ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В.ЛОМОНОСОВА»

ЭКОНОМИЧЕСКИЙ ФАКУЛЬТЕТ

«УТВЕРЖДАЮ»

Декан экономического факультета МГУ

профессор _____ А.А.Аузан

«___» _____2021 год

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины:

Основы информационной безопасности

Уровень высшего образования:

МАГИСТРАТУРА

Направление подготовки:

38.04.01. ЭКОНОМИКА

Форма обучения:

ОЧНАЯ

Рабочая программа рассмотрена и одобрена
Учебно-методической комиссией экономического факультета
(протокол №_____, дата)

Москва 2021

Рабочая программа дисциплины разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки магистратуры 38.04.01. Экономика

ОС МГУ утвержден решением Ученого совета МГУ имени М.В.Ломоносова от 28 декабря 2020 года, протокол №7

Год (годы) приема на обучение: 2021 и последующие

9. **Место и статус дисциплины в структуре основной профессиональной образовательной программы подготовки магистра**

Статус дисциплины: *вариативная*

Триместр: 4

10. **Входные требования (реквизиты) для освоения дисциплины**

Для успешного освоения данного курса требуются знания и умения, полученные в следующих дисциплинах: теория вероятностей и математическая статистика (в объеме программы вступительных испытаний).

11. **Планируемые результаты обучения по дисциплине, соотнесенные с требуемыми компетенциями выпускников**

Компетенции выпускников (коды)	**Индикаторы (показатели) достижения компетенций**	**Планируемые результаты обучения по дисциплине (модулю), сопряженные с компетенциями**
Готовность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач профессиональной деятельности **(М.ОПК-1)**	Коллоквиум	**УМЕТЬ** принимать участие в устной и письменной дискуссии по построению и анализу математических моделей ЗИ на основе криптографических методов **М.ОПК-1.Ум.1**
Способность применять продвинутые инструментальные криптографические методы в прикладных и/или фундаментальных исследованиях **(М.ОПК-5)**	Коллоквиум, письменная итоговая работа, письменная контрольная работа	**ЗНАТЬ** основные принципы построения криптосистем и криптографических протоколов **М.ОПК-5.Зн.1**
		УМЕТЬ применять на практике криптографические модели и методы к задачам защиты информации **М.ОПК-5.Ум.1**
Способность обобщать и критически оценивать результаты, полученные отечественными и зарубежными исследователями, выявлять перспективные направления, составлять программу исследований **(М.ПК-1)**	Реферат	**УМЕТЬ** применять современные методы и инструменты научно-исследовательской деятельности в области информационной безопасности

Способность представлять результаты проведенного исследования научному сообществу в виде статьи или доклада **(М.ПК-4)**	Реферат, письменная итоговая работа, письменная контрольная работа	**УМЕТЬ** представлять результаты сбора информации об объекте анализа и его результатах в структурированном виде в письменной форме **М.ПК-4.Ум.2**
		УМЕТЬ создавать презентацию по итогам исследований и делать устные научные доклады, в том числе удаленно с использованием дистанционных технологий **М.ПК-4.Ум.2**
Способность готовить материалы по оценке безопасности информационных систем в области практической информационной безопасности **(М.ПК-8)**	Реферат	**ЗНАТЬ** требования к проведению мероприятий и документированию результатов по оценке безопасности компьютерных систем **М.ПК-8.Зн.1**
Способность анализировать и использовать различные источники информации для проведения исследований в области информационной безопасности **(М.ПК-9)**	Реферат	**УМЕТЬ** оценивать качество источников информации в области криптографии и компьютерной безопасности **М.ПК-9.Ум.1**
		УМЕТЬ анализировать стойкость криптографических моделей защиты информации **М.ПК-9.Ум.2**

МПК-3. Способен использовать соответствующий математический аппарат и инструментальные средства для сбора, обработки, анализа и систематизации информации	**МПК-3.И-1.** Использует современные программные и аналитические средства для сбора, первичной обработки и анализа данных	**МПК-3.И-1.У-1.** Умеет применять современные программные и аналитические способы сбора, анализа и систематизации информации

12. **Объем дисциплины по видам занятий**

Объем дисциплины составляет 3 зачетных единицы: 108 академических часов, из которых 52 академических часа составляет контактная работа с преподавателем, из них 28 академических часов — лекции, 24 академических часа — групповая контактная работа, 0 академических часов — индивидуальная контактная работа, 56 академических часов составляет самостоятельная работа магистранта

13. **Формат обучения** преимущественно очный, с использованием обучающей среды On.Econ, частично дистанционный с исользованием обучающей среды On.Econ, а также других технологий видео-конференцсвязи (Discord, Zoom и прочих).

14. **Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий**

Наименование и краткое содержание разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Всего (часы)**	В том числе					
		Контактная работа (работа во взаимодействии с преподавателем) ***Виды контактной работы, часы***				**Самостоятельная работа обучающегося** ***Виды самостоятельной работы, часы***	
		Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	**Всего**	Домашняя работа	**Всего**
Тема 1. История возникновения и развития криптографии как основы для построения систем ЗИ. Основные понятия и задачи криптографии.	8	2	2	—	4	4	4
Тема 2. Математические методы и модели построения криптосистем, криптопротоколов и криптоалгоритмов.	12	4	4	—	8	4	4
Тема 3. Криптопротоколы аутентификации и ЭЦП.	12	4	4	—	8	4	4
Тема 4. Прикладные криптопротоколы.	8	2	2	—	4	4	4
Тема 5. Безопасность компьютерных	8	2	2	—	4	4	4

систем.							
Тема 6. Тестирование на проникновение и анализ защищенности.	12	4	4	—	8	4	4
Тема 7. Основы обеспечения ИБ в современном цифровом пространстве с точки зрения пользователя (сотрудника компании).	8	2	2	—	4	4	4
Тема 8. Цифровая гигиена. Современные угрозы. Управление ключами и парольная политика.	8	2	2	—	4		4
Текущая аттестация: *— написание рефератов*	12	—	—	—	—	12	12
Текущая аттестация: *— сдача коллоквиума*	8	2	2	—	4	4	4
Текущая аттестация: *— письменная контрольная работа*	6	2	—	—	2	4	4
Промежуточная аттестация (контроль): *— письменная итоговая работа*	2					4	
Итого	**108**	**52**				**56**	

Краткое содержание тем дисциплины

Тема 1. История возникновения и развития криптографии как основы для построения систем ЗИ. Основные понятия и задачи криптографии. Простейшие шифры. Шифр замены и шифр перестановки. Формальное определение криптосистемы. Симметрические и асимметрические криптосистемы. Понятие стойкости шифра. Абсолютно стойкие шифры. Стандарты шифрования РФ и США.

Основная литература по теме:

- С.Б. Гашков, Э.А. Применко, М.А. Черепнёв. Криптографические методы защиты информации. Учебное пособие. – М.: Издательский центр «Академия», 2010. – 304 с.
- Э.А. Применко. Алгебраические основы криптографии. – М.: Ленанд, 2015. – 288 с.
- А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. Теоретические основы компьютерной безопасности.

Дополнительная литература:

- А.В. Бабаш, Г.П. Шанкин. Криптография. – М. Солон – Р, 2002. – 152 с.
- А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии. Учебное пособие. – М.: Гелиос. АРВ, 2001. – 480 с.
- Б.В. Столпаков, В.Г. Никонов. Что было в тех землях не знатно. Исторические свидетельства о начале становления российской криптографии (XVI – XVII вв). – М.: Медиа Группа «Авангард», 2016. – 256 с.

Тема 2. Математические методы и модели построения криптосистем, криптопротоколов и криптоалгоритмов. Группа, кольцо, поле. Основные определения и свойства. Теорема Лагранжа. Порядок элемента конечной группы. Циклическая группа. Конечное поле. Характеристика и степень поля. Теоремы о примитивном элементе. Алгоритм вычисления обратного элемента. Кольцо целых чисел. Кольцо вычетов по модулю натурального числа. Теоремы Эйлера и Ферма. Задачи факторизации и дискретного логарифмирования. Китайская теорема об остатках. Криптосистемы Эль-Гамаля и RSA.

Основная литература по теме:

- Э.А. Применко. Алгебраические основы криптографии. – М.: Ленанд, 2015. – 288 с.
- С.Б. Гашков, Э.А. Применко, М.А. Черепнёв. Криптографические методы защиты информации. Учебное пособие. – М.: Издательский центр «Академия», 2010. – 304 с.
- А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. Теоретические основы компьютерной безопасности.
- Применко Э.А., Борисов А.В. Алгебраические основы криптографии в задачах и упражнениях. – М.: КУРС, 2019. – 104 с.

Дополнительная литература:

- М.П. Минеев, В.Н. Чубариков. Лекции по арифметическим вопросам криптографии. – М.: Научно-издательский центр «Луч», 2014. – 224 с.
- И.М. Виноградов. Основы теории чисел. – М.: НИЦ «Регулярная и хаотическая динамика», 2003. – 176 с.

Тема 3. Криптопротоколы аутентификации и ЭЦП. Формальный протокол (схема) аутентификации. Схемы аутентификации Шнора и Шаума. Протокол аутентификации Фейге – Фиата – Шамира. Протокол аутентификации на основе криптосистемы RSA. Общая модель протокола ЭЦП. Хэш-функции. Протокол ЭЦП RSA. Схема протокола Эль-Гамаля. Схемы ЭЦП Шнора и Фиата Шамира. Схема Рабина. Стандарты протоколов ЭЦП РФ и США.

Основная литература по теме:

- С.Б. Гашков, Э.А. Применко, М.А. Черепнёв. Криптографические методы защиты информации. Учебное пособие. – М.: Издательский центр «Академия», 2010. – 304 с.
- А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. Криптографические протоколы. Йошкар Ола: Издательство Московского открытого социального университета, 2001. – 187 с.
- Э.А. Применко, А.В. Борисов. Алгебраические основы криптографии в задачах и упражнениях. – М.: КУРС, 2019. – 104 с.

Дополнительная литература:

- А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии. Учебное пособие. – М.: Гелиос. АРВ, 2001. – 480 с.
- А. Саломаа. Криптография с открытым ключом: Перевод с английского языка. – М.: МИР, 1996. – 318 с.

Тема 4. Прикладные криптопротоколы. Протоколы открытого распределения секретных сеансовых ключей и выработки общего ключа. Протоколы разделения секрета и скрытой передачи информации. Протоколы голосования. Протоколы выработки случайной последовательности и подбрасывания монеты по телефону. Протоколы доказательства с нулевым разглашением.

Основная литература по теме:

- С.Б. Гашков, Э.А. Применко, М.А. Черепнёв. Криптографические методы защиты информации. Учебное пособие. – М.: Издательский центр «Академия», 2010. – 304 с.
- А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. Криптографические протоколы. Йошкар Ола: Издательство Московского открытого социального университета, 2001. – 187 с.

Дополнительная литература:

- С.Б. Гашков, Э.А. Применко, М.А. Черепнёв. Криптографические методы защиты информации. Учебное пособие. – М.: Издательский центр «Академия», 2010. – 304 с.
- А. Саломаа. Криптография с открытым ключом: Перевод с английского языка. – М.: МИР, 1996. – 318 с.

Тема 5. Введение в безопасность компьютерных систем. Основные модели нарушителей. Использование криптографических методов ЗИ на практике. Понятие уязвимости. Уязвимости в сетевых протоколах. Уязвимости в веб-приложениях. Уязвимости в исполняемых файлах. Подходы к оценке уровня критичности уязвимостей.

Основная литература по теме:

- Шон Харрис. CISSP — Руководство для подготовки к экзамену, 5-я редакция.
- Dafydd Studdard and Marcus Pinto. The Web Application Hacker’s Handbook, 2nd edition.
- Michal Zalewski. The Tangled Web.
- Jon Erickson. Hacking – The Art of Exploitation.

Дополнительная литература:

- Open Source Security Testing Methodology Manual.
- Justin Seitz. Black Hat Python.

Тема 6. Тестирование на проникновение и анализ защищенности. Тестирование на проникновение, его типы, длительность и основные этапы. Методология по проведению тестов на проникновение и основные стандарты. Анализ защищенности, его типы, длительность и основные этапы. Методология по проведению мероприятий по анализу защищенности и основные стандарты.

Основная литература по теме:

- Dafydd Studdard and Marcus Pinto. The Web Application Hacker's Handbook, 2nd edition.
- Michal Zalewski. The Tangled Web.
- Jon Erickson. Hacking – The Art of Exploitation.
- Open Source Security Testing Methodology Manual.
- Chris Anley. The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd edition.

Дополнительная литература:

- Gordon Lyon. Nmap Network Scanning.
- Justin Seitz. Black Hat Python.

Тема 7. Основы обеспечения ИБ в современном цифровом пространстве. Распространенные ошибки конфигурации при администрировании операционных систем Linux, Windows. Современные межсетевые экраны, IDS и IPS. SIEM и SOC. Модель красной и синей команд.

Основная литература по теме:

- Open Source Security Testing Methodology Manual.
- Shon Harris, David Miller et al. Security Information and Event Management (SIEM) Implementation.

Дополнительная литература:

- Andrew Baker, Brian Caswell and Jay Beale. Snort Intrusion Detection and Prevention Toolkit.
- Pavel Yosifovich, Mark Russinovich, et al. Windows Internals, Part 1: System architecture, processes, threads, memory management, and more.
- Justin Seitz. Black Hat Python.

Тема 8. Поиск информации и цифровая гигиена. Поиск информации на основе открытых источников. Классификация источников информации. Современные угрозы сети Интернет и понятие цифровой гигиены. Типы вредоносного ПО. Социальная инженерия. Основные методы социальной инженерии. Управление ключами и парольная политика.

Основная литература по теме:

- Шон Харрис. CISSP — Руководство для подготовки к экзамену, 5-я редакция.

Дополнительная литература:

- Michael Bazzell. Open Source Intelligence Techniques – Resources For Searching and Analyzing Online Information.
- Chris Anley. The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd edition.

15. **Фонд оценочных средств для оценивания результатов обучения по дисциплине**

15.1. **Примеры оценочных средств:**

Результаты обучения по дисциплине	Виды оценочных средств
УМЕТЬ принимать участие в устной и письменной дискуссии по построению и анализу математических моделей ЗИ на основе криптографических методов **М.ОПК-1.Ум.1**	Коллоквиум
ЗНАТЬ основные принципы построения криптосистем и криптографических протоколов **М.ОПК-5.Зн.1**	Коллоквиум, письменная итоговая работа, письменная контрольная работа
УМЕТЬ применять на практике криптографические модели и методы к задачам защиты информации **М.ОПК-5.Ум.1**	Реферат
УМЕТЬ применять современные методы и инструменты научно-исследовательской деятельности в области информационной безопасности	Реферат
УМЕТЬ представлять результаты сбора информации об объекте анализа и его результатах в структурированном виде в письменной форме **М.ПК-4.Ум.2**	Реферат, письменная итоговая работа, письменная контрольная работа
УМЕТЬ создавать презентацию по итогам исследований и делать устные научные доклады, в том числе удаленно с использованием дистанционных технологий **М.ПК-4.Ум.2**	Коллоквиум
ЗНАТЬ требования к проведению и документированию результатов мероприятий по оценке безопасности компьютерных систем **М.ПК-8.Зн.1**	Реферат
УМЕТЬ оценивать качество источников информации в области криптографии и компьютерной безопасности **М.ПК-9.Ум.1**	Реферат
УМЕТЬ анализировать стойкость криптографических моделей защиты информации **М.ПК-9.Ум.2**	Реферат, письменная итоговая работа, письменная контрольная работа

15.2. **Критерии оценивания (баллы) по дисциплине:**

Виды оценочных средств	Баллы
Письменная контрольная работа	40
Коллоквиум	40
Реферат	40
Промежуточная аттестация: письменная итоговая работа	30
Итого	**150**

15.3. **Оценка по дисциплине выставляется, исходя из следующих критериев:**

Оценка	Минимальное количество баллов	Максимальное количество баллов
Отлично	127,5	150,0
Хорошо	97,5	127,0
Удовлетворительно	60,0	97,0
Неудовлетворительно	0,0	59,5

Примечание: в случае, если магистрант за триместр набирает менее 20% баллов от максимального количества по дисциплине, то уже на промежуточном контроле (и далее на пересдачах) действует следующее правило сдачи: «магистрант может получить только оценку «Удовлетворительно», и только если получит за промежуточный контроль, включающий весь материал дисциплины, не менее, чем 85% от баллов за промежуточный контроль».

15.4. **Типовые задания и иные материалы, необходимые для оценки результатов обучения:**

Ниже приведены примерные темы рефератов.

1. На этапе активного сбора информации производится перечисление открытых портов на целевом сервере с помощью инструмента Nmap. Перечислить ключевые отличия запуска инструмента с правами суперпользователя и без них. Перечислить также основные преимущества запуска инструмента с правами суперпользователя.

2. Веб-приложение на целевом сервере заведомо содержит публично задокументированную уязвимость, однако разработчиком были удалены все вхождения версий на основных пользовательских страницах (прим. – главная страница). Также известно, что данное веб-приложение является ПО с открытым исходным кодом. Перечислить возможные подходы к идентификации версии веб-приложения. Провести сравнительный анализ выделенных подходов. Высокоуровнево описать процесс эксплуатации после идентификации версии.

3. Описать алгоритм работы Nmap с параметром запуска -sC (остальные параметры запуска выбрать произвольно). Описать категории Nmap Scripting Engine (NSE). Какая категория NSE применяется при запуске Nmap с параметром -sC? Провести сравнительный анализ категорий Nmap Scripting Engine с точки зрения: а) риска нанести ущерб доступности целевой инфраструктуры, б) «бесшумности» проведения работ и противодействия SIEM-системам.

*4. В результате эксплуатации веб-приложения, размещенного на веб-сервере Microsoft IIS вам удалось получить доступ к командной оболочке служебного пользователя на целевом сервере с ОС Windows Server 2012 R2. Исполнив команду «**whoami /priv**» Вы обнаружили, что среди привилегий, доступных имеется привилегия SeImpersonatePrivilege. Исследуйте и опишите уязвимость, позволяющую злоумышленнику повысить привилегии до системного уровня. Также приведите хронологию появления публичных эксплойтов для этой уязвимости с ключевым словом «Potato».*

5. Исследовать и описать как можно больше методов передачи файлов с рабочей станции злоумышленника на целевой сервер. ОС злоумышленника – Kali Linux 2021.1. ОС целевого сервера – Ubuntu 20.04 LTS. Графические оболочки недоступны, имеются только две командные оболочки: одна на стороне злоумышленника, другая – на стороне цели посредством reverse-shell с помощью Netcat.

6. Исследовать и описать как можно больше методов передачи файлов с рабочей станции злоумышленника на целевой сервер. ОС злоумышленника – Kali Linux 2021.1. ОС целевого сервера – Windows Server 2012 R2. Графические оболочки недоступны, имеются только две командные оболочки: одна на стороне злоумышленника, другая – на стороне цели посредством reverse-shell с помощью Netcat.

7. Исследовать исторические материалы для построения общей картины зарождения и применения криптографии в древние времена. Описать использование криптографии от средних веков до нового времени. Ключевые события в мире криптографии в период первой мировой войны. Включить в реферат биографические справки.

8. Исследовать ранние подходы к проверке стойкости криптосистем. Основные понятия криптоанализа.

Ниже приведены примерные вопросы для коллоквиума.

16. *Описать уязвимость переполнения буфера в памяти стека.*
17. *IDS-системы. IPS-системы. NGFW.*
18. *SIEM-системы, SOC-системы.*
19. *Описать модель «красной» и «синей» команд.*
20. *Перечислить и описать уязвимости из набора OWASP Top 10.*

21. *Перечислить типы вредоносного ПО.*
22. *Методология тестирования на проникновение. Этапы, длительность, общие стандарты.*
23. *Описать распространённые атаки на хэши паролей.*
24. *Описать различия SYN-сканирования и TCP-сканирования.*
25. *Простешие шифры. Шифр замены и шифр перестановки. Формальное определение криптосистемы.*
26. *Симметрические и асимметрические криптосистемы. Понятие стойкости шифра. Абсолютно стойкие шифры. Стандарты шифрования РФ и США.*
27. *Группа, кольцо, поле. Основные определения и свойства. Теорема Лагранжа. Порядок элемента конечной группы. Циклическая группа. Конечное поле. Характеристика и степень поля. Теоремы о примитивном элементе. Алгоритм вычисления обратного элемента.*
28. *Кольцо целых чисел. Кольцо вычетов по модулю натурального числа. Теоремы Эйлера и Ферма. Задачи факторизации и дискретного логарифмирования. Китайская теорема об остатках. Криптосистемы Эль-Гамаля и RSA.*
29. *Формальный протокол (схема) аутентификации. Схемы аутентификации Шнора и Шаума. Протокол аутентификации Фейге – Фиата – Шамира. Протокол аутентификации на основе криптосистемы RSA.*
30. *Общая модель протокола ЭЦП. Хэш-функции. Протокол ЭЦП RSA. Схема протокола Эль-Гамаля. Схемы ЭЦП Шнора и Фиата Шамира. Схема Рабина. Стандарты протоколов ЭЦП РФ и США.*
31. *Протоколы открытого распределения секретных сеансовых ключей и выработки общего ключа. Протоколы разделения секрета и скрытой передачи информации.*
32. *Протоколы голосования. Протоколы выработки случайной последовательности и подбрасывания монеты по телефону. Протоколы доказательства с нулевым разглашением.*

Ниже приведены образцы заданий письменной контрольной работы и письменной итоговой работы.

а) *Докажите, что порядок элемента конечной группы есть делитель порядка группы.*
б) *Докажите, что число элементов конечного поля равно некоторой степени простого числа.*
в) *Задача факторизации. Описание и обоснование криптосистемы Ривеста-Шамира-Адельмана. Привести пример.*
г) *Алгоритм построения конечного поля. Построить поле из 27 элементов.*
д) *Протокол ЭЦП. Параметры и алгоритмы протокола. Схема подписи Эль-Гамаля.*
е) *Поточный шифр. Теорема Шеннона. Поточный шифр на основе ЛРП.*
ж) *Протоколы разделения секрета. Групповой и индивидуально-групповой протоколы разделения секрета.*
з) *Перечислите инструменты, подходящие для восстановления паролей на основе хэшей.*
и) *Перечислите инструменты, подходящие для подбора пароля пользователя admin в веб-приложении на языке PHP.*
к) *Перечислить стандартные директории файловой системы ОС UNIX, обладающие набором разрешений «drwxrwxrwt» (или «1777»). О чем говорит указанный набор привилегий?*

л) *Какой параметр запуска утилиты Netcat отвечает за указание файла, который следует исполнить при подключении? Какие версии Netcat поддерживают данный параметр запуска на сегодняшний день?*
м) *Написать произвольный web-shell на языке PHP.*
н) *В чем заключается отличие bind-shell от reverse-shell?*

7.5 Методические рекомендации и требования к выполнению заданий:

— Реферат пишется студентом индивидуально в электронном виде, на его выполнение отводится 1 неделя. Задание сдается в формате .docx или .pdf в виде отчета, раскрывающего заданную тему.

— Участие в дискуссиях

— Письменная контрольная работа проводится в аудитории по индивидуальным вариантам. Продолжительность работы – полтора-два часа. Работа содержит практические задания и теоретические вопросы. Промежуточная аттестация по курсу проводится в аналогичной форме форме. Работа содержит практические задания и теоретические вопросы.

— Коллоквиум проводится в аудитории по следующему алгоритму. Студентам предоставляется индивидуальное задание и дается время на подготовку. После этого происходит устная сдача решения преподавателю и дальнейшая устная беседа по темам, пройденным в рамках курса к этому моменту.

8. Ресурсное обеспечение

8.1. Перечень основной и дополнительной литературы

Основная литература:

- Э.А. Применко. Алгебраические основы криптографии. – М.: Ленанд, 2015. – 288 с.
- С.Б. Гашков, Э.А. Применко, М.А. Черепнёв. Криптографические методы защиты информации. Учебное пособие. – М.: Издательский центр «Академия», 2010. – 304 с.
- А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. Теоретические основы компьютерной безопасности.
- Применко Э.А., Борисов А.В. Алгебраические основы криптографии в задачах и упражнениях. – М.: КУРС, 2019. – 104 с.

- А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. Криптографические протоколы. Йошкар Ола: Издательство Московского открытого социального университета, 2001. – 187 с.
- Шон Харрис. CISSP — Руководство для подготовки к экзамену, 5-я редакция.
- Michael Bazzell. Open Source Intelligence Techniques – Resources For Searching and Analyzing Online Information.
- Dafydd Studdard and Marcus Pinto. The Web Application Hacker's Handbook, 2nd edition.
- Michal Zalewski. The Tangled Web.
- Open Source Security Testing Methodology Manual.
- Jon Erickson. Hacking – The Art of Exploitation.
- Gordon Lyon. Nmap Network Scanning.
- Chris Anley. The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd edition.

Дополнительная литература:

- А.В. Бабаш, Г.П. Шанкин. Криптография. – М. Солон – Р, 2002. – 152 с.
- Б.В. Столпаков, В.Г. Никонов. Что было в тех землях не знатно. Исторические свидетельства о начале становления российской криптографии (XVI – XVII вв). – М.: Медиа Группа «Авангард», 2016. – 256 с.
- С.Б. Гашков, Э.А. Применко, М.А. Черепнёв. Криптографические методы защиты информации. Учебное пособие. – М.: Издательский центр «Академия», 2010. – 304 с.
- А. Саломаа. Криптография с открытым ключом: Перевод с английского языка. – М.: МИР, 1996. – 318 с.
- А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии. Учебное пособие. – М.: Гелиос. АРВ, 2001. – 480 с.
- М.П. Минеев, В.Н. Чубариков. Лекции по арифметическим вопросам криптографии. – М.: Научно-издательский центр «Луч», 2014. – 224 с.
- И.М. Виноградов. Основы теории чисел. – М.: НИЦ «Регулярная и хаотическая динамика», 2003. – 176 с.
- Pavel Yosifovich, Mark Russinovich, et al. Windows Internals, Part 1: System architecture, processes, threads, memory management, and more.
- Bruce Dang. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools and Obfuscation.
- Justin Seitz. Black Hat Python.

8.2. Перечень лицензионного программного обеспечения

—

8.3. Перечень профессиональных баз данных и информационных справочных систем

—

8.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости)

—

9. Язык преподавания:

Русский, но в отдельных случаях допускается предоставление материалов на английском языке. Учебно-вспомогательные материалы, в том числе источники литературы, могут быть на английском языке

10. Преподаватель (преподаватели):

Применко Эдуард Андреевич, к.ф.-м.н., доцент, Москва; Гилязов Руслан Раджабович, м.н.с., Москва.

11. Разработчики программы:

Применко Эдуард Андреевич, к.ф.-м.н., доцент, Москва; Гилязов Руслан Раджабович, м.н.с., Москва.