

Документ подписан электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 26.09.2023 10:54:08  
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: **Информационная безопасность автоматизированных банковских систем**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**

Курс: **3, 4**

Семестр: **6, 7**

Учебный план набора 2016 года

**Распределение рабочего времени**

№	Виды учебной деятельности	6 семестр	7 семестр	Всего	Единицы
1	Лекции	18	0	18	часов
2	Лабораторные работы	28	0	28	часов
3	Контроль самостоятельной работы (курсовой проект / курсовая работа)	0	18	18	часов
4	Всего аудиторных занятий	46	18	64	часов
5	Из них в интерактивной форме	16	0	16	часов
6	Самостоятельная работа	26	18	44	часов
7	Всего (без экзамена)	72	36	108	часов
8	Общая трудоемкость	72	36	108	часов
		2.0	1.0	3.0	З.Е.

Зачёт: 6 семестр

Курсовой проект / курсовая работа: 7 семестр

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

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

### 1.2. Задачи дисциплины

- Получение знаний и умений по методам сбора и аудита событий информационной безопасности в современных средствах защиты информации;
- Получение умений и навыков централизованного управления клиентскими модулями и реагирования на угрозы безопасности;
- Получение знаний о методах контроля работоспособности и целостности клиентских модулей средств защиты информации;
- Изучение методов контроля и оценки установленного программного и аппаратного обеспечения на защищаемых компьютерах в локальной сети;
- Изучение методов обеспечения и контроля антивирусной защиты рабочих станций в сети организации.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Управление средствами защиты информации» (Б1.В.ОД.13) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Безопасность операционных систем, Безопасность сетей ЭВМ, Организационное и правовое обеспечение информационной безопасности, Управление средствами защиты информации.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Программно-аппаратные средства обеспечения информационной безопасности, Управление средствами защиты информации.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;
- ПК-26 способностью администрировать подсистему информационной безопасности автоматизированной системы;
- ПК-28 способностью управлять информационной безопасностью автоматизированной системы;

В результате изучения дисциплины обучающийся должен:

- **знать** принципы организации информационных систем в соответствии с требованиями по защите информации; возможности и назначение современных средств защиты информации от несанкционированного доступа.
- **уметь** выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных средств защиты информации; организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; администрировать подсистему информационной безопасности автоматизированной системы; управлять информационной безопасностью автоматизированной системы; эффективно использовать различные методы и средства защиты информации для компьютерных сетей; администрировать подсистемы информационной безопасности автоматизированных систем.
- **владеть** способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы; навыками выявления и уничтожения компьютерных вирусов; методами и средствами выявления угроз безопасности автоматизированным системам.

## 4. Название разделов (тем) дисциплины

Названия разделов дисциплины
6 семестр
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 программно-аппаратными средствами защиты информации.
6 Анализ нормативных требований по управлению средствами защиты информации
7 семестр
5 Администрирование и управление средствами защиты информации от несанкционированного доступа.