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: **4**
Семестр: **7**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	36	36	часов
3	Контроль самостоятельной работы (курсовой проект / курсовая работа)	18	18	часов
4	Всего аудиторных занятий	72	72	часов
5	Самостоятельная работа	72	72	часов
6	Всего (без экзамена)	144	144	часов
7	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Зачёт: 7 семестр
Курсовой проект / курсовая работа: 7 семестр

Томск

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.03.03) относится к блоку 1 (вариативная часть).

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

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы;

– 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; эффективно использовать различные методы и средства защиты информации для компьютерных сетей; обеспечивать централизованное управление средствами защиты информации автоматизированных систем предприятия; администрировать подсистемы информационной безопасности автоматизированных систем.

– **владеть** навыками анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; навыками выявления и уничтожения компьютерных вирусов; методами и средствами выявления угроз безопасности автоматизированным системам.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины

7 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.
5 Администрирование и управление средствами защиты информации от несанкционированного доступа.
6 Анализ нормативных требований по управлению средствами защиты информации