МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Проректор по учебной работе

_____
(подпись, ФИО)
«____»_____20__ г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Информационная безопасность

УГСН	09.00.00 Информатика и вычислительная техника
Направление подготовки (специальность)	09.03.01 Информатика и вычислительная техника "Цифровые комплексы, системы и сети"
Квалификация	*Бакалавр*
Форма обучения	*Очная*
Год начала подготовки	*2023*
Объем дисциплины, ч. / з.е. / недели	*144/4/3*
Образовательные технологии	*Традиционные*
Форма контроля (промежуточная аттестация)	*Экзамен*
Подразделение – разработчик	*Кафедра "Вычислительная техника"*

Самара 2023

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы 3

2. Место модуля в структуре образовательной программы 3

3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 4

4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 5

4.1. Содержание лекционных занятий 6

4.2. Содержание лабораторных занятия 7

4.3. Содержание практических занятий 8

4.4. Содержание самостоятельной работы 9

5. Перечень учебной литературы и учебно-методического обеспечения по модулю 9

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 10

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю 10

ПРИЛОЖЕНИЕ 11

Фонд оценочных средств 11

1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 1

Наименование категории (группы) компетенций	**Код и наименование компетенции**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения** (знать, уметь, владеть)
Профессиональные компетенции			
-	ПК-6 Способен проводить работы по установке, настройке, испытаниям и техническому обслуживанию средств защиты информации от несанкционированного доступа	ПК-6.1 Знает угрозы несанкционированного доступа к информации; угрозы специальных программных воздействий на информацию и её носителей; методы и средства защиты информации от несанкционированного доступа	Обладает информацией по проведению работ по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации
		ПК-6.2 Умеет проводить установку, настройку и испытания программных и программно-аппаратных средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами	Умеет проводить работы по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации
		ПК-6.3 Владеет навыками проведения технического обслуживания программно-аппаратных средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами	Владеет навыками работы по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации

2. Место модуля в структуре образовательной программы

Модуль входит в Обязательную часть.

Входные требования:

Предшествующие осваиваемые модули: Учебная практика: проектная практика, Защита информации от утечки по техническим каналам, Теоретические основы обработки сигналов, Методология разработки безопасного программного обеспечения;

Последующие осваиваемые модули: Безопасность вычислительных сетей.

3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Таблица 3

Вид учебной работы	Всего часов	В том числе часов в электронной форме	В том числе часов в форме практической подготовки	Семестр 1 часов/часов в электронной форме/в форме практической подготовки
Аудиторная контактная работа (всего), в том числе:	**40**	**0**	**0**	**40**
лекционные занятия (ЛЗ)	16	0	0	16
лабораторные работы (ЛР)	24	0	0	24
практические занятия (ПЗ)	0	0	0	0
Внеаудиторная контактная работа, КСР	**3**	**0**	**0**	**3**
Самостоятельная работа (всего), в том числе:	**65**	**0**	**0**	**65**
Подготовка к лабораторным работам	*65*	*0*	*0*	*65*
ИТОГО: час.	**108**	**0**	**0**	**108**
ИТОГО: з.е.	**3.0**	**0.0**	**0.0**	**3.0**

4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

Таблица 4

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	**ЛР**	**ПЗ**	**СРС**	**Всего часов**
1.	Защита информации в современных информационных системах	4	0	0	0	4
2.	Подсистема безопасности в ОС семейства Windows	6	12	0	32	50
3.	Подсистема безопасности в ОС семейства UNIX (Linux)	6	12	0	33	51
	КСР					*3*
	Итого:	*16*	*24*	*0*	*65*	*108*

4.1. Содержание лекционных занятий

Таблица 4.1

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количество часов в электронной форме
Семестр 1					
1.	Защита информации в современных информационных системах	Основные понятия и положения защиты информации в информационно вычислительных системах	Основные понятия и положения защиты информации в информационно вычислительных системах	2	0
2.	Защита информации в современных информационных системах	Угрозы безопасности информации в информационно-вычислительных системах. Программно-технический уровень обеспечения информационной безопасности и его организация.	Угрозы безопасности информации в информационно-вычислительных системах. Программно-технический уровень обеспечения информационной безопасности и его организация.	2	0
3.	Подсистема безопасности в ОС семейства Windows	Анализ подсистемы безопасности в ОС семейства Windows. Идентификация, аутентификация и авторизация в ОС семейства Windows	Анализ подсистемы безопасности в ОС семейства Windows. Идентификация, аутентификация и авторизация в ОС семейства Windows	2	0
4.	Подсистема безопасности в ОС семейства Windows	Аудит в ОС семейства Windows. Возможности шифрования файлов в ОС семейства Windows	Аудит в ОС семейства Windows. Возможности шифрования файлов в ОС семейства Windows	2	0
5.	Подсистема безопасности в ОС семейства Windows	Прочие возможности подсистемы безопасности в ОС семейства Windows. Усиление подсистемы безопасности в ОС	Прочие возможности подсистемы безопасности в ОС семейства Windows. Усиление подсистемы безопасности в ОС семейства Windows	2	0

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количество часов в электронной форме
		семейства Windows			
6.	Подсистема безопасности в ОС семейства UNIX (Linux)	Анализ подсистемы безопасности в ОС семейства UNIX	Основные механизмы защиты в ОС семейства UNIX. Особенности организации файловой системы в UNIX. Принципиальные недостатки защитных механизмов ОС семейства UNIX.	2	0
7.	Подсистема безопасности в ОС семейства UNIX (Linux)	Идентификация, аутентификация и авторизация в ОС семейства UNIX	Идентификация, аутентификация и авторизация в ОС семейства UNIX	2	0
8.	Подсистема безопасности в ОС семейства UNIX (Linux)	Аудит в ОС семейства UNIX	Аудит в ОС семейства UNIX	2	0
			Итого за семестр:	*16*	*0*
			Итого:	**16**	**0**

4.2. Содержание лабораторных занятий

Таблица 4.2

№ ЛабЗ	Наименование раздела	Наименование лабораторной работы	Содержание лабораторной работы (перечень рассматриваемых дидактических единиц: подтем, вопросов)	Количество часов	Количество часов в электронной форме	Количество часов в форме практической подготовки
Семестр 1						
1.	Подсистема безопасности в ОС семейства Windows	Анализ подсистемы безопасности в ОС семейства Windows. Пользователи и группы.	Изучение системы администрирования пользователей и групп в операционных системах. Изучение системы защиты информации файловых систем NTFS и ext4fs. Реализация системы разграничение прав доступа к каталогам файловой системы и файлам. Разграничение прав доступа к файловой системе по сети.	2	0	*0*
2.	Подсистема безопасности в ОС семейства Windows	Идентификация, аутентификация и авторизация в ОС семейства Windows. Массовая регистрация пользователей.	Изучение системы администрирования пользователей при помощи стандартного API операционной системы. Изучение методов назначения прав доступа к объектам файловой системы из скриптовых языков.	2	0	*0*
3.	Подсистема безопасности в ОС семейства Windows	Аудит в ОС семейства Windows. Политика безопасности.	Изучение возможности управления групповой политики операционных систем семейства Microsoft Windows.	2	0	*0*

№ ЛабЗ	Наименование раздела	Наименование лабораторной работы	Содержание лабораторной работы (перечень рассматриваемых дидактических единиц: подтем, вопросов)	Количество часов	Количество часов в электронной форме	Количество часов в форме практической подготовки
4.	Подсистема безопасности в ОС семейства Windows	Усиление подсистемы безопасности в ОС семейства Windows. Ограниченное использование программ.	Изучение возможности изменения уровней безопасности операционной системы путем блокирования определённых приложений.	2	0	*0*
5.	Подсистема безопасности в ОС семейства Windows	Возможности шифрования файлов в ОС семейства Windows. Взлом паролей пользователей.	Взлом паролей Microsoft Windows 10	2	0	*0*
6.	Подсистема безопасности в ОС семейства Windows	Усиление подсистемы безопасности в ОС семейства Windows. Прозрачное шифрование файловой системы.	Изучение возможностей применения «прозрачного» шифрования данных в файловых системах.	2	0	*0*
7.	Подсистема безопасности в ОС семейства UNIX (Linux)	Анализ подсистемы безопасности в ОС семейства UNIX. Шифрование и хеширование	Изучение методов контроля целостности и шифрования данных.	2	0	*0*
8.	Подсистема безопасности в ОС семейства UNIX (Linux)	Анализ подсистемы безопасности в ОС семейства UNIX. Шифрование и хеширование	Изучение методов контроля целостности и шифрования данных.	2	0	*0*
9.	Подсистема безопасности в ОС семейства UNIX (Linux)	Отказоустойчивость. RAID массивы.	Изучение возможностей программный средств создания отказоустойчивых хранилищ данных для обеспечения целостности и доступности информации.	2	0	*0*
10.	Подсистема безопасности в ОС семейства UNIX (Linux)	Отказоустойчивость. RAID массивы.	Изучение возможностей программный средств создания отказоустойчивых хранилищ данных для обеспечения целостности и доступности информации.	2	0	*0*
11.	Подсистема безопасности в ОС	Аудит в ОС семейства UNIX. Домены.	Изучение возможностей создания контура безопасности предприятия на основе доменной структуры. Применение групповых политик безопасности к пользователям и	2	0	*0*

№ ЛабЗ	Наименование раздела	Наименование лабораторной работы	Содержание лабораторной работы (перечень рассматриваемых дидактических единиц: подтем, вопросов)	Количество часов	Количество часов в электронной форме	Количество часов в форме практической подготовки
	семейства UNIX (Linux)		компьютерам предприятия.			
12.	Подсистема безопасности в ОС семейства UNIX (Linux)	Аудит в ОС семейства UNIX. Аудит событий.	Изучение механизмов регистрации различных событий в ОС. Ознакомление с методами анализа событий по различным критериям.	2	0	*0*
			Итого за семестр:	*24*	*0*	*0*
			Итого:	**24**	**0**	***0***

4.3. Содержание самостоятельной работы

Таблица 4.4

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
Семестр 1			
Подсистема безопасности в ОС семейства Windows	Подготовка к лабораторным работам	Подсистема безопасности в ОС семейства Windows	32
Подсистема безопасности в ОС семейства UNIX (Linux)	Подготовка к лабораторным работам	Подсистема безопасности в ОС семейства UNIX	33
		Итого за семестр:	*65*
		Итого:	**65**

5. Перечень учебной литературы и учебно-методического обеспечения по модулю

Таблица 5

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ
1.	ОС Windows ОС Linux; Российский новый университет, 2009	ЭБС IPR Books
2.	Таненбаум, Э. Современные операционные системы / Э. Таненбаум .- 2-е изд..- СПб., Питер, 2002.- 1037 с.	Книжный фонд СамГТУ
3.	Немет, Э. UNIX : Рук.систем.администратора / Э.Немет,Г.Снайдер,С.Сибасс,Т.Р.Хейн .- 3-е изд..- М., Питер, 2008.- 924 с.	Книжный фонд СамГТУ
4.	Сетевые средства Linux; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021	ЭБС IPR Books

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

Таблица 6

№ п/п	Наименование	Ссылка на веб-страницу ресурса	Режим доступа
1.	*Scopus: база данных рефератов и цитирования [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.scopus.com*	*Ресурсы ограниченного доступа*
2.	*eLIBRARY.RU (НЭБ - Научная электронная библиотека "Российский индекс научного цитирования") [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.elibrary.ru/*	*Ресурсы открытого доступа*
3.	*УИС РОССИЯ - Университетская информационная система РОССИЯ [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.cir.ru/*	*Ресурсы открытого доступа*
4.	*Единое окно доступа к образовательным ресурсам [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://window.edu.ru/*	*Ресурсы открытого доступа*
5.	*Словари и энциклопедии on-line [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://dic.academic.ru/*	*Ресурсы открытого доступа*

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю

Лекционные занятия проводятся в:
Корпус № 8/113 - Учебная аудитория.

Практические занятия не предусмотрены.

Самостоятельная работа проводятся в:
Корпус № 8/200 - Читальный зал.

Лабораторные занятия проводятся в:
Корпус № 8/109 - Учебная лаборатория.

ПРИЛОЖЕНИЕ
Фонд оценочных средств

Фонд оценочных средств для текущего контроля успеваемости, промежуточной аттестации обучающихся по модулю

Настоящий Фонд оценочных средств (ФОС) по модулю Безопасность операционных систем является неотъемлемым приложением к рабочей программе модуля. На данный ФОС распространяются все реквизиты утверждения, представленные в рабочей программе модуля.

1. Перечень оценочных средств

Таблица 1

№ п/п	Оценочное средство	Краткая характеристика оценочного средства	Количество	Представление оценочного средства в ФОС
1	Устный опрос	Диалог преподавателя со студентом, цель которого – систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала.	3	Перечень вопросов для обсуждения

Раздел 2. Этапы формирования компетенций, соотнесенные с видами оценочных средств

Таблица 2

Контролируемые разделы модуля	Код и формулировка индикатора компетенции	Результат обучения	Оценочные средства	Номер оценочного средства
Защита информации в современных информационных системах	ПК-6.1 Знает угрозы несанкционированного доступа к информации; угрозы специальных программных воздействий на информацию и её носителей; методы и средства защиты информации от несанкционированного доступа	Обладает информацией по проведению работ по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации	Устный опрос	1
Подсистема безопасности в ОС семейства Windows	ПК-6.2 Умеет проводить установку, настройку и испытания программных и программно-аппаратных средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами	Умеет проводить работы по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации	Устный опрос	2

Подсистема безопасности в ОС семейства UNIX (Linux)	ПК-6.3 Владеет навыками проведения технического обслуживания программно-аппаратных средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами	Владеет навыками работы по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации	Устный опрос	3

3. Содержание оценочных средств текущего контроля

Оценочное средство 1:
Содержание оценочных средств текущего контроля находятся в файле "Вопросы к тестированию.pdf"

4. Содержание оценочных средств промежуточной аттестации

Формат контроля промежуточной аттестации: *Компьютерное тестирование.*

Форма проведения промежуточной аттестации: .

Типовые задания: Содержание оценочных средств текущего контроля находятся в файле "Вопросы к тестированию.pdf".

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций *(данный раздел находится в разработки в части БРТ)*

Модуль состоит из набора разделов. Объем учебного раздела раскрывает отдельную (ые) тему(ы) дисциплины / этап прохождения практики. Модуль разбивается на 2-4 раздела в семестр.

Раздел состоит из учебных элементов (дидактических единиц). Объем учебного материала учебного элемента раскрывает отдельный вопрос темы или тему дисциплины (если раздел содержит несколько тем). Путем набора соответствующих учебных элементов формируется раздел, содержание которого соответствует запланированным результатам освоения ОП согласно учебному плану.

По каждому разделу устанавливается перечень обязательных видов работы студента, включающий: посещение лекционных, практических (семинарских, лабораторных) занятий; ответы на теоретические вопросы на семинаре; решение практических задач и выполнение заданий на практическом занятии; выполнение лабораторных работ; выполнение контрольных работ; написание рефератов; участие в коллоквиумах по отдельным темам; тестирование по теме (группе тем); другие виды работ, определяемые преподавателем (в соответствии с установленными требованиями балльно-рейтинговой технологии).

Каждый раздел завершается определенной (ыми) формой (ами) контроля для оценки уровня усвоения учебного материала и определения рейтинговой оценки качества усвоения учебного материала.

Рейтинговая оценка знаний студентов определяется по 100-балльной шкале в каждом семестре и включает текущий, рубежный и итоговый контроль.

Распределение баллов рейтинговой оценки между видами контроля

Таблица 3

Форма промежуточной аттестации	Количество баллов			
	Текущий контроль	Рубежный контроль	Итоговый контроль	Сумма баллов
Экзамен	0	0	30	30

Перевод оценок 100-балльной шкалы в оценки промежуточной аттестации

Таблица 4

100-балльная шкала	85-100	70-84	50-69	0-49
5-балльная шкала	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно

Бинарная шкала	Зачтено	Не зачтено

Распределение рейтинговых баллов по разделам модуля с указанием применяемых для их начисления оценочных средств представлено в Технологической карте БРТ.

Раздел УМ	Оценочные средства		Итого
	Устный опрос	**Экзамен**	
Раздел 1			
ЛЗ 1.1	0		0
ЛЗ 1.2	10		10
Итого по разделу 1	10		10
Раздел 2			
ЛЗ 2.1	0		0
ЛЗ 2.2	30		30
Итого по разделу 2	30		30
Раздел 3			
ЛЗ 3.1	0		0
ЛЗ 3.2	30		30
Итого по разделу 3	30		30
Промежуточная аттестация		30	30
Итого	70	30	100

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения дисциплины:

Теоретические вопросы для подготовки к промежуточной аттестации (Экзамен):

1. Шаблоны безопасности в ОС семейства Windows.
2. Подсистема защиты в ОС семейства Windows.
3. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства Windows.
4. Возможности усиления подсистемы безопасности в ОС семейства Windows.
5. Противодействие вирусным атакам в системе. Выбор антивируса.
6. Организация антивирусной защиты.
7. Основные механизмы защиты в ОС семейства UNIX
8. Принципиальные недостатки защитных механизмов ОС семейства UNIX
9. Особенности подсистемы безопасности в ОС семейства UNIX.
10. Механизм идентификации пользователей в ОС семейства UNIX.
11. Механизм аутентификации пользователей в ОС семейства UNIX.
12. Подключаемые модули аутентификации PAM и работе с ними в ОС семейства UNIX.
13. Механизм разграничения доступа к файлам в ОС семейства UNIX.
14. Система шифрования файлов PGP в ОС семейства UNIX.
15. Конфигурация подсистемы защиты в ОС семейства UNIX.
16. Выявление и устранение уязвимости в подсистеме защиты в ОС семейства UNIX.
17. Bash-скрипты и работа с ними в ОС семейства UNIX.
18. Возможности усиления подсистемы безопасности в ОС семейства UNIX
19. Централизованная система регистрации системных сообщений Syslog. Возможности системы Syslog.
20. Шифование файлов при помощи PGP. Особенности PGP
21. Подсистема аудита в UNIX
22. Ведение и анализ журналов безопасности в ОС