МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»

Снежинский физико-технический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
(СФТИ НИЯУ МИФИ)

«УТВЕРЖДАЮ»
Зам. руководителя по учебной
и научно-методической работе
_____П.О.Румянцев
«_____»_____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации
наименование дисциплины

Направление подготовки (специальность) __38.05.01 «Экономическая безопасность»

Специализация «Экономист»

Квалификация (степень) выпускника_____Специалист_____

Форма обучения_____очная_____

г. Снежинск
2021 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель преподавания дисциплины

Целью настоящего курса является изучение современных принципов и методов защиты данных и компьютерной безопасности при обработке информации в вычислительных системах, что является необходимым условием обеспечения жизнедеятельности компьютерных систем.

Задачи изучения дисциплины

Задачами изучения курса являются приобретение систематизированных знаний и представлений о методологии, обеспечивающей комплексный подход к построению систем защиты информации и компьютерной безопасности в автоматизированных системах; принципах построения систем защиты, определении системно-концептуального подхода к защите; способах, методах и средствах защиты информации и компьютерной безопасности. А также умение использовать основные правила, которыми необходимо руководствоваться при организации защиты; методами создания механизмов защиты; знать термины и определения; анализ риска и оценку эффективности используемых средств и методов защиты.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Защита информации» относится к Блоку 1 Общепрофессионального модуля рабочего учебного плана специальности 38. 05. 01. «Экономическая безопасность» и изучается одновременно с такими дисциплинами как «Антикоррупционные законодательство и политика», «Государственная система правоохранительных органов» на четвертом курсе в восьмом семестре.

3. КОМПЕТЕНЦИИ СТУДЕНТА, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ / ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОБРАЗОВАНИЯ И КОМПЕТЕНЦИИ СТУДЕНТА ПО ЗАВЕРШЕНИИ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими компетенциями:

Способностью работать с различными источниками информации, информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, применять в профессиональной деятельности автоматизированные информационные системы, используемые в экономике, автоматизированные рабочие места, проводить информационно-поисковую работу с последующим использованием данных при решении профессиональных задач (ОК-16).

В результате освоения курса студент должен:

Знать: основные понятия и направления в защите компьютерной информации, принципы защиты информации, принципы классификации и примеры угроз безопасности компьютерным системам, современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности, основные инструменты обеспечения многоуровневой безопасности в информационных системах.

Уметь: конфигурировать встроенные средства безопасности в операционной системе, проводить анализ защищенности компьютера и сетевой среды с использованием сканера безопасности; устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; устанавливать и использовать один из межсетевых экранов; устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; настроить инструменты резервного копирования и восстановления информации.

Владеть: методами аудита безопасности информационных систем, методами системного анализа информационных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет ____4____ кредита, _144_____ часа.

№ п/п	Раздел учебной дисциплины	Недели	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах)			Текущий контроль успеваемости *(неделя, форма)*	Аттестация раздела *(неделя, форма)*	Максимальный балл за раздел *
			Лекции	Практ. занятия/ семинары	Лаб. работы			
_8_ семестр								
1	Анализ концептуальных подходов к защите информации в системах обработки данных.	1-4	2	8	-			
2	Анализ средств защиты информации.	5-7	4	10	-	4, домашняя работа		10
3	Нейтрализация излучений и наводок.	8-10	2	8	-			
4	Криптографические методы и способы закрытия информации. Изучение и практическая реализация современных методик защиты	11-14	4	10	-		11,14 контрольная работа №1 и №2	30

№ п/п	Раздел учебной дисциплины	Недели	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах)			Текущий контроль успеваемости *(неделя, форма)*	Аттестация раздела *(неделя, форма)*	Максимальный балл за раздел *
			Лекции	Практ. занятия/ семинары	Лаб. работы			
	компьютерной информации.							
5	Порядок разработки механизма защиты. Асимметричная криптография и электронная цифровая подпись.	15-16	2	8	-	16, практическая работа		10
6	Система правового регулирования в области защиты информации.	17-18	4	10	-			
…	Экзамен							0 - 50
	Итого за 8 семестр:							100

* *100 баллов за семестр, включая зачет или экзамен.*

Содержание тем лекционных занятий

2.1 Введение.

- Предмет и структура курса. Связь со смежными курсами. Проблемы защиты информации в системах электронной обработки данных (СОД). Аспекты уязвимости информации. Примеры несанкционированных действий в СОД. Пути несанкционированного получения информации. Наиболее вероятные каналы утечки информации и организации несанкционированного доступа к защищаемым данным. Классификация каналов утечки информации.

2.2 Анализ концептуальных подходов к защите информации в системах обработки данных.

- Этапы развития проблемы защиты информации в СОД как самостоятельного направления. Характеристика этапов. Особенности. Основные механизмы защиты на каждом этапе. Теорема Харрисона. Системность подхода к самой проблеме защиты информации. Целостный механизм-система защиты. Модель защиты- защитные пояса. Стандартизация в области защиты информации. Основные термины и определения.
- Обзор “Оранжевой книги”. Уровни “Оранжевой книги”. Краткая характеристика уровней D,C,B,A. Программа компьютерной безопасности DOE. Элементы программы: управление риском; требования и руководства - индексы защиты (Protection Index - PI); структура управления обеспечением компьютерной безопасности. План безопасности DOE. Содержание плана безопасности: введение; спецификация требований безопасности; описание системы; управление конфигурацией; риск и уязвимость; меры безопасности.

2.3. Анализ средств защиты информации.

- Классификация способов и средств защиты информации: способы - препятствия, управление, кодирование информации, регламентация, принуждение, побуждение; средства - формальные (физические, аппаратные - технические; программные), неформальные - организационные, законодательные, морально-этические.

- Технические средства защиты информации. Объекты применения и задачи средств физической защиты. Краткая характеристика средств физической защиты: датчики различных типов; теле- и фотосистемы наблюдения; СВЧ- и радиолокационные системы; лазерные системы; оптические системы в видимой части спектра; акустические системы; устройства маркировки; кабельные системы; устройства с идентификационными картами; системы опознавания по голосу, по отпечаткам пальцев, по почерку, по геометрии руки, по сетчатке глаза.
- Аппаратные средства защиты информации, применяемые в центральном процессоре, в ОЗУ, в процессоре управления вводом-выводом, в управлении внешними запоминающими устройствами, общие аппаратные методы защиты.

2.4. Нейтрализация излучений и наводок.

- Безопасность излучений и наводок от средств ЭВТ. Структура электромагнитного излучения дисплея. Энергетический спектр видеосигнала. Восстановление информации по электромагнитному излучению дисплея. Повышение безопасности электромагнитного излучения дисплея. Безопасность электромагнитного излучения кабелей передачи данных. Наводки между проводами и кабелями.

2.5. Криптографические методы и способы закрытия информации.

-Терминология и некоторые допущения. Криптология. Правило Керкхоффа. Потребность в криптологии. Периоды развития криптологии. Шифр Вернама. Код Бодо.
- Шифрование информации методом замены. Таблицы Вижинера. Пример.
- Шифрование по методу перестановки. Маршруты Гамильтона. Пример.
-Шифрование методом гаммирования. Правила логической эквивалентности и логической неэквивалентности. Пример.
- Шифрование с использованием методов алгебры матриц. Пример.
-Аппаратная реализация криптосистем. Пример аппаратной реализации криптосистемы. Схема шифратора “Lucifer”. Алгоритм шифрования и расшифрования. Преимущества аппаратной реализации алгоритма шифрования.
-Зарождение стандарта шифрования данных DES (Data Encryption Standard). Шифрование данных. Модель криптографической системы. Вопросы Шеннона о стойкости криптосистем с теоретической и практической точек зрения. Стандарт шифрования данных. Структура стандарта шифрования.
-Криптографические системы с открытым ключом. Использование необратимых или односторонних функций. Криптосистема Р. Ривеста, А. Шамира, Л. Адельмана (RSA) с ключом общего пользования. Концепция метода RSA. Пример шифрования и расшифрования методом RSA. Стойкость криптографических систем с открытым ключом.
-Криптосистема на основе математической теории хаоса. Использование логистического уравнения в конечных разностях как одной из простейших нелинейных функций, обладающих хаотическими свойствами. Структурная схема аппаратной реализации системы шифрования. Новые направления применения криптографических методов защиты - электронные ключевые подписи.
-Отечественный стандарт на шифрование данных - ГОСТ 28147-89. Сертифицированная система криптографической защиты информации (СКЗИ) “Верба”. Модификации СКЗИ “Верба” - “Верба - 0”, аппаратно-программный комплекс “Титан”, комплекс криптографических средств защиты (ККСЗ) информации “Янтарь”. Краткая характеристика.

2.6. Порядок разработки механизма защиты.

- Организационные меры защиты и порядок разработки механизма защиты. Программа внедрения средств, методов и мероприятий по защите информации. Порядок разработки механизма защиты.

2.7. Система правового регулирования в области защиты информации.

- Гражданский кодекс Российской Федерации. Федеральный закон “О государственной тайне”. Конституция Российской Федерации. Законодательные акты: Гражданский Кодекс Российской Федерации, Уголовный Кодекс Российской Федерации, Федеральные законы. Основные цели защиты информации, определенные законодательно. Подлежащая защите информация.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

IT — методы:

- практические/семинарские занятия — 36 часов;
- самостоятельная работа студентов — 36 часов.

Исследовательский метод — работа над домашним заданием.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов представлены в фонде оценочных средств.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

а) основная литература:

1. Аскеров Т.М. «SD Информатика» (часть 6. Информационная безопасность и защита информации) – Термика, Москва. [электронный ресурс]

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Аудитория №201, оснащенная экраном, проектором и компьютером.