

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 26.09.2023 11:13:25  
Уникальный программный ключ:  
27e516f4c088deb62ba68945f4406e13fd454355

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**Федеральное государственное бюджетное образовательное учреждение высшего образования**  
**«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ**  
**УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»**  
**(ТУСУР)**

**АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ**

**УПРАВЛЕНИЕ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ**

Уровень образования: **высшее образование - специалитет**  
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**  
Направленность (профиль) / специализация: **Безопасность автоматизированных систем в кредитно-финансовой сфере**  
Форма обучения: **очная**  
Факультет: **Факультет безопасности (ФБ)**  
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**  
Курс: **4**  
Семестр: **7**  
Учебный план набора 2021 года

**Объем дисциплины и виды учебной деятельности**

Виды учебной деятельности	7 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Лабораторные занятия	36	36	часов
Курсовая работа	36	36	часов
Самостоятельная работа	54	54	часов
Общая трудоемкость	144	144	часов
(включая промежуточную аттестацию)	4	4	з.е.

Формы промежуточной аттестация	Семестр
Зачет	7
Курсовая работа	7

## 1. Общие положения

### 1.1. Цели дисциплины

1. Целью преподавания дисциплины является освоение методов мониторинга и управления программными средствами защиты информации, реализованными на основе клиент-серверной технологии.

### 1.2. Задачи дисциплины

1. Получение знаний и умений по методам сбора и аудита событий информационной безопасности в современных средствах защиты информации.

2. Получение умений и навыков централизованного управления клиентскими модулями средств защиты информации и реагирования на угрозы безопасности.

3. Получение знаний о методах контроля работоспособности и целостности клиентских модулей средств защиты информации.

4. Изучение методов контроля и оценки установленного программного и аппаратного обеспечения на защищаемых компьютерах в локальной сети.

5. Изучение методов обеспечения и контроля антивирусной защиты рабочих станций в сети организации.

## 2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль специальности (special hard skills - SHS).

Индекс дисциплины: Б1.О.03.20.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

## 3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции
<b>Универсальные компетенции</b>	
-	-
<b>Общепрофессиональные компетенции</b>	
ОПК-13. Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ОПК-13.1. Знает методики измерения и оценки параметров в автоматизированных системах, типовые средства для инструментальной оценки уровня защищённости автоматизированных систем
	ОПК-13.2. Умеет проводить анализ защищенности информации от несанкционированного доступа в автоматизированных системах
	ОПК-13.3. Владеет навыками организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем при расследовании компьютерных преступлений и инцидентов

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1. Знает критерии оценки защищенности автоматизированной системы, технические средства контроля эффективности мер защиты информации
	ОПК-15.2. Умеет осуществлять контроль обеспечения уровня защищенности в автоматизированных системах, документировать процедуры и результаты контроля функционирования системы защиты информации автоматизированной системы
	ОПК-15.3. Владеет навыками оценки защищенности автоматизированных систем с помощью типовых программных средств
<b>Профессиональные компетенции</b>	
-	-

#### 4. Названия разделов (тем) дисциплины

Названия разделов (тем) дисциплины
<b>7 семестр</b>
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети
2 Централизованная инвентаризация ресурсов локальной сети. Удалённый контроль работоспособности средств защиты информации на рабочих станциях
3 Централизованная защита от вирусов в локальной сети
4 Централизованный учет и управление средствами персональной идентификации и аутентификации
5 Анализ нормативных требований по управлению средствами защиты информации