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 инцидентами и непрерывностью бизнеса

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: **5**
Семестр: **9**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	54	54	часов
5	Всего (без экзамена)	108	108	часов
6	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 9 семестр

Томск

1. Цели и задачи дисциплины

1.1. Цели дисциплины

дать основы управления инцидентами информационное безопасности, а также формирование знаний процессах и системах управления инцидентами информационной безопасности и непрерывностью бизенса.

1.2. Задачи дисциплины

- дать основы:
- - нормативного обеспечений управления инцидентами информационной безопасности и непрерывностью бизнеса;
- - планирования, подготовки, использования, анализа и улучшения процесса управления инцидентами информационной безопасности;
- - документации системы управления инцидентами информационной безопасности;
- - реагирования на инциденты информационной безопасности;
- - функционала инструментальных средств управления событиями информационной безопасности;
- - циклической модели улучшения процессов.
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Управление инцидентами и непрерывностью бизнеса» (Б1.В.05.01) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Базы данных и экспертные системы, Управление средствами защиты информации.

Последующими дисциплинами являются: Управление информационной безопасностью.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-20 способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
- ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы;
- ПСК-5.5 способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы;
- ПСК-5.1 способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;

В результате изучения дисциплины обучающийся должен:

- **знать** принципы построения системы управления информационной безопасности объекта в части систем управления инцидентами информационной безопасности и непрерывности бизнеса, современные подходы к управлению инцидентами информационной безопасности и непрерывности бизнеса объекта и направления их развития, основные международные и российские стандарты, регламентирующие управление инцидентами информационной безопасности и непрерывности бизнеса, принципы разработки процессов управления инцидентами информационной безопасности и непрерывности бизнеса, принципы создания основных документов, регламентирующих вопросы управления инцидентами информационной безопасности и непрерывности бизнеса
- **уметь** анализировать текущее состояние информационной безопасности на предприятии с целью разработки требований к разрабатываемым процессам управления инцидентами информационной безопасностью и непрерывностью бизнеса. Определять цели и задачи, решаемые разрабатываемыми процессами управления инцидентами информационной безопасности и непрерывности бизнеса .Применять процессный подход к управлению инцидентами информационной безопасности и и непрерывности бизнеса. Используя современные методы и средства, разрабатывать процессы управления инцидентами информационной безопасности и и непрерывности бизне-

са учитывающие особенности функционирования предприятий и решаемых ими задач, и оценивать их эффективность. Разрабатывать документальное обеспечение для процессов управления инцидентами информационной безопасности и и непрерывности бизнеса, включая различные политики и применять его на практике.

– **владеть** терминологией и процессным подходом построения систем управления инцидентами информационной безопасности и систем управления непрерывностью бизнеса. Навыками построения как отдельных процессов управления инцидентами управления инцидентами информационной безопасности и и непрерывности бизнеса, так и систем процессов в целом.

4. Название разделов (тем) дисциплины

Названия разделов дисциплины
9 семестр
1 Нормативная база управления инцидентами информационной безопасности и обеспечение непрерывности бизнеса
2 Управление инцидентами информационной безопасности
3 Управление непрерывностью бизнеса организации