



Направление подготовки 10.04.01 «Информационная безопасность»
 Магистерская программа «Безопасность автоматизированных систем»
 Аннотация к РПД Б1.О.05 «Технологии обеспечения информационной безопасности»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

10.04.01 «Информационная безопасность»

Магистерская программа: Безопасность автоматизированных систем

Б1.О.05 «Технологии обеспечения информационной безопасности»

Индекс	Наименование	Семестр 2										Итого за курс												
		Академических часов					Кон- троль	з.е.	Академических часов					з.е.										
		Всего	Кон такт.	Лек	Лаб	Пр			КРП	СР	Кон- троль	Всего	Кон такт.		Лек	Лаб	Пр	КРП	СР	Кон- троль				
Б1.О.05	Технологии обеспечения информационной безопасности	144	68	34	34							Экз РГР	4	144	68	34	34					40	36	4

Формируемые компетенции: ОПК-1, ОПК-2

Содержание дисциплины

№	Наименование видов занятий и тематик, содержание
1	<p>Лекционные занятия 17 шт. по 2 часа:</p> <p><i>1.1. Основы информационной безопасности (ИБ).</i> Определенные цели и принципы защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности.</p> <p><i>1.2. Классификация методов и средств защиты информации.</i> Глубина классификации и репутит. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно-техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде.</p> <p><i>1.3. Задачи информационной безопасности.</i> Задача обеспечения конфиденциальности. Задача обеспечения аутентификации. Задача обеспечения идентификации. Задача обеспечения целостности.</p> <p><i>1.4. Угрозы информационной безопасности.</i></p>

Классификация угроз информационной безопасности. Угрозы несанкционированного доступа к данным. Угрозы нарушения целостности данных. Угрозы нарушения конфиденциальности данных.

1.5. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.

Основы законодательства в области обеспечения информационной безопасности. Правовое обеспечение информационной безопасности. Закон «Об информации, информатизации и защите информации». Защита персональных данных. Другие законы и нормативные акты.

1.6. Понятие и виды защищаемой информации.

Путь конфиденциального документа от создания до уничтожения: решение, разработка проекта, подготовка содержания, реквизитов, передача, получение, исполнение и архивация. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Защита конфиденциальной информации при ее передаче по сети. Система защищенного электронного документооборота.

1.7. Защита информации. Общая характеристика способов и средств защиты информации.

Способы и средства защиты информации от несанкционированного доступа. Способы и средства защиты информации от вредоносного кода. Способы и средства защиты информации от межсетевых воздействий. Способы и средства криптографической защиты информации.

1.8. Криптографические методы защиты информации.

Основные понятия и термины криптографии. Краткая история развития шифров. Примеры. Основные проблемы криптографии. Параллельные системы. Оценка секретных систем. Криптостойкость. Методы криптоанализа и взлома.

1.9. Криптографические методы защиты информации. Одностороннее шифрование.

Виды алгоритмов хэширования. Алгоритмы выработки имитовставки. Гаммирование. Хэш-функции. Семейство алгоритмов SHA.

1.10. Криптографические методы защиты информации. Симметричное шифрование.

Виды алгоритмов хэширования. Алгоритмы выработки имитовставки. Гаммирование. Хэш-функции. Алгоритм SHA. Симметричные шифры. Криптография с открытым ключом. Блочные и потоковые шифры. Алгоритмы DES, AES.

1.11. Криптографические методы защиты информации. Асимметричное шифрование.

Асимметричное шифрование, преимущества и недостатки. Понятие открытого и закрытого ключа. Алгоритм Диффи – Хеллмана. Схема алгоритма RSA.

1.12. Электронная цифровая подпись и цифровые сертификаты.

Электронная цифровая подпись. Понятие о цифровой подписи. Подпись RSA. Подпись ElGamal. Подпись DSA. ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01. Инфраструктура открытых ключей. Сертификаты открытых ключей.

1.13. Обеспечение высокой доступности, туннелированные и управление.

Методы и средства обеспечения высокой доступности. Проактивное управление, задание реакций, резервное копирование. Синхронное и асинхронное тиражирование. Туннелирование данных. Мониторинг и контроль.

1.14. Практические аспекты криптографии.

Способы взлома и кражи данных в сетях. Защита протокола WiFi. Протокол HTTPS. Виртуальные персональные сетевые каналы VPS. Схема работы протокола TOR. Сетевой протокол прикладного уровня, позволяющий производить удалённое управление SSH.

1.15. Методы организации безопасного доступа.

	<p>Схемы идентификации и аутентификации. Одно- и многофакторная аутентификация. Система разграничения доступа к информации в компьютерной системе. Концепция построения систем разграничения доступа. Средства и методы ограничения доступа к файлам.</p> <p><i>1.16. Программно-аппаратные средства защиты информации.</i></p> <p>Аппаратные и программно-аппаратные средства криптозащиты данных. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев». Защита программ от несанкционированного копирования.</p> <p><i>1.17. Классификация вирусов. Применение антивирусных программ.</i></p> <p>Классификация вирусных программ. Основные признаки заражения от вредоносных программ. Методы заражения. История антивирусных программ, сведения о надежности и механизмах работы современных антивирусных программ. Основные моменты использования современных антивирусных программ.</p>
2	<p>Лабораторные работы 9 шт. по 4 (2) часа:</p> <p><i>2.1. Перехват и анализ сетевых пакетов.</i> Изучить возможности библиотеки WinPcap, Изучить возможности библиотеки SharpPcap; осуществить перехват и анализ сетевых пакетов на сетевом транспортном и прикладном уровнях модели OSI.</p> <p><i>2.2. Современные симметричные криптосистемы.</i> Изучение принципов работы симметричных криптосистем, многие из которых являются национальными или ведомственными стандартами; изучение реализации симметричной криптографии в среде .NET Framework; программная реализация существующих симметричных криптоалгоритмов.</p> <p><i>2.3. Современные асимметричные криптосистемы.</i> Изучение принципов работы асимметричных криптосистем; изучение реализаций асимметричной криптографии в среде .NET Framework; реализация существующих асимметричных криптоалгоритмов.</p> <p><i>2.4. Хэширование и электронная цифровая подпись.</i> Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП); изучение реализаций хэш-функций и ЭЦП в среде .NET Framework; реализация существующих хэш-функций и алгоритмов ЭЦП.</p> <p><i>2.5. Работа с системными журналами в операционной системе.</i> Изучение методов работы с системными журналами. Отслеживание событий записи в системные журналы. Перехват системных событий. Анализ записей системных журналов.</p> <p><i>2.6. Работа с системными журналами в операционной системе. Файловая система.</i> Отслеживание событий изменения файловой системы (создание, удаление, переименование и изменение выбранных файлов и папок). Отслеживание событий изменения аппаратной конфигурации компьютера.</p> <p><i>2.7. Удаленный доступ и управление операционной системой.</i> Удаленный доступ к ресурсам операционной системы с использованием технологии WMI. Знакомство с утилитой командной строки wmic.</p> <p><i>2.8. Управление политиками безопасности.</i> Исследование методов контроля доступа к ресурсам операционной системы. Обеспечение безопасности доступа кода (утверждение и отклонение полномочий). Управление политиками безопасности.</p>

	<p>2.9. Практическая реализация распределения ключей. Безопасное распределение ключей. Алгоритм Диффи-Хеллмана.</p>
3	Практические занятия не предусмотрены в структуре дисциплины.
4	Курсовая работа не предусмотрена в структуре дисциплины.
5	<p>Расчетно-графическая работа студентов выдается согласно индивидуально выбранной теме и включает следующие этапы: постановка задачи разработки защищенного алгоритма; обзор, сравнительный анализ и подбор подходящих стандартов информационной безопасности; формирование требований к применению алгоритма; формирование и реализация функциональных требований; этапы построения и реализации защищенного алгоритма на практике.</p> <p>Примеры индивидуальных тем на разработку защищенного алгоритма:</p> <ol style="list-style-type: none"> 1) Разработка криптосистемы Ривеста-Шамира-Адлемана.. 2) Криптосистема, основанная на проблеме Диффи-Хеллмана.. 3) Разработка криптосистемы, основанной на эллиптических кривых. 4) Управление ключами, основанное на системах с открытым ключом. 5) Реализация системы потокового шифрования.
6	<p>Самостоятельная работа студентов:</p> <ol style="list-style-type: none"> 6.1. 2 контрольных опроса после 10-й и 17-й лекций; 6.2. Закрепление материала по тематике лекционных занятий: закрепление изучения материалов лекций 1.1-1.17 – основы разработки систем на языках высокого уровня; классификация методов и средств защиты информации; проектирование защищенного программного обеспечения; оценка качества разработанных защищенных программных средств систем; обеспечение уровня безопасности. 6.3. Подготовка к экзамену по дисциплине (оценочные материалы приведены в разделе 6 настоящей РПД).

Год начала подготовки (по учебному плану) _____ 2023
 Образовательный стандарт (ФГОС) _____ утвержденный приказом Минобрнауки России от «26» ноября 2020 г. № 1455