Частное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ УПРАВЛЕНИЯ И ЭКОНОМИКИ»

РАССМОТРЕНО И ОДОБРЕНО

На заседании кафедры информационных технологий и математики
Протокол № 9 от 25.05.2023 г.

УТВЕРЖДАЮ

Первый проректор
С.В. Авдашкевич
28.06.2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина:	Б1.В.06 Информационная безопасность организации
Направление подготовки:	38.04.05 Бизнес-информатика
Направленность (профиль):	Консалтинг в сфере IT
Уровень высшего образования:	Магистратура
Форма обучения:	очная, заочная, очно-заочная
Разработчики:	Старший преподаватель Мурзинцев С. В.

Санкт-Петербург
2023

1. Цели и задачи дисциплины:

Цель освоения дисциплины:

формирование у студентов методически правильных основ знаний и практических навыков по обеспечению информационной безопасности (ИБ) организаций, необходимых обучающимся, занимающимся эксплуатацией корпоративных информационных систем.

Задачи дисциплины:

получение обучающихся необходимых для работы теоретических знаний о современных средствах, методах и технологиях обеспечения информационной безопасности корпоративных информационных систем;

получение практических навыков организации работ по обеспечению информационной безопасности и защиты информации на предприятиях.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы высшего образования

Планируемые результаты освоения ОП ВО (код и содержание компетенций)	**Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)**	**Примечание**
ПК-7 Способен планировать управление требованиями к ИС	ПК-7.1 Знает инструменты и методы управления требованиями; основы информационной безопасности организации; предметную область автоматизации; современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP..., ITIL, ITSM); управление содержанием проекта: документирование требований, анализ продукта, модерируемые совещания.	06.015 Профессиональный стандарт «Специалист по информационным системам»
	ПК-7.2 Умеет планировать работы по созданию (модификации) и сопровождению ИС.	
	ПК-7.3 Способен разрабатывать, согласовывать и утверждать план управления требованиями к ИС.	

Планируемые результаты обучения по ОП ВО (индикаторы достижения компетенций)	**Планируемые результаты обучения по дисциплине**
ПК-7.1. Знает инструменты и методы управления требованиями; основы информационной безопасности организации; предметную область автоматизации; современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP..., ITIL, ITSM); управление содержанием проекта: документирование требований, анализ продукта, модерируемые совещания.	Знать инструменты и методы управления требованиями; основы информационной безопасности организации; предметную область автоматизации; современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP..., ITIL, ITSM); управление содержанием проекта: документирование требований, анализ продукта, модерируемые совещания.
ПК-7.2. Умеет планировать работы по созданию (модификации) и сопровождению ИС.	Уметь планировать работы по созданию (модификации) и сопровождению защиты информации в информационных системах предприятия.
ПК-7.3. Способен разрабатывать, согласовывать и утверждать план управления требованиями к ИС.	Владеть навыком разработки, согласования и способен утверждать план управления требованиями к ИС в сфере защиты информации.

3. Содержание, объем дисциплины и формы проведения занятий

№ п/п	Наименование темы дисциплины	Компетенции	Оценочные средства текущего контроля		
			ЗНАТЬ	УМЕТЬ	ВЛАДЕТЬ
			ПК-7.1	ПК-7.2	ПК-7.3
1	Сетевая безопасность организации.	ПК-7	Деловая и (или) ролевая игра/Кейс-задача №1 (20) Деловая и (или) ролевая игра/Кейс-задача №2 (20)	Деловая и (или) ролевая игра/Кейс-задача №1 (20) Деловая и (или) ролевая игра/Кейс-задача №2 (20)	Деловая и (или) ролевая игра/Кейс-задача №1 (20) Деловая и (или) ролевая игра/Кейс-задача №2 (20)
2	Классификация угроз на предприятии.	ПК-7	Деловая и (или) ролевая игра/Кейс-задача №3 (20) Деловая и (или) ролевая игра/Кейс-задача №4 (20)	Деловая и (или) ролевая игра/Кейс-задача №3 (20) Деловая и (или) ролевая игра/Кейс-задача №4 (20)	Деловая и (или) ролевая игра/Кейс-задача №3 (20) Деловая и (или) ролевая игра/Кейс-задача №4 (20)
3	Классификация типов программно-аппаратных средств защиты информации, используемых в организации.	ПК-7	Деловая и (или) ролевая игра/Кейс-задача №5 (20)	Деловая и (или) ролевая игра/Кейс-задача №5 (20)	Деловая и (или) ролевая игра/Кейс-задача №5 (20)
Количество баллов (100 баллов):			100		

Содержание учебного материала, лабораторные работы и практические занятия, курсовая работа
Тема 1: Сетевая безопасность организации. Введение в информационную безопасность, Правовое обеспечение информационной безопасности, Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности. **Практические занятия/самостоятельная работа:** Защита коммерческой тайны. Государственные автоматизированные системы. Использование и защита **Лабораторная работа:** -
Тема 2: Классификация угроз на предприятии. Классификация сетевых угроз, Файерволлы, Антивирусы, Обновление и настройка операционной системы, Шифрование и пароли, Архивирование и резервное копирование, Социальная инженерия. **Практические занятия/самостоятельная работа:** Защита персональных данных на предприятии. Тестирование на проникновение (Penetration testing). **Лабораторная работа:** -
Тема 3: Классификация типов программно-аппаратных средств защиты информации, используемых в организации. Идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, стеганография, экранирование. **Практические занятия/самостоятельная работа:** Криптография. Шифры перестановки, Шифры простой замены, Шифры сложной замены. **Лабораторная работа:** -
Курсовая работа: не предусмотрено учебным планом

Очная форма обучения

Вид учебной работы	Всего часов	Семестр 3
Аудиторные занятия (АЗ):	42	42
Лекционные занятия (Лек)	14	14
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	28	28
Самостоятельная работа студента (СР)	60	60
Курсовая работа	0	0
Другие виды самостоятельной работы*	60	60
Контроль самостоятельной работы (КСР)	6	6

Вид учебной работы	Всего часов	Семестр 3
Контактная работа (КоР)	48	48
Форма промежуточной аттестации	0	Зачет
Подготовка к экзамену и сдача экзамена (СР, КоР)	0	0
Общая трудоемкость дисциплины, часы/ЗЕТ	108/3	108/3

* Подготовка к аудиторным занятиям, подготовка к зачету (при наличии)

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
1	Сетевая безопасность организации.	3	4	10	0	20	10
2	Классификация угроз на предприятии.	3	4	10	0	20	10
3	Классификация типов программно-аппаратных средств защиты информации, используемых в организации.	3	6	8	0	20	8
	Итого:		14	28	0	60	28

* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

Заочная форма обучения

Вид учебной работы	Всего часов	Семестр 4
Аудиторные занятия (АЗ):	8	8
Лекционные занятия (Лек)	2	2
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	6	6
Самостоятельная работа студента (СР)	91	91
Курсовая работа	0	0
Другие виды самостоятельной работы*	91	91
Контроль самостоятельной работы (КСР)	5	5
Контактная работа (КоР)	13	13
Форма промежуточной аттестации	0	Зачет
Подготовка к экзамену/зачету и сдача экзамена/зачета (СР, КоР)	4	4
Общая трудоемкость дисциплины, часы/ЗЕТ	108/3	108/3

* Подготовка к аудиторным занятиям

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
1	Сетевая безопасность организации.	4	2	2	0	30	10
2	Классификация угроз на предприятии.	4	0	2	0	30	10
3	Классификация типов программно-аппаратных средств защиты информации, используемых в организации.	4	0	2	0	31	8
	Итого:		2	6	0	91	28

* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и (или) путем выделения часов из часов, отведенных на самостоятельную работу, и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

Очно-заочная форма обучения

Вид учебной работы	Всего часов	Семестр 4
Аудиторные занятия (АЗ):	24	24
Лекционные занятия (Лек)	12	12
Лабораторные занятия (Лаб)	0	0
Практические занятия (Пр)	12	12

Вид учебной работы	Всего часов	Семестр 4
Самостоятельная работа студента (СР)	80	80
Курсовая работа	0	0
Другие виды самостоятельной работы*	80	80
Контроль самостоятельной работы (КСР)	4	4
Контактная работа (КоР)	28	28
Форма промежуточной аттестации	0	Зачет
Подготовка к экзамену и сдача экзамена (СР, КоР)	0	0
Общая трудоемкость дисциплины, часы/ЗЕТ	108/3	108/3

* Подготовка к аудиторным занятиям, подготовка к зачету (при наличии)

№	Наименование темы дисциплины	Семестр/ Курс	Количество учебных часов				Практическая подготовка
			В том числе по видам аудиторных занятий			СР	
			Лек	Пр	Лаб		
1	Сетевая безопасность организации.	4	4	4	0	26	10
2	Классификация угроз на предприятии.	4	4	4	0	26	10
3	Классификация типов программно-аппаратных средств защиты информации, используемых в организации.	4	4	4	0	28	8
	Итого:		12	12	0	80	28

* Практическая подготовка при реализации дисциплин организована путем проведения практических занятий и (или) выполнения лабораторных и (или) курсовых работ и (или) путем выделения часов из часов, отведенных на самостоятельную работу, и предусматривает выполнение работ, связанных с будущей профессиональной деятельностью.

4. Способ реализации дисциплины

Без использования онлайн-курса.

5. Учебно-методическое обеспечение дисциплины:

Основная литература:

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Учебное пособие для вузов / Суворова Г. М. - Ярославский государственный педагогический университет имени К.Д. Ушинского (г. Ярославль)., 2023 г. - 253 с. - ISBN 978-5-534-13960-0 – Режим доступа: https://urait.ru/book/informacionnaya-bezopasnost-519780

2. КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ: СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ И КОМПЛАЕНС В КОМПАНИИ. Учебное пособие для вузов / Панарина М. М. - Национальный исследовательский университет «Высшая школа экономики» (г. Москва)., 2023 г. - 158 с. - ISBN 978-5-534-15342-2 – Режим доступа: https://urait.ru/book/korporativnaya-bezopasnost-sistema-upravleniya-riskami-i-komplaens-v-kompanii-520423

3. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Учебник и практикум для вузов / Казарин О. В., Забабурин А. С. - Российский государственный гуманитарный университет (г. Москва).; Московский государственный университет имени М.В. Ломоносова (г. Москва)., 2023 г. - 312 с. - ISBN 978-5-9916-9043-0 – Режим доступа: https://urait.ru/book/programmno-apparatnye-sredstva-zaschity-informacii-zaschita-programmnogo-obespecheniya-513300

Дополнительная литература:

1. ЗАЩИТА ИНФОРМАЦИИ 3-е изд., пер. и доп. Учебное пособие для вузов / Внуков А. А. - Национальный исследовательский университет «Высшая школа экономики» (г. Москва)., 2023 г. - 161 с. - ISBN 978-5-534-07248-8 – Режим доступа: https://urait.ru/book/zaschita-informacii-512268

2. ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Учебник и практикум для вузов / Под ред. Поляковой Т. А., Стрельцова А.

А. - Всероссийский государственный университет юстиции (РПА Минюста России) (г. Москва).; Московский государственный университет имени М.В. Ломоносова (г. Москва)., 2023 г. - 325 с. - ISBN 978-5-534-03600-8 – Режим доступа: https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-511239

3. ПРАВОВОЕ РЕГУЛИРОВАНИЕ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ. Монография / Жарова А. К. - Национальный исследовательский университет «Высшая школа экономики» (г. Москва)., 2023 г. - 301 с. - ISBN 978-5-534-14919-7 – Режим доступа: https://urait.ru/book/pravovoe-regulirovanie-sozdaniya-i-ispolzovaniya-informacionnoy-infrastruktury-v-rossiyskoy-federacii-519998

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения

1. Операционная система
2. Пакет прикладных офисных программ
3. Антивирусное программное обеспечение
4. LMS Moodle
5. Вебинарная платформа
6. Oracle VM Virtualbox

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», информационных справочных систем и профессиональных баз данных, необходимых для освоения дисциплины

1. ibooks.ru : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://ibooks.ru. - Текст: электронный
2. Электронно-библиотечная система СПбУТУиЭ : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: http://libume.ru. - Текст: электронный
3. Юрайт : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://urait.ru. - Текст: электронный
4. eLibrary.ru : научная электронная библиотека [Электронный ресурс] : профессиональная база данных. - Режим доступа: http://elibrary.ru. - Текст: электронный
5. Архив научных журналов НЭИКОН [Электронный ресурс] : профессиональная база данных. - Режим доступа: arch.neicon.ru. - Текст: электронный
6. КиберЛенинка : научная электронная библиотека [Электронный ресурс] : информационная справочная система. - Режим доступа: http://cyberleninka.ru. - Текст: электронный
7. Лань : электронно-библиотечная система [Электронный ресурс] : профессиональная база данных. - Режим доступа: https://e.lanbook.com. - Текст: электронный
8. it-world.ru [Электронный ресурс] : информационная справочная система . - Режим доступа: https://www.it-world.ru. - Текст: электронный
9. Виртуальный компьютерный музей [Электронный ресурс] : информационная справочная система . - Режим доступа: https://www.computer-museum.ru. - Текст: электронный
10. Компьютерра : информационная справочная система . - Режим доступа: https://www.computerra.ru/. - Текст: электронный
11. Управление производством [Электронный ресурс] : информационная справочная система . - Режим доступа: http://www.up-pro.ru. - Текст: электронный
12. HR-tv.ru [Электронный ресурс] : информационная справочная система . - Режим доступа: https://thehrd.ru/. - Текст: электронный
13. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: профессиональная база данных. - Режим доступа: https://digital.gov.ru. - Текст:

электронный

14. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: профессиональная база данных . - Режим доступа: https://rkn.gov.ru. - Текст: электронный

15. Math-Net.Ru: профессиональная база данных . - Режим доступа: https://www.mathnet.ru/. - Текст: электронный

16. Экономика. Социология. Менеджмент: федеральный образовательный портал: профессиональная база данных. - Режим доступа: http://ecsocman.hse.ru/. - Текст: электронный

17. Executive.ru: профессиональная база данных . - Режим доступа: https://www.e-xecutive.ru. - Текст: электронный

8. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа, семинарского типа - практических занятий, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованная: рабочими местами для обучающихся, оснащенными специальной мебелью; рабочим местом преподавателя, оснащенным специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской; лицензионным программным обеспечением

2. Учебная аудитория для проведения занятий семинарского типа - практических занятий – компьютерный класс, оборудованный рабочими местами для обучающихся, оснащенными специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета; рабочим местом преподавателя, оснащенным специальной мебелью, персональным компьютером с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета; техническими средствами обучения - мультимедийным оборудованием (проектор, экран, колонки) и маркерной доской; лицензионным программным обеспечением

3. При применении электронного обучения, дистанционных образовательных технологий используются: виртуальные аналоги учебных аудиторий - вебинарные комнаты на вебинарных платформах, рабочее место преподавателя, оснащенное персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному порталу Университета umeos.ru, веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройствами), программным обеспечением; рабочее место обучающегося оснащено персональным компьютером (планшет, мобильное устройство) с возможностью подключения к сети «Интернет», доступом к электронной информационно-образовательной среде Университета и к информационно-образовательному порталу Университета umeos.ru, веб-камерой, микрофоном и гарнитурой (в т.ч. интегрированными в устройства). Авторизация на информационно-образовательном портале Университета umeos.ru и начало работы осуществляются с использованием персональной учетной записи (логина и пароля). Лицензионное программное обеспечение

4. Помещение для самостоятельной работы, оборудованное специальной мебелью, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета, лицензионным программным обеспечением

9. Оценочные материалы по дисциплине

Описание оценочных средств (показатели и критерии оценивания, шкалы оценивания) представлено в приложении к основной профессиональной образовательной программе

«Каталог оценочных средств текущего контроля и промежуточной аттестации».

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности приводятся в соответствующих методических материалах и локальных нормативных актах Университета.

Для оценивания учебных достижений студентов в Университете действует балльно-рейтинговая система.

Если оценка, соответствующая набранной в семестре сумме рейтинговых баллов, удовлетворяет студента, то она является итоговой оценкой по дисциплине при проведении промежуточной аттестации в форме экзамена/зачета с оценкой/зачета.

Условием сдачи экзамена/зачета с оценкой/зачета с целью повышения итоговой оценки по дисциплине является сдача студентом экзамена, за который он получает экзаменационные баллы без учета баллов, полученных за текущий контроль:

Шкала оценивания учебных достижений по дисциплине,завершающейся зачетом без оценки

Баллы по дисциплине	60 и менее		61-73		74-90		91-100
Итоговая оценка по дисциплине	Незачет		Зачет				
Баллы в международной шкале ECTS с буквенным обозначением уровня	50 и менее	51-60	61-67	68-73	74-83	84-90	91-100
	F	Fx	E	D	C	B	A
Уровень сформированности компетенций	Не сформированы		Пороговый		Высокий		Повышенный

Шкала оценивания учебных достижений по дисциплине, завершающейся экзаменом/ зачетом с оценкой

Баллы по дисциплине	60 и менее		61-73		74-90		91-100
Итоговая оценка по дисциплине	Неудовлетворительно		Удовлетворительно		Хорошо		Отлично
Баллы в международной шкале ECTS с буквенным обозначением уровня	<50	51-60	61-67	68-73	74-83	84-90	91-100
	F	Fx	E	D	C	B	A
Уровень сформированности компетенций	Не сформированы		Пороговый		Высокий		Повышенный

9.1. Типовые контрольные задания для текущего контроля

Деловая и (или) ролевая игра / Кейс-задача №1.

1. Установить и настроить систему обнаружения вторжений в операционной системе , сгенерировать троянскую программу запустить её в операционной системе, подключиться и показать каким образом отреагирует.
2. Анализ существующих сканеров безопасности, выбор трех сканеров и их демонстрация работы

Деловая и (или) ролевая игра / Кейс-задача №2

Задание: создание модели угроз для организации.

Описание организации: Основное направление деятельности компании - внедрение и поддержка систем по управлению ИТ-архитектурой предприятия. Компания имеет исключительные права на локализацию и адаптацию оригинального программного обеспечения (далее - ПО), принадлежащего немецкой компании-партнеру. Данный софт направлен на визуализацию и оптимизацию всех процессов в компаниях с разветвленной системой ИТ-коммуникаций, именно поэтому клиентами компании являются в основном крупные корпорации, банки и государственные ведомства. Компания также предоставляет дополнительные услуги по внедрению и поддержке системы управления корпоративным контентом, принадлежащей глобальной ИТ-компании. Офисов РФ в следующих городах Москва, Санкт-Петербург, Новосибирск. Численность компьютеров в офисах от 50-100, имеются 10 ноутбуков у

сотрудников, которые подключаются удаленно к офисам из различных стран.

Деловая и (или) ролевая игра / Кейс-задача №3

1. Демонстрация взлома Wi-Fi сети, распространенные практики, методы программно-аппаратного обеспечения, которое может использовать злоумышленник.
2. Анализ существующих сканеров безопасности, выбор трех сканеров и их демонстрация.

Деловая и (или) ролевая игра / Кейс-задача №4

1. Демонстрация эксплуатации Web уязвимости на сайте с загрузкой Web-шелла.
2. Демонстрация SQL - инъекции, получение хеша пароля из базы данных и расшифровка его с использованием hashcat

Деловая и (или) ролевая игра / Кейс-задача №5

Шифровка и расшифровка сообщений с использованием шифров, простой замены, сложной замены и методом перестановки. Задание: расшифруйте сообщение с использованием шифра Цезаря и реализуйте в среде Excel и/или в иной.

ЗГ, ЪИОСЕИН ФПИУХИР, РС АХС ДЮОС ДЮ ИЬИ ТСОДИЗЮ. ТОСШС ХС, ЪХС СР ЛРСЖЗГ ЕРИКГТРС ФПИУХИР, ЕСХ Е ЪИП ЧСНЦФ!

СМОТЗИД М СМЫЙЗТ СЙ УФТХМЦЙ! СМОТЗИД М СМЫЙЗТ, М Ж ТХТЕЙССТХЦМ Ч ЦЙЩ, ОЦТ ХМПАСЙЙ ЖДХ. ХДРМ УФЙИПТКДЦ М ХДРМ ЖХЙ ИДИЧЦ!

ЗМХУЦРАК ТНПУИЙЕ ТНЬКИУ ТК ФУТНСЕГЧ ЦЕСН, Е ЙРД ЙКЧКО УЬКТБ ШЧУСНЧКРБТУ ЖКМ ПУТЫЕ НС ЗЦК УЖЯДЦТДЧБ Н ХЕЦЧУРПУЗАЗЕЧБ.

УЛ ЮЖСД, УОРФЙФ УЛ ШЦФЙЖД, ХФЭОУЕД ХЦОТЩЧ. О ЛЯЛ ЧЭОШЖД КФСЙФТ ХЦЛКЩХЦЛКОШВ, ЭШФ РФШ - КЦЛИУЛЛ О УЛХЦОРФЧУФИЛУУФЛ МОИФШУФЛ.

В РИ ШЛУЦУЖ, В РИЕУСТГХСОСЖ, В ТФЛШЛГХУ. В ЛКЦЪГБ ЗЦЫЛ ФЕСЛШ ТГЩЛИРХСЕ. Л ПРИ ТСЪИПЦ-ХС ЕФИЖЗГ ТСТГЗГБХФВ СЪИРЯ ЖОЦТЮИ ЗЦЫЛ.

УЙЬЙЩТИТЖ СДИТ ПВЕМЦА. УЙЬЙЩТИЯ ХТХЦДЖПГВЦ ЕТПАЬЧВ ЫДХЦА ЫЙПТЖЙЫЙХЦЖД. РДПТ ЦТЗТ — ПЧЫЬЧВ ЙЗТ ЫДХЦА. УЙЬЙЩТИЯ ХТЛИДПМ РМФ.

ТКУЖЪУЙНСЕ ЖУРБЭЕД ЦСКРУЦЧБ, ЬЧУЖА ФХУЧНЗУЦЧУДЧБ ЗХЕИЕС, ТУ ИУХЕМЙУ ЖУРБЭЕД, ЬЧУЖА ФУОЧН ТЕФКХКПУХ ЙХШМБДС.

ФЗЖ УЛРФШФЦФЛ ИЦЛТЕ ЫЦЖУОСО УЛХФКИОМУФЧШВ О ТФСЭЖУОЛ: ФУ — СДЗЩЕЧВ ЛЛ РЦЖЧФШФП, ФУЖ — ЩКОИСЕЕЧВ ЛЙФ ЗЛНФЗЦЖНОД.

АХС СЪИРЯ ТИЪГОЯРС, НСЖЗГ КГДЮЕГБХ ЗУЦКИМ. РИ Ц ЕФВНСЖС ДЮО ЗУЦЖ. Л В ДСБФЯ ФХГХЯ ХГНЛП, НГН ЕКУСФОЮИ, НСХСУЮП РЛЪХС РИ ЛРХИУИФРС, НУСПИ ЩЛЧУ.

ЙХЦА ЦДОТЙ ЦЖЙФИТЙ УФДЖМПТ. ЖХЦДП УТЧЦФЧ, ЧРЯПХГ, УФМЖЙП ХЙЕГ Ж УТФГИТО - М ХФДЛЧ КЙ УФМЖЙИМ Ж УТФГИТО ХЖТВ УПДСЙЦЧ.

9.2. Примерный перечень тем курсовой работы

Не предусмотрено учебным планом

9.3. Типовые контрольные задания для промежуточной аттестации: зачет

Примерный перечень теоретических вопросов к зачету

1. Выберете этапы процесса оценки риска?
2. Что такое «снижение риска (risk reduction)»?
3. Что такое уязвимость?
4. Что такое угроза информационной безопасности?

5. Что такое атака на информационную систему?
6. Выберите, правильные утверждения:
7. Что такое модель угроз безопасности информации?
8. Что такое атака «отказ в обслуживании»?
9. Что такое не декларируемые возможности программного обеспечения?
10. Какое программное обеспечение может использовать злоумышленник при проникновении в систему?
11. Выберите этапы, через которые проходит злоумышленник при взломе системы?
12. Что такое кейлогер?
13. Какие виды кейлогеров бывают?
14. Что такое атака Brute-force (полный перебор), выберете правильные утверждения?
15. Каким образом можно проверить подозрительные файлы?
16. Что такое антивирусная программа и для чего необходима, выберите правильные утверждения.
17. Что такое «социальная инженерия»?
18. Для каких целей может использоваться «социальная инженерия»?
19. Что такое эксплоит, виды эксплоитов? Выберите правильные утверждения:
20. Какие базовые средства защиты в операционной системе Windows Вы знаете?

Примерный перечень практических заданий к зачету

Используя шифр простой замены “Полибианский квадрат” зашифруйте и расшифруйте сообщение "У меня всё хорошо"

Используя шифр простой замены “Шифр цезаря” зашифруйте и расшифруйте сообщение "Нет необходимости писать"

Используя шифр простой замены “ Шифрующие таблицы Трисемуса”” зашифруйте и расшифруйте сообщение "Не приезжай, опасно"

Используя шифр простой замены “ Шифрующие таблицы Трисемуса” зашифруйте и расшифруйте сообщение "Биграммный шифр Плейфера”

Организуйте удаленное защищенное соеденение с операционной системой используя программы для удаленного администрирования.