АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

(название дисциплины)

10.04.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(код направления (специальности) подготовки)

1,2,3

(семестр)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

– Целью освоения дисциплины «Администрирование информационной безопасности в распределенных информационно-вычислительных системах» являются обеспечение подготовки специалистов в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.04.01 «Информационная безопасность». Целью освоения дисциплины является формирование у студентов теоретических знаний и практических навыков по управлению информационной безопасностью автоматизированных систем. Кроме того, курс обеспечивает формирование у магистрантов обобщенного представления о методах анализа, оценки и управления рисками в условиях существования угроз, а также при разработке и принятии управленческих решений в условиях неопределенности и риска, характерных для функционирования современных предприятий.

– Задачами дисциплины «Администрирование информационной безопасности в распределенных информационно-вычислительных системах» являются: - освоение принципов реализации и основных подходов к оптимальному управлению различными механизмами информационной безопасности в системах. Формирование представлений: - о риске, его видах и источниках возникновения; - о количественных и качественных методах анализа и оценки риска; - о методах управления рисками и снижения их последствий; - о функционировании риск-менеджмента на современном предприятии.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

– Данная дисциплина относится к базовым дисциплинам Блока Б1 (код Б1.В.01). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и лабораторных работ.

– Дисциплина изучается на 1 и 2 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по направлению 10.04.01 по курсам «Анализ и моделирование информационно-телекоммуникационных сетей», «Методы и средства защиты объектов информатизации», «Методология информационной безопасности», «Оценка и контроль обеспечения информационной безопасности», «Методы информационно-аналитической работы».

– Кроме того, требования к «входным» знаниям, умениям и готовностям обучающегося определяются требованиями к уровню подготовки выпускника бакалавриата при освоении курсов «Защита информации в корпоративных информационных системах» или аналогичных, в соответствии с программой подготовки бакалавров в следующих или смежных областях знаний: -информационная безопасность; -энергетика, энергетическое машиностроение и электротехника; -авиационная и ракетно-космическая техника; -фотоника, приборостроение, -оптические и биотехнические системы и технологии; -электронная техника, радиотехника и связь; -автоматика и управление; -информатика и вычислительная техника; -физико-технические науки и технологии; -управление в технических системах.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими общекультурными и профессиональными компетенциями:

– ПК-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации;

– ПК-13 – способностью организовать управление информационной безопасностью.

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

- Адекватная безопасность. Базовый уровень безопасности. Компрометация.
- Риск. Риски, связанные с информационными технологиями. Остаточный риск.
- Санкционирование безопасной эксплуатации. Категория безопасности. Уровень защищенности.
- Основные определения и критерии классификации угроз
- Угроза. Атака. Злоумышленник. Источники угроз.
- Основные источники внутренних отказов. Примеры угроз доступности.
- Основные угрозы целостности. Угрозы статической и динамической целостности.
- Общие положения управления рисками
- Цикл управления рисками: (пере)оценка (измерение) рисков; выбор эффективных и экономичных защитных средств (нейтрализация рисков).
- Основные этапы управления рисками.
- Интегрирование управления рисками в жизненный цикл ИС на этапах инициации.
- Подготовительные этапы управления рискам.
- Инфологическая модель. Карта информационной системы организации.
- Идентификация активов,
- Анализ угроз и оценка рисков
- Перечень наиболее распространенных угроз. Модель угроз организации.
- Оценка стоимости защитных мер.
- Проблема совместимости нового средства защитных мер со сложившейся организационной и аппаратно-программной структурой, с традициями организации.
- План тестирования (автономного и комплексного) программно-технических механизмов защиты. Проверка того, что остаточные риски стали приемлемыми.
- Выявление источников возникновения угроз. Типы злоумышленников.
- Метрики, используемые для оценки вероятности осуществления угрозы. Размер потенциального ущерба.
- Управление рисками как деятельность административного уровня информационной безопасности.
- Роли в этой деятельности: руководителя организации, начальника управления (отдела) информатизации, владельцев систем и информации, руководителей производственных отделов и отдела закупок.
- Роли в этой деятельности: начальника отдела (управления) информационной безопасности, администраторов безопасности, системных и сетевых администраторов, специалистов по обучению персонала.
- Детальное рассмотрение процесса оценки рисков
- Девять основных этапов процесса оценки рисков, их входная и выходная информация. Определение характеристик информационной системы. Информация об эксплуатационном окружении системы.
- Методы получения информации: вопросники, интервью, просмотр документации. Применение инструментов автоматического сканирования. Идентификация уязвимостей на стадии проектирования ИС, на этапе реализации, на этапе эксплуатации.
- Автоматические средства сканирования, средства тестирования и оценки, тестирование проникновением.
- Результирующая документация. Определение приоритетов, оценка и реализация контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков.
- Различные возможности в процессе управления рисками: принятие риска; уклонение от риска.
- Возможный формат отчета об оценке рисков. Возможный формат плана реализации контрмер.

Составитель: доц. кафедры ИЗИ к.т.н., Мишин Д.В.

должность, ФИО, подпись

Заведующий кафедрой ИЗИ М.Ю. Монахов

ФИО, подпись

Директор института ИТР А.А. Галкин

ФИО, подпись

Дата, Печать института (факультета)