Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

Кафедра прикладной математики и информатики

«Утверждаю»
Проректор по учебно-методической
работе
_____ Ю.А. Устименко
«23» июня 2022 г.

Рабочая программа дисциплины
Б1.В.03 Защита информации

Направление подготовки: **01.03.02 Прикладная математика и информатика**
Направленность (профиль): **Математическое и информационное моделирование**
Форма обучения: очная
Курс – 4
Семестр – 7
Всего зачетных единиц – 2, часов – 72

Форма отчетности: зачет – 7 семестр

Программу разработал
кандидат технических наук, доцент Т.А. Самойлова

Одобрена на заседании кафедры
«16» июня 2022 г., протокол № 10

Заведующий кафедрой _____ С.В. Козлов

Смоленск
2022

1. Место дисциплины в структуре ОП

Дисциплина «Защита информации» относится к дисциплинам части, формируемой участниками образовательных отношений, и является вспомогательной для производственной практики студентов на предприятиях. Она изучается в 7 семестре.

При изучении данной дисциплины необходимы компетенции студентов, сформированные при изучении таких дисциплин, как «Информационные технологии», «Информационные системы», «Базы данных» и др. В курсе рассматриваются вопросы криптографической защиты информационных систем, а также способы аутентификации и авторизации информационных систем. Она знакомит студента с системой основных типов и способов защиты информации, обеспечивает приобретение навыков проектирования систем информационной безопасности. Дисциплина обеспечивает овладение современными программными и аппаратными средствами защиты информации.

Изучение курса основано на традиционных методах высшей школы, тесной взаимосвязи со смежными курсами, а также на использовании современного программного обеспечения.

2. Планируемые результаты обучения по дисциплине

Компетенция	Индикаторы достижения
УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	**Знать:** причины, признаки и последствия опасностей, способы защиты от возникновения чрезвычайных ситуаций; основные понятия дисциплины; основные направления и методы по защите граждан в условиях чрезвычайных ситуаций (от опасностей природного, техногенного и социального характера); способы поддержания безопасных условий жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций, способы использования приемов первой помощи; государственную систему защиты населения от опасных и чрезвычайных ситуаций. **Уметь:** самостоятельно использовать теоретические источники для пополнения знаний о способах поддержания безопасных условий жизнедеятельности; выявлять признаки, причины и условия возникновения опасных и чрезвычайных ситуаций; прогнозировать возникновение опасных и чрезвычайных ситуаций; применять полученные знания и умения в целях обеспечения безопасности жизнедеятельности. **Владеть:** способами создания и приемами для поддерживания безопасных условий жизнедеятельности; аналитическими умениями в области выявления и оценки различных видов опасностей в чрезвычайных ситуациях; методикой и навыками оценки допустимого риска в чрезвычайных ситуациях.
ПК-1. Способен осуществлять поиск, анализ, систематизацию научной информации в области прикладной математики и информатики для реализации научно-исследовательских проектов и решения прикладных задач по проектированию и разработке программного обеспечения.	**Знает**: теоретические основы и технологии организации научно-исследовательской деятельности. **Умеет**: осуществлять поиск, анализ, систематизацию научной информации в области прикладной математики и информатики для реализации научно-исследовательских проектов и решения прикладных задач по проектированию и разработке программного обеспечения. **Владеет**: навыками организации и проведения научно-исследовательской деятельности в ходе выполнения профессиональных функций.

ПК-2.Способен анализировать требования и проектировать программное и информационное обеспечение компьютерных сетей, вычислительные модели и модели данных для реализации элементов новых (или известных) программных продуктов.	**Знает**: возможности существующей программно-технической аппаратуры, современных и перспективных средств разработки программных продуктов, технических средств; методологии разработки программного обеспечения, технологии программирования; методы и средства проектирования программного обеспечения, баз данных, программных интерфейсов; принципы построения архитектуры программного обеспечения и виды архитектуры программного обеспечения, типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения; методики формализации и алгоритмизации поставленных задач. **Умеет**: проводить анализ требований к программному обеспечению, вырабатывать варианты их реализации, проводить оценку и обоснование вырабатываемых решений; использовать существующие типовые решения и шаблоны проектирования программного обеспечения, применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов; использовать методы и приемы формализации и алгоритмизации задач, применять стандартные алгоритмы, использовать программные средства для графического отображения алгоритмов. **Владеет**: методами анализа возможностей реализации требований к программному обеспечению, оценки времени и трудоемкости их реализации, навыками по проектированию программного обеспечения, баз данных, программных интерфейсов, информационных ресурсов сети Интернет.
ПК-3. Способен разрабатывать и отлаживать программный код.	**Знает**: методологию разработки программного обеспечения, информационно-коммуникационных систем, баз данных, информационных ресурсов в сети Интернет; технологии программирования; особенности выбранной среды программирования и системы управления базами данных, синтаксис выбранного языка программирования, особенности программирования на нем, стандартные библиотеки языка программирования; компоненты программно-технических архитектур; методы повышения читаемости кода, системы кодировки символов, форматы хранения исходных текстов программ; методы и приемы отладки кода, типы и форматы сообщений об ошибках и состоянии аппаратных средств, современные компиляторы, отладчики оптимизаторы программного кода. **Умеет**: применять выбранные языки программирования для написания программного кода, использовать выбранную среду программирования и средства системы управления базами данных, использовать возможности имеющейся технической и программной архитектуры; структурировать, комментировать, размечать, форматировать программный код в соответствии с

	требованиями; выявлять ошибки в программном коде, применять методы и приемы его отладки, интерпретировать сообщения об ошибках, предупреждениях, применять современные компиляторы, отладчики, оптимизаторы программного кода. **Владеет**: навыками по созданию программного кода в соответствии с техническим заданием, оптимизации программного кода с использованием специализированных программных средств, форматированию программного кода, анализу, проверке, отладке исходного программного кода.

3. Содержание дисциплины

1. Понятие защиты информации. Средства защиты. Информационные угрозы и атаки. Криптографическая защита информации. Требования к системам защиты. Классификация методов криптографии. Хэш-функции, их роль в криптографии. Алгоритмы SHA-2, SHA-256, SHA-384, SHA-512, SHA-3 (Keccak), ГОСТ 34.11-2018 (российский стандарт вычисления хэш-функции). Библиотеки криптографических алгоритмов.
2. Симметричное шифрование. Подстановочные алгоритмы. Система шифрования Цезаря. Пример шифрования методом "полибианского квадрата". Шифр Атбаш. Шифр Гронсфельда. Шифры перестановки. Блочная перестановка. Шифр перестановки «Скитала».
3. Современные алгоритмы симметричного шифрования. Шифр Файстеля. Алгоритмы DES. ГОСТ Р 34.12–2015 («Магма» и «Кузнечик»). Стандарт ГОСТ 34.12-2018. Табличные замены. Стандарт AES. Шифры MARS • NewDES • RC5 • RC6 • TEA • Triple DES • Twofish. Режимы работы блочных алгоритмов. Достоинства и недостатки симметричных алгоритмов. Библиотеки классов CryptoAPI в .NET и pycryptodome в Python.
4. Симметричные современные поточные шифры. Генератор ключевого потока. Классификация поточных шифров. Алгоритмы A5, RC4, SEAL, Chameleon, SOBER, Leviathan, Phelix, Особенности синхронных и асинхронных поточных шифров. Алгоритмы Salsa20, ChaCha20 и XChaCha20. Криптоанализ. Атаки на поточные шифры.
5. Асимметричное шифрование. Использование однонаправленных функций. Метод Эль-Гамаля. Алгоритм Диффи — Хеллмана. Алгоритм RSA. Генерация открытого и секретного ключей. Криптографические системы на эллиптических кривых. Пакет реализация RSA на Python. Пример шифрования - дешифрования. Недостатки ассиметричного шифрования.
6. Электронно-цифровая подпись. Схема взаимодействия отправителя (передача) и получателя (прием). Принцип работы ЭЦП с хешированием сообщений. Отечественный стандарт. Алгоритмы DSA, ECDSA (Elliptic Curve Digital Signature Algorithm), KCDSA, схема Шнорра.
7. Защита данных методом сжатия. Степень сжатия. Сжатие с потерями и без. Теоремы сжатия. Алгоритмы RLE, Лемпеля-Зива-Велча, Хаффмена. Свойства алгоритмов сжатия.
8. Защита информации в СУБД. Аутентификация и назначение полномочий пользователям. Режимы безопасности SQLServer. Назначение полномочий, ограничение доступа средствами SQL. Использование ролей для защиты данных. Защита в СУБД средствами копирования. Восстановление данных после сбоя. Шифрование протоколов обмена между клиентом и сервером.

4. Тематический план

№ п/п	Разделы и темы	Всего часов	Формы занятий		
			лекции	лабораторные	самостоятельная

				занятия	работа
1	Понятие ЗИ. Хеширование	9	2	2	5
2	Симметричное шифрование	9	2	2	5
3	Современные алгоритмы симметричного шифрования	9	2	2	5
4	Современные поточные шифры	9	2	2	5
5	Асимметричное шифрование	9	2	2	5
6	Электронно-цифровая подпись	9	2	2	5
7	Защита данных методом сжатия	9	2	2	5
8	Защита информации в СУБД	9	2	2	5
ИТОГО		72	16	16	40

5. Виды образовательной деятельности

Занятия лекционного типа

1. Понятие защиты информации. Средства защиты. Информационные угрозы и атаки. Криптографическая защита информации. Требования к системам защиты. Классификация методов криптографии. Хэш-функции, их роль в криптографии. Алгоритмы SHA-2, SHA-256, SHA-384, SHA-512, SHA-3 (Keccak), ГОСТ 34.11-2018 (российский стандарт вычисления хэш-функции). Библиотеки криптографических алгоритмов.
2. Симметричное шифрование. Подстановочные алгоритмы. Система шифрования Цезаря. Пример шифрования методом "полибианского квадрата". Шифр Атбаш. Шифр Гронсфельда. Шифры перестановки. Блочная перестановка. Шифр перестановки «Скитала».
3. Современные алгоритмы симметричного шифрования. Шифр Файстеля. Алгоритмы DES. ГОСТ Р 34.12–2015 («Магма» и «Кузнечик»). Стандарт ГОСТ 34.12-2018. Табличные замены. Стандарт AES. Шифры MARS • NewDES • RC5 • RC6 • TEA • Triple DES • Twofish. Режимы работы блочных алгоритмов. Достоинства и недостатки симметричных алгоритмов. Библиотеки классов CryptoAPI в .NET и pycryptodome в Python.
4. Симметричные современные поточные шифры. Генератор ключевого потока. Классификация поточных шифров. Алгоритмы A5, RC4, SEAL, Chameleon, SOBER, Leviathan, Phelix, Особенности синхронных и асинхронных поточных шифров. Алгоритмы Salsa20, ChaCha20 и XChaCha20. Криптоанализ. Атаки на поточные шифры.
5. Асимметричное шифрование. Использование однонаправленных функций. Метод Эль-Гамаля. Алгоритм Диффи — Хеллмана. Алгоритм RSA. Генерация открытого и секретного ключей. Криптографические системы на эллиптических кривых. Пакет реализация RSA на Python. Пример шифрования - дешифрования. Недостатки ассиметричного шифрования.
6. Электронно-цифровая подпись. Схема взаимодействия отправителя (передача) и получателя (прием). Принцип работы ЭЦП с хешированием сообщений. Отечественный стандарт. Алгоритмы DSA, ECDSA (Elliptic Curve Digital Signature Algorithm), KCDSA, схема Шнорра.
7. Защита данных методом сжатия. Степень сжатия. Сжатие с потерями и без. Теоремы сжатия. Алгоритмы RLE, Лемпеля-Зива-Велча, Хаффмена. Свойства алгоритмов сжатия.
8. Защита информации в СУБД. Аутентификация и назначение полномочий пользователям. Режимы безопасности SQLServer. Назначение полномочий, ограничение доступа средствами SQL. Использование ролей для защиты данных. Защита в СУБД средствами копирования. Восстановление данных после сбоя. Шифрование протоколов обмена между клиентом и сервером.

Занятия семинарского типа – лабораторные занятия

Лабораторная работа 1 "Реализация методов хеширования".

Задание 1. Используя библиотечный пакет **pycryptodome**, вычислите методами SHA3-512 и keccak хеш-функции текстового файла произвольного размера. Сравните длины полученных хешей.

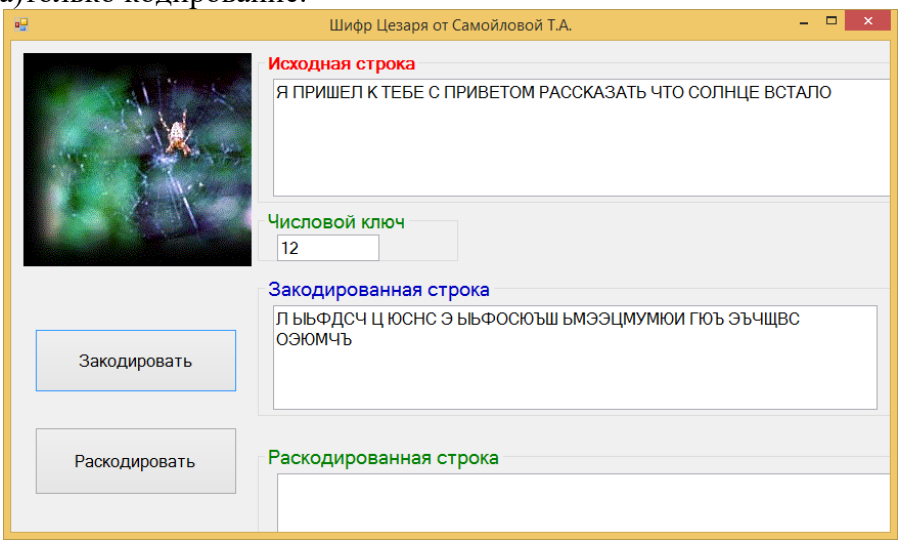
Задание 2. Используя библиотеку hashlib, разработайте модель цепочки блокчейн, содержащей 3-5 элементов с транзакциями в виде списков. Вычислите хеш всей цепочки, а затем измените транзакцию (повредите целостность цепи, представьте, что вы – хакер) и организуйте вывод сообщения о нарушении структуры.

Задание 3. Используя библиотечный пакет **pycryptodome**, вычислите методом HMAC код аутентификации для произвольного сообщения передающей стороны. Задайте ключ аутентификации. **Вычисление MAC** выполните методом хеширования SHA256. Выполните проверку MAC на принимающей стороне, сохранив и нарушив целостность сообщения.

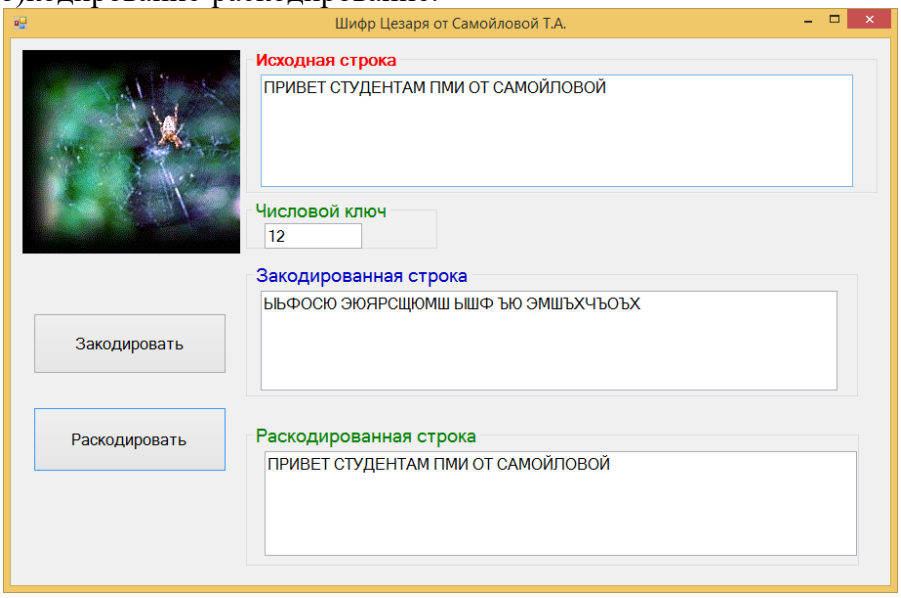
Лабораторная работа 2 "Шифры замены в симметричных криптосистемах ".

Задание 1. Средствами VS C# разработайте форму для кодирования и раскодирования текстовых сообщений шифром Цезаря. В тексте допускаются только большие русские буквы. Далее приведена форма при отладке.

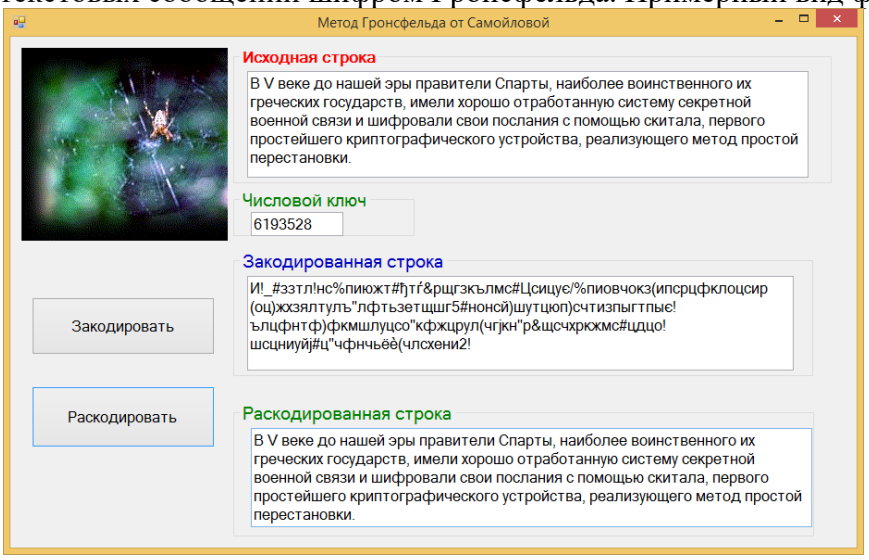
а)только кодирование:



б)кодирование-раскодирование:



Задание 2 Средствами VS C# разработайте форму для кодирования и раскодирования текстовых сообщений шифром Гронсфельда. Примерный вид формы:

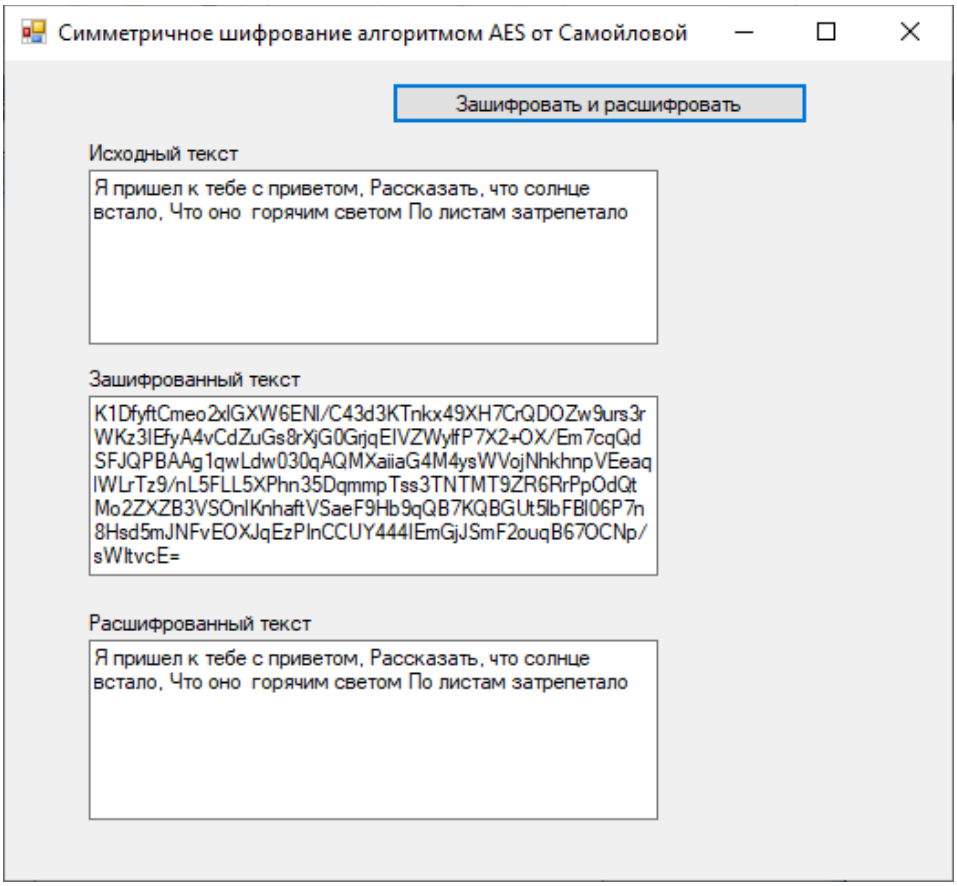


Задание 3. Средствами VS C# разработайте форму для взлома шифра Цезаря методом грубой силы (полный перебор ключей).

Лабораторная работа 3 "Современная симметричная криптография алгоритмом AES".
Задание 1.
Разработайте две Python - программы для шифрования / дешифрования текстового файла с использованием симметричной криптографии алгоритмом AES. Режим шифрования указан в вариантах к заданию. Сохраните исходный текст, шифровку и ключ в отдельных файлах.
Варианты заданий к лабораторной работе

Номер варианта	Режим
1	ECB
2	CFB
3	CBC
4	CCM
5	CTR
6	EAX
7	GCM
8	OCB
9	OFB

Задание 2. Разработайте десктоп – приложение для шифрования / дешифрования текстовых данных с использованием симметричной криптографии алгоритмом AES. Используйте класс создания ключа и соли (IV). Заполнитель указан в вариантах к заданию. Режим шифрования – CBC.
Форма проекта:



Варианты задания к лабораторной работе

Номер варианта	Заполнитель
1	PKCS7
2	ANSIX923
3	PKCS7
4	None
5	ISO10126
6	Zeros
7	PKCS7
8	ANSIX923
9	ISO10126
10	Zeros
11	None
12	ISO10126

Лабораторная работа 4. «Современные поточные шифры»

Задание 1.
Разработайте Python - программу для шифрования / дешифрования текстового сообщения (в сообщении укажите свою фамилию) потоковым алгоритмом RC4.
Задание 2. Разработайте Python - программу для шифрования текстового сообщения (в сообщении укажите свою фамилию) потоковым алгоритмом ChaCha20.
Задание 3. Разработайте Python - программу для шифрования текстового сообщения (в сообщении укажите свою фамилию) потоковым алгоритмом ChaCha20_Poly1305.

Лабораторная работа 5. « Асимметричное шифрование»

Задание 1. Разработайте и протестируйте приложение, выполняющее использование класса ECDiffieHellmanCng для обмена ключами, а также использование ключа для шифрования сообщения, которое можно отправлять по открытому каналу и расшифровывать получателем. В приложении выполняет симметричное шифрование и дешифрование с помощью реализации алгоритма AES. ECDiffieHellman несет ответственность только за предоставление ключа алгоритму AES. Это гибридная криптографическая система (DH + AES), одна для обмена ключами, а другая для шифрования.
Форма программы, шифрующей и дешифрующей текстовое сообщение:
Задание 2. В качестве примера разработайте четыре Python - приложения для реализации ассиметричной криптографии средствами Диффи – Хеллмана (пакет **PyDH**):

- Приложение 1 для создания открытого и закрытого ключей на стороне Алисы и сохранения их в файлах (открытый ключ для передачи Алисе), сохранение параметров Алисы в файле.
- Приложение 2 для создания открытого и закрытого ключей на стороне Боба и сохранения их в файлах (открытый ключ для передачи Бобу), сохранение параметров Боба в файле.
- Приложение 3 (сторона Алисы) загружает открытый ключ Боба, загружает свои параметры, берет свой секретный ключ и формирует секретный ключ для симметричного шифрования.
- Приложение 4 (сторона Боба) загружает открытый ключ Алисы, загружает свои параметры, берет свой секретный ключ и формирует секретный ключ для симметричного шифрования.

Если приложения сделаны правильно, то сформированные секретные ключи для симметричного шифрования в приложениях 3, 4 (стороны Алиса и Боба) должны совпасть.
Задание 3.
Разработайте Python - приложения для реализации асимметричной криптографии средствами RSA:

- Приложение 1 для создания открытого и закрытого ключей и сохранения их в файлах.
- Приложение 2 для шифрования текста с помощью открытого ключа.
- Приложение 3 для дешифрования текста с помощью секретного ключа.

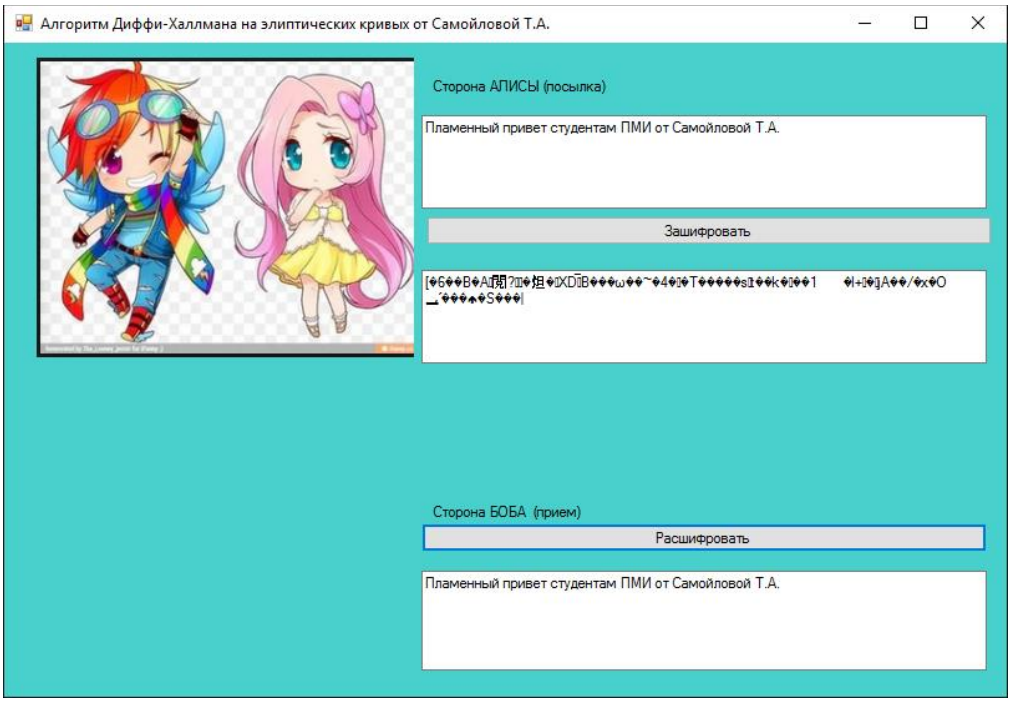
Код приложения 1 – Боб генерирует ключи (файлы public.pem, private.pem), секретный оставляет себе, открытый – отправляет Алисе

Лабораторная работа 6 " Электронная цифровая подпись".

Задание 1. Разработайте консольное приложения для реализации ЭЦП RSA.
ЭЦП создайте и верифицируйте для WORD-документа.
Задание 2 Разработайте десктоп - приложения для реализации ЭЦП:

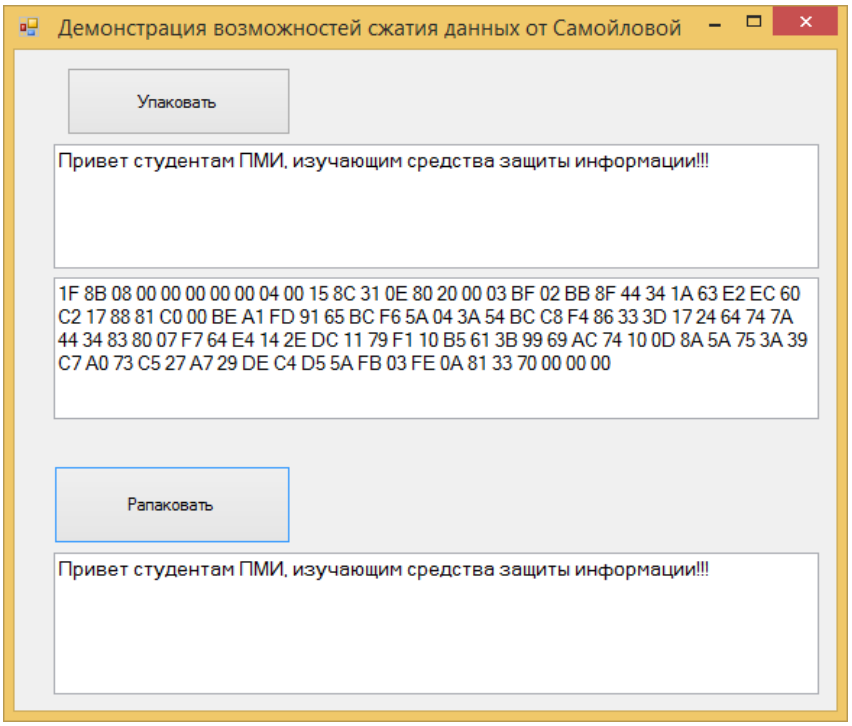
- Приложение 1 для создания открытого и закрытого ключей и сохранения их в XML-файлах.
- Приложение 2 (передающая сторона) для создания дайжеста для Word-документа с помощью секретного ключа.

Приложение 3 (принимающая сторона) для верификации подписи с помощью открытого ключа.
Задание 3. Выполните анализ содержимого сертификата ЭЦП, используя класс Security.Cryptography.**X509Certificates**.

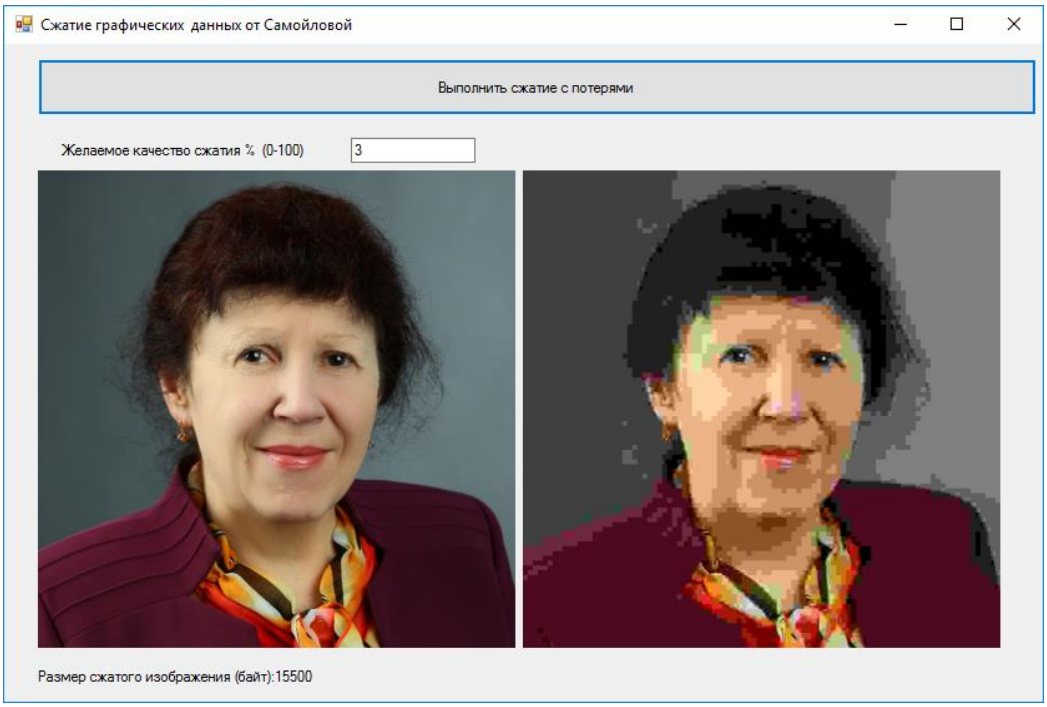


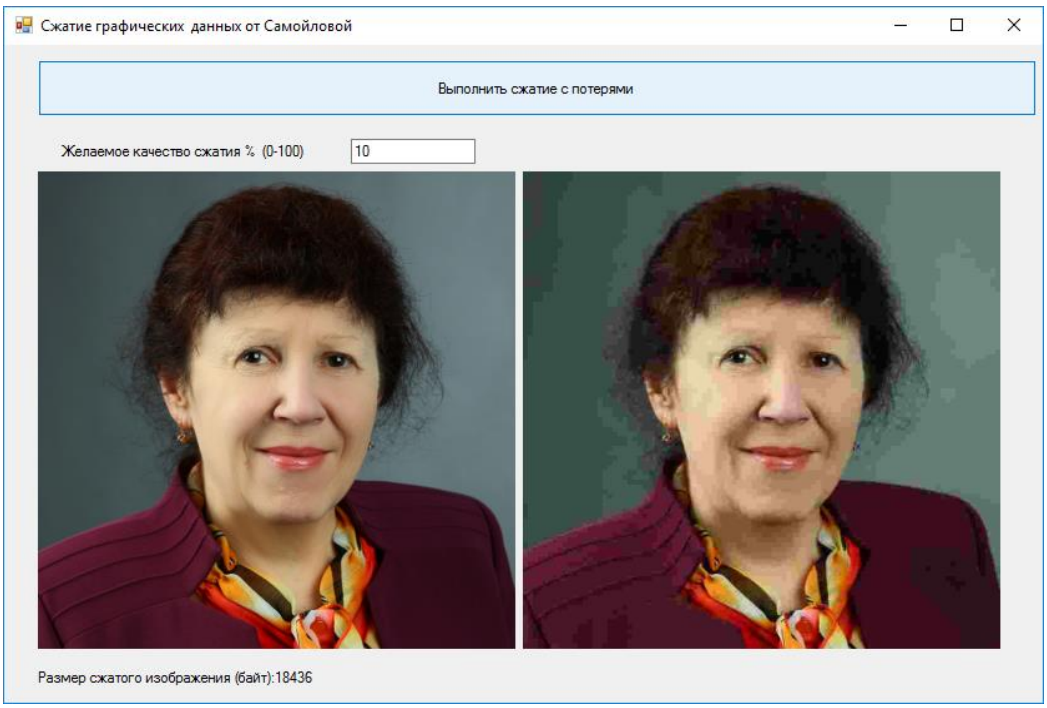
Лабораторная работа 7 " Методы сжатия информации "

Задание 1
Средствами C# , **без использования библиотечных средств System.IO.Compression**, закодируйте и раскодируйте текст, используя алгоритм сжатия RLE.
Задание 2. Используя библиотечные средства System.IO.Compression: MemoryStream и GZipStream, выполните сжатие и распаковку строковых данных. Форма ввода - вывода данных:

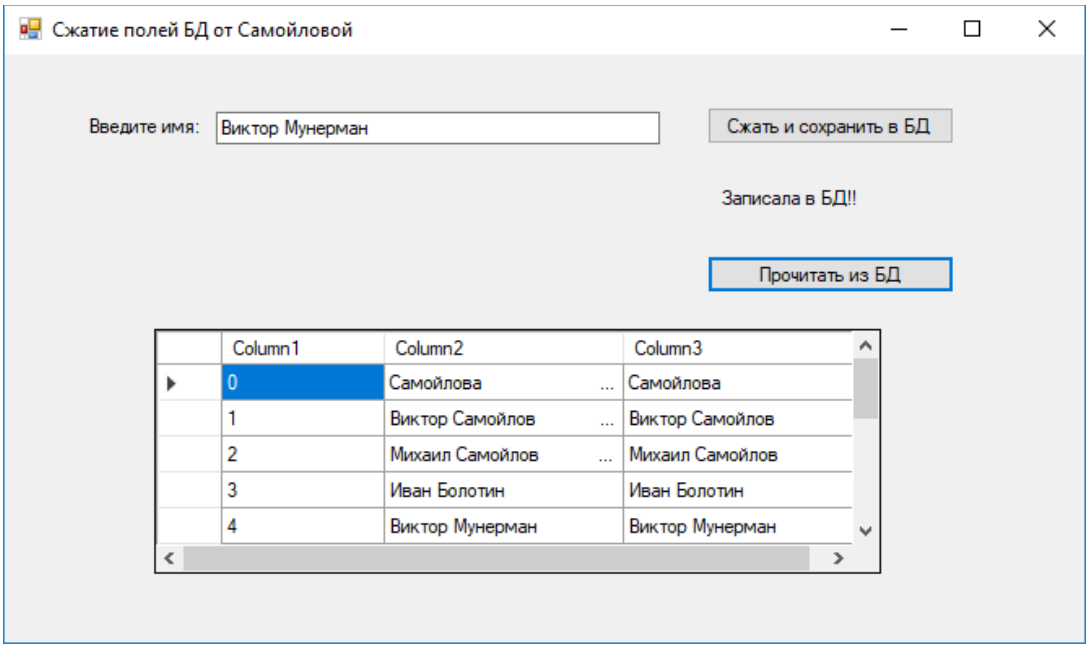


Задание 3
Средствами C# , используя средства System.Drawing. Imaging, сожмите изображение с разными уровнями потерь. Примерный вид окон программы (разные уровни потерь):



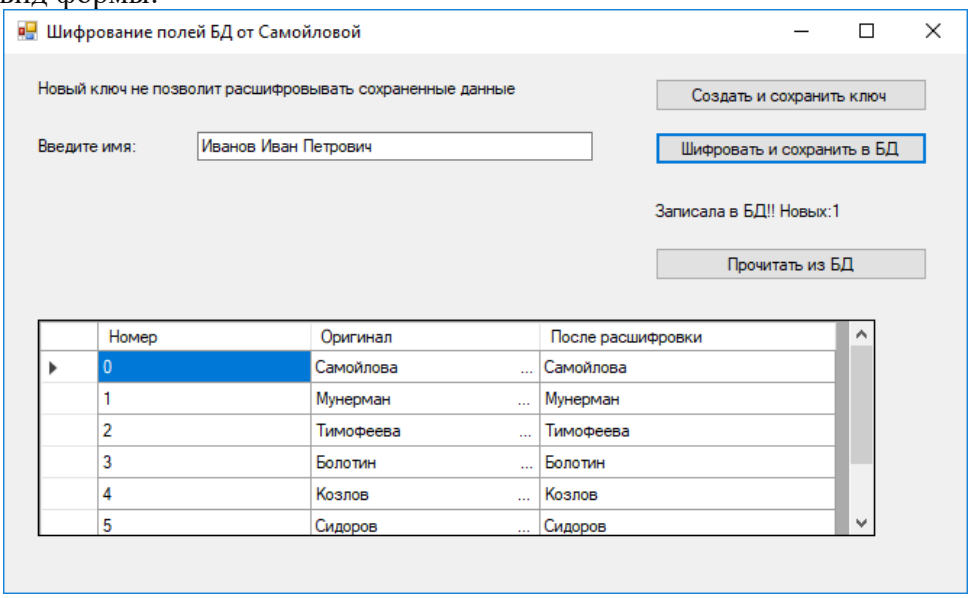


Задание 4. Создать базу данных, содержащую **поле** со сжатыми текстовыми данными типа varbinary(max). Разработать десктоп - приложения ввода данных с последующим сжатием и размещением в БД. Сжатие без потерь выполнить классом **GZipStream (**комбинация алгоритма LZ77 и алгоритма Хаффмана**)** библиотеки **System.IO.Compression.** Желательно использование Entity Framework + LINQ для доступа к полям таблицы. Примерный вид формы:



Лабораторная работа 8 " Защита информации в СУБД "

Задание 1. Создать базу данных, содержащую **поле** с зашифрованными текстовыми данными типа varbinary(max). Разработать десктоп - приложения ввода данных с последующим шифрованием и размещением в базе данных. Шифрование выполнить алгоритмом **AES.** Желательно использование Entity Framework + LINQ для доступа к полям таблицы. Примерный вид формы:



Задание 2. Создайте на SQL Server базу данных DB_Crypt_ваша_фамилия с таблицей Student, содержащей имена и конфиденциальные данные о кредите. Выполните шифрования полей базы данных средствами T-SQL.

Задания для лабораторных работ, размещены в системе дистанционного обучения СмолГУ (www.moodle.smolgu.ru). На занятиях для каждой работы задание предоставляется студентам в электронном виде.

Самостоятельная работа

Текущая самостоятельная работа студента направлена на углубление и закрепление знаний студентов, развитие практических умений. Она заключается в работе с лекционными

материалами, поиске и обзоре литературы и электронных источников, информации по заданным темам курса, опережающей самостоятельной работе, в изучении тем, вынесенных на самостоятельную проработку, подготовке к лабораторным занятиям.

Самостоятельная внеаудиторная работа студентов включает:

- проработку лекционного материала, составление конспекта лекций по темам, вынесенным на самостоятельное изучение;
- выполнение домашних заданий;
- подготовку к защите лабораторных работ.

Темы для самостоятельного изучения

1. История развития методов защиты информации.
2. Организационные методы защиты информации на предприятиях России.
3. Библиотека security cryptography Visual Studio.NET.
4. Библиотека pycryptodome в Python.
5. Защита приложений средствами SQL-Server.

Консультирование студентов осуществляться в индивидуальном порядке на занятиях и во внеурочное время. Выполнение самостоятельной работы оценивается по электронным материалам, подготовленным студентами. Результаты деятельности накапливаются в индивидуальных портфолио студентов.

Учебно-методическое обеспечение для самостоятельной работы

1. Защита информации, учебный курс, Интернет-Университет Информационных Технологий, www.intuit.ru/department/security/bcript/

6. Критерии оценивания результатов освоения дисциплины (модуля)

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Теоретические вопросы

1. Понятие защиты информации. Средства защиты.
2. Информационные угрозы и атаки. Криптографическая защита информации.
3. Требования к системам защиты. Классификация методов криптографии.
4. Хэш-функции, их роль в криптографии. Алгоритмы SHA-2, SHA-256, SHA-384, SHA-512, SHA-3 (Keccak), ГОСТ 34.11-2018 (российский стандарт вычисления хэш-функции). Библиотеки криптографических алгоритмов.
5. Симметричное шифрование. Подстановочные алгоритмы.
6. Система шифрования Цезаря. Пример шифрования методом "полибианского квадрата".
7. Шифр Атбаш. Шифр Гронсфельда.
8. Шифры перестановки. Блочная перестановка. Шифр перестановки «Скитала».
9. Современные алгоритмы симметричного шифрования. Шифр Файстеля.
10. Алгоритмы DES. ГОСТ Р 34.12–2015 («Магма» и «Кузнечик»). Стандарт ГОСТ 34.12-2018. Табличные замены. Стандарт AES. Шифры MARS • NewDES • RC5 • RC6 • TEA • Triple DES • Twofish.
11. Режимы работы блочных алгоритмов. Достоинства и недостатки симметричных алгоритмов.
12. Библиотеки классов CryptoAPI в .NET и pycryptodome в Python.
13. Симметричные современные поточные шифры. Генератор ключевого потока. Классификация поточных шифров.
14. Алгоритмы A5, RC4, SEAL, Chameleon, SOBER, Leviathan, Phelix, Особенности синхронных и асинхронных поточных шифров. Алгоритмы Salsa20, ChaCha20 и XChaCha20. Криптоанализ. Атаки на поточные шифры.

15. Асимметричное шифрование. Использование однонаправленных функций. Метод Эль-Гамаля. Алгоритм Диффи — Хеллмана. Алгоритм RSA.
16. Генерация открытого и секретного ключей. Криптографические системы на эллиптических кривых. Пакет реализация RSA на Python. Пример шифрования - дешифрования. Недостатки ассиметричного шифрования.
17. Электронно-цифровая подпись. Схема взаимодействия отправителя (передача) и получателя (прием).
18. Принцип работы ЭЦП с хешированием сообщений. Отечественный стандарт. Алгоритмы DSA, ECDSA (Elliptic Curve Digital Signature Algorithm), KCDSA, схема Шнорра.
19. Защита данных методом сжатия. Степень сжатия. Сжатие с потерями и без.
20. Теоремы сжатия. Алгоритмы RLE, Лемпеля-Зива-Велча, Хаффмена. Свойства алгоритмов сжатия.
21. Защита информации в СУБД. Аутентификация и назначение полномочий пользователям.
22. Режимы безопасности SQLServer. Назначение полномочий, ограничение доступа средствами SQL.
23. Использование ролей для защиты данных. Защита в СУБД средствами копирования.
24. Восстановление данных после сбоя.
25. Шифрование протоколов обмена между клиентом и сервером.

Критерии оценивания теоретических вопросов

Нормы оценивания ответов на теоретические вопросы

№ п/п	Теоретический вопрос	Количество баллов (*)
1	Дан краткий ответ на поставленный вопрос	1 балл
2	Дан развернутый ответ на вопрос с анализом результатов	2 балла

(*) Возможна градация в 0,25 балла.

Шкала оценивания. Оценка «зачтено» за ответы на теоретические вопросы выставляется, если набрано не менее 3 баллов при ответе на три вопроса, в противном случае выставляется «не зачтено».

Задания для лабораторных занятий

Задачи по темам курса предложены к каждому лабораторному занятию.

Задания для лабораторных и самостоятельной работ, образцы решений основных типовых задач практики также размещены в системе дистанционного обучения СмолГУ (www.moodle.smolgu.ru).

Образец задания

1. Используя библиотеку hashlib, разработайте модель цепочки блокчейн, содержащей 3-5 элементов с транзакциями в виде списков. Вычислите хеш всей цепочки, а затем измените транзакцию (повредите целостность цепи, представьте, что вы – хакер) и организуйте вывод сообщения о нарушении структуры.

2. Разработайте консольное приложения для реализации ЭЦП RSA. ЭЦП создайте и верифицируйте для WORD-документа.

3. Средствами C#, без использования библиотечных средств System.IO.Compression, закодируйте и раскодируйте текст, используя алгоритм сжатия RLE.

Критерии оценивания выполнения лабораторных работ

Нормы оценивания каждой лабораторной работы:

№п/п	Структурная часть работы	Количество баллов (*)
1	Ответ на теоретические вопросы по теме лабораторной работы	1 балл
2	Демонстрация выполнения конкретного	2 балла

	задания, предложенного для самостоятельного решения к лабораторной работе	

(*) с возможностью градации до 0,25 балла.

Шкала оценивания. Оценка «зачтено» за лабораторную работу выставляется, если набрано не менее 2 баллов, в противном случае за работу выставляется «не зачтено».

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Зачетная работа (пример задания)

1. Разработайте Python - программу для шифрования / дешифрования текстового сообщения (в сообщении укажите свою фамилию, дату зачета) потоковым алгоритмом RC4.
2. Используя библиотечные средства System.IO.Compression, выполните сжатие и распаковку строковых данных (в данных укажите свою фамилию, дату зачета).

Критерии оценивания зачетной работы

Нормы оценивания работы

№ п/п	Структурная часть контрольной работы	Количество баллов (*)
1	Правильно реализован каждый метод решения	1 балл
2	Анализ результатов	2 балла

(*) Возможна градация в 0,25 балла.

Шкала оценивания работы:

п/п	Оценка	Количество баллов
1	Отлично	4,75-5
2	Хорошо	3,75-4,5
3	Удовлетворительно	3-3,5
4	Неудовлетворительно	менее 3

Критерий получения зачета

Зачет выставляется по результатам работы студента в течение семестра.

Для получения зачета студент должен:

- уметь отвечать на теоретические вопросы, рассмотренные на лекциях;
- уметь решать задачи, предложенные на лабораторных занятиях;
- уметь решать задачи, предложенные на зачетной контрольной работе.

7. Перечень основной и дополнительной учебной литературы

7.1. Основная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / — Москва : Издательство Юрайт, 2022. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/413854
2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов /— Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477968

7.2. Дополнительная литература

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов /— Москва : Издательство Юрайт, 2020. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/450820
2. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов /— Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6.

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Система дистанционного обучения СмолГУ (moodle.smolgu.ru).
2. Интернет-Университет Информационных Технологий, http://www.intuit.ru
3. Каталог образовательных Internet-ресурсов, http://window.edu.ru.
4. Библиотека разработчика Microsoft, http:// http://msdn.microsoft.com

8. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного типа, оснащенная стандартной учебной мебелью, интерактивной доской, мультимедиапроектором, ноутбуком и колонками.

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации - компьютерная аудитория с выходом в Интернет.

Помещение для самостоятельной работы – компьютерный класс с доступом к сети «Интернет» и ЭИОС СмолГУ.

9. Программное обеспечение

Kaspersky Endpoint Security для бизнеса Стандартный АО «Лаборатория Касперского», лицензия 1FB6-161215-133553-1-6231.

Microsoft Open License, лицензия 49463448 в составе: Microsoft Windows Professional 7 Russian; Microsoft Office 2010 Russian.

Python 3.9; PyCharm Pro; Microsoft Visual Studio