подготовки специальности СПО: 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

1. Оценочные средства для текущего контроля.

Текущий контроль проводится в форме домашнего задания для самостоятельного выполнения. Результаты фиксируются в образовательной платформе, на которой зарегистрированы студенты и преподаватель.

2. Оценочные средства для промежуточного контроля

При промежуточной аттестации в форме зачета студенту в обязательном порядке описываются критерии проставления оценки:

«зачтено» - выставляется обучающемуся при условии выполнения им всех контрольных мероприятий: посещение занятий в объеме не менее 70% контактной работы с преподавателем, выполнения и защиты не менее 90% заданий текущего контроля.

«не зачтено» - выставляется обучающемуся при условии невыполнения им контрольных мероприятий: посещение занятий в объеме менее 60% контактной работы с преподавателем, выполнения и защиты менее 70% заданий текущего контроля.

При необходимости преподаватель может выдать дополнительное задание студенту, охватывающее все темы и разделы курса и определяющее уровень сформированности компетенций.

Формой аттестации по дисциплине является дифференцированный зачет. Итогом дифференцированного зачета является оценка знаний и умений обучающегося по пятибалльной шкале.

Условия проведения дифференцированного зачета:

дифференцированный зачет проводится по вариантам.

количество вариантов - 15.

Задания предусматривают одновременную проверку усвоенных знаний и освоенных умений по всем темам программы. Ответы предоставляются письменно.

При промежуточной аттестации в форме дифференцированного зачета студенту выдается билет с вопросами и задачами.

Число вопросов – 3 (2 вопроса для контроля сформированности знаний, 1 вопрос для контроля сформированности умений и навыков).

Продолжительность – 45 минут.

Шкала оценивания промежуточной аттестации – «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии выполнения контрольного испытания и условия проставления зачёта:

для контроля сформированности знаний:

ниже базового - 0 балл;

базовый уровень – 1 балл;
выше базового – 2 балла.

для контроля сформированности умений:
отсутствие умения – 0 балл;
наличие умения – 2 балла.

Критерии итоговой оценки за дифференциальный зачет:

«отлично» - при сумме баллов 5 или 6;

«хорошо» - при сумме баллов 4;

«удовлетворительно» - при сумме баллов 3;

«неудовлетворительно» - при сумме баллов 0, 1 или 2.

Для итогового контрольного испытания студенту в обязательном порядке предоставляется:

база заданий, предназначенных для предъявления обучающемуся на итоговом контрольном испытании;

методические материалы, определяющие процедуру проведения итогового испытания и проставления зачёта.

Задание выполняется письменно и/или с использованием ЭВМ.

База заданий, предъявляемая обучающимся на итоговом контрольном испытании.

1. Понятие угрозы. Классификация угроз безопасности
2. Международные стандарты обмена информацией. Понятие угрозы.
3. Особенности каналов утечки и несанкционированного доступа к информации в информационных системах. Аппаратная реализация современных методов несанкционированного доступа к информации.
4. Использование компьютерных вирусов для организации каналов утечки и несанкционированного доступа к информации.
5. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение.
6. Методы и средства обеспечения безопасности в информационных системах.
7. Технические средства обеспечения безопасности ЭВМ.
8. Методы защиты информации от несанкционированного доступа в сетях ЭВМ.
9. Идентификация и аутентификация. Методы управления доступом к информации. Аудит, контроль целостности.
10. Криптографические методы защиты информации.
11. Аппаратные и технические средства обеспечения безопасности информации.
12. Программные средства обеспечения безопасности информации.
13. Проектирование информационного обеспечения с учетом требований информационной безопасности.
14. Программные средства обеспечения безопасности информации.
15. Организационное обеспечение информационной безопасности.
16. Общая характеристика правового регулирования информации. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

17. Основные законы и нормативные руководящие документы, касающиеся государственной тайны, информационной безопасности и защиты информации, нормативно-справочные документы.

Пример билета приведен в Приложении.

Преподаватель имеет право после проверки письменных ответов задавать студенту в устной форме уточняющие вопросы в рамках задания, выданного студенту.

6. Внесение изменений и дополнений в рабочую программу дисциплины

Содержание рабочих программ дисциплин ежегодно обновляется протоколами заседаний кафедры по утвержденной «Положением о структуре, содержании и оформлении рабочих программ дисциплин по образовательным программам, соответствующим ФГОС СПО с учетом профессиональных стандартов» форме.

ПРИЛОЖЕНИЕ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тверской государственный технический университет»

Специальность: 09.02.12 Техническая эксплуатация и сопровождение информационных систем
Кафедра «Информационные системы»
Дисциплина «Основы информационной безопасности»
Семестр 4

ЗАДАНИЕ ДЛЯ ПРОФЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
в форме дифференцированного зачета

БИЛЕТ № 1

1. Задание для контроля сформированности знаний – 0, или 1, или 2 балла:
Понятие угрозы. Классификация угроз безопасности.

2. Задание для контроля сформированности знаний – 0, или 1, или 2 балла:
Понятие политики информационной безопасности.

3. Задание для контроля сформированности умений – 0 или 2 балла:
Построить линейный конгруэнтный датчик псевдослучайных чисел. Проанализировать криптостойкость полученной гаммы шифра.

Критерии итоговой оценки за зачет:
«отлично» - при сумме баллов 5 или 6;
«хорошо» - при сумме баллов 4;
«удовлетворительно» - при сумме баллов 3;
«неудовлетворительно» - при сумме баллов 0, 1 или 2.

Составитель: доц. кафедры ИС В.В. Алексеев

Заведующий кафедрой Б.В. Палюх

Лист регистрации изменений в рабочей программе общепрофессиональной дисциплины

№ изменения	Номер листа			№ протокола и дата заседания кафедры	Дата внесения изменения в РПД	Ф.И.О. лица, ответственного за внесение изменений
	измененного	нового	изъятого			