Институт дистанционного образования

Кафедра кибербезопасности, обработки и хранения информации

УТВЕРЖДАЮ
Директор ИАиИТ Ускенбаева Р.К.
«31» 08 2022 г

СИЛЛАБУС

IDO6592 «Этичный хакинг и противодействие взлому»
(код и наименование дисциплины)

«Информационная безопасность» (дистанционное обучение)
(*шифр, название образовательной программы)*

_ кредита
(количество)

Семестр: зима, 2022-2023 учебный год
(указать номер триместра по курсу)

Алматы 2022

1 Информация о преподавателе

1.1 лектор:

Батыргалиев Асхат Болатканович, ассоциированный профессор

(ФИО преподавателя, должность)

Форма обучения – очное/дистанционное

офис: онлайн Офис-часы: _____

(кабинет, корпус)

Тел., WhatsApp +7(701) - 288-5805 e-mail: askhat.b.b@gmail.com

1.2 преподаватель, ведущий практическую / лабораторную работу

Батыргалиев Асхат Болатканович, ассоциированный профессор

(ФИО преподавателя, должность)

офис: онлайн Офис-часы: _____

(кабинет, корпус)

Тел., WhatsApp +7(701) - 288-5805 e-mail: askhat.b.b@gmail.com

2 Цель и задача курса

Цель:

Получение знаний, навыков и умений для успешного выявления и устранения проблем безопасности в смешанных компьютерных сетях.

Задачи:

– освоение понятийного аппарата;

– изучение основных механизмов проведения атак;

– изучение теоретических основ этичного хакинга;

– приобретение знаний по защите информации в компьютерных системах и сетях;

– развитие потребности к самообразованию и постоянному повышению своего профессионального уровня;

– привитие творческого, научного отношения к процессу этичного хакинга, пентестинга и противодействию компьютернымatакам.

3 Описание курса:

Курс предназначен для обучающихся по образовательной программе «Информационная безопасность»

(шифр, название образовательной программы)

В рамках курса будут рассмотрены материалы по работе компьютерных систем и сетей, типичные уязвимости сетевых протоколов, операционных систем и приложений, последовательности различных видов атак на компьютерные системы и сети, и предложены рекомендации по укреплению защищенности компьютерных систем и сетей.

4. Результаты обучения

После завершения курса обучающийся должен**:**

Уметь:

– использовать основную терминологию в области безопасности;

– разбираться в методах взлома, концепциях хакинга, угрозах информационной безопасности и векторах атак;

– вести сбор информации, владеть техниками сбора и методологией;

– отличать принципы работы троянов, бэкдоров, вирусов, «червей» и другого вредоносного ПО;

– проводить сканирование компьютеров и идентификацию сервисов;

– выполнять резервное копирование и восстановление данных;

– применять набор средств социальной инженерии и других методов противодействия инцидентам;

– предвидеть возможные действия хакера и успешно им противостоять.

Знать:

– основную терминологию в области безопасности;

– понятие несанкционированного доступа;

– угрозы информационной безопасности;

– понятие APT-атаки;

– основы межсетевых экранов;

– назначение систем предотвращения утечки данных (DLP-систем) и принципы их функционирования;

– методы анализа трафика;

– Технология защиты конфиденциальной информации от внутренних угроз (IPC);

– системы обнаружения вторжений (IDS);

– системы управления событиями (SIEM).

5 Календарно-тематический план

Неделя	Тема лекции	Тема лабораторной работы	Ссылка на литературу	Задание
1	Введение в этичный хакинг	Мотивы, цели и задачи хакерских атак. Категории угроз	1-20	
2	Сбор информации	Технологии и методология сбора информации	1-20	
3	Сканирование сети	Обзор техник и инструментов сканирования сетей	1-20	
4	Анализ уязвимостей	Сканеры уязвимостей	1-20	Проведите сканирование сети, определите выявленные уязвимости
5	Анализаторы трафика (снифферы)	Программные и аппаратные анализаторы	1-20	
6	Социальная инженерия	Фазы и типы атак	1-20	
7	Атаки типа отказ в обслуживании (Denial-of-Services)	Средства реализации DOS атак	1-20	Проведите анализ сети. Составьте отчет
	Первая аттестация			
8	SQL инъекции. Атаки на беспроводные сети	Типы SQL инъекций. Wi-Fi технология, беспроводные сети и устройства	1-20	

Неделя	Тема лекции	Тема лабораторной работы	Ссылка на литературу	Задание
9	Межсетевое экранирование	Программные и аппаратные межсетевые экраны	20-22	
10	Безопасность облачных вычислений	Угрозы облачных вычислений		
11	Технология защиты конфиденциальной информации от внутренних угроз (IPC)	Формирование регулярных выражений и настройка системы перехвата передаваемой информации		Осуществите настройку программного межсетевого экрана
12	Системы обнаружения вторжений (IDS)	Интеграция DLP-систем с системами обнаружения и предотвращения вторжений (IDS/IPS)		
13	Системы управления событиями (SIEM)	Интеграция DLP-систем с SIEM-системами		Составить методический документ по комплексной защите объекта информатизации
	Вторая финальная аттестация			
	Экзамен			

6 Литература

Основная литература	Дополнительная литература
[1] Сандерс, Крис. Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях, 3-е изд.: Пер. с англ. - СПб.: ООО "Диалектика", 2019 - 448 с.: ил. - Парал. тит. англ.	[11] Системы мониторинга, управления и обнаружения атак в компьютерных сетях: учебное пособие / Е. А. Гузенкова [и др.]. – Екатеринбург: УрГУПС, 2016. – 290 с.
[2] Парасрам Шива, Замм Алекс, Хериянто Теди, Али Шакил, Буду Дамиан, Йохансен Джерард, Аллен Ли. Kali Linux. Тестирование на проникновение и безопасность. - СПб.: Питер, 2020. - 448 с.: ил. - (Серия «Для профессионалов»).	[12] Лабораторный практикум по информационной безопасности: мониторинг сетевого взаимодействия: учеб.-метод пособие / сост.: А.А. Менщиков, К.А. Сазонов, Ю.А. Шитов. – Электрон. дан. – Красноярск: Сиб. федер. ун-т, 2020.
[3] Милосердов А.В. Тестирование на проникновение с помощью Kali Linux 2.0. По материалам сайта WebWare.biz, 2015. - 348 с.: ил.	[13] Алиев Т.И., Соснин В.В., Шинкарук Д.Н. Компьютерные сети и телекоммуникации: задания и тесты. – СПб: Университет ИТМО, 2018. – 112 с.
[4] Travis Marlette. Splunk Best Practices. Birmingham B3 2PB, UK, 2016. – 238p.	[14] Uenstrom M. Securing networks Cisco. – M.: Williams, 2015. – 698 p.
[5] Миллер Дж. Д. Implementing Splunk 7. 2018, Packt Publishing – 490p.	[24] Анализатор протоколов Wireshark/ П.Н. Толмачев, Н.А. Ермакова, П.В. Подворный, С.А. Сапсай: Учебно-методическое пособие для выполнения лабораторных работ. – М.: РУТ (МИИТ), 2016. – 38 с.
[6] Дэвис Р. Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК Пресс, 2021. – 310 с.: ил	[15] Шаньгин В.Ф. Информационная безопасность компьютерных систем и

	сетей. - М.: Форум-Инфра-М, 2013. – 416 с.
[7] Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. – СПб: Университет ИТМО, 2018. – 45 с.	[16] Justin Hutchens. Kali Linux Network Scanning Cookbook. 2014, Packt Publishing – 452p.
[8] Ric Messier. Изучение Kali Linux. Тестирование безопасности, тестирование на проникновение и Этичный Хакинг. Перевод на русский Condor. - O'Reilly Media, 2018. – 584 с.	[17] Vivek Ramachandran, Cameron Buchanan. Kali Linux Wireless Penetration Testing Beginner's Guide. 2014, Packt Publishing – 214p.
[9] Uldis Dzerkals. EVE-NG Professional Cookbook. Version 1.4. EVE-NG Limited, 204p.	[18] Bragg R. Rhodes Owsley M. Strassberg KE Network Security. Complete Guide – M: Economy, 2016. – 312 p.
[10] Грэм Дэниел Г. Этичный хакинг. Практическое руководство по взлому. - СПб.: Питер, 2022. - 384 с.: ил. - (Серия «Библиотека программиста»).	[19] Charit Mishra. Secure your network through protocol analysis. 2018, Packt Publishing – 155p.
	[20] Методические указания к лабораторным работам. Комплексное обеспечение информационной безопасности автоматизированных систем. – Ставрополь.: 2017. – 274 с.
	[21] Лапонина О.Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны: Учебное пособие / О.Р. Лапонина - М.: Национальный Открытый Университет «ИНТУИТ», 2014. - 378 с., ил., табл. - (Серия «Основы информационных технологий»).
	[22] Технологии межсетевого экранирования и защищенной обработки информации: учеб. пособие / Е.А. Гузенкова [и др.]. – Екатеринбург: УрГУПС, 2016. – 239 с.

7 Рамка компетенций

Дескрипторы обучения	**Компетенции**				
	Естественно-научные и теоретико-мировозренческие	Социально-личностные и гражданские	Общеинженерные профессиональные	Межкультурно-коммуникативные	Специально-профессиональные
Знание и понимание			*		*
Применение знаний и пониманий			*		*
Выражение суждений и анализа действий	*	*			*
Коммуникативные и креативные способности				*	
Самообучаемость и цифровые навыки			*		*

8 График сдачи требуемых работ

№ п/п	Виды контроля	Макс балл недели	Недели										
			1	2	3	4	5	6	7	8	9	10	Итого макс баллов
1	Активность на лекционных обсуждениях												**6**
2	Выполнение заданий (СРСП)												**8**
4	Выполнение практических заданий												**18**
6	1-я промежуточная аттестация (Midterm)												**10**
7	Самостоятельная работа студента (СРС)												**8**
8	2-я финальная аттестация (Endterm)												**10**
9	Итоговый экзамен*												**40**
10	Всего в сумме												**100**

9 Оценочный рейтинг и возможные итоговые варианты оценок по критериям

Буквенная оценка	GPA	баллы	Критерий
A	4	95-100	Показывает самые высокие стандарты знаний, превышающие объем преподаваемого курса
A-	3,67	90-94	Соответствует самым высоким стандартам знаний
B+	3,33	85-89	Очень хорошо и соответствует высоким стандартам знаний
B	3	80-84	Хорошо и соответствует большинству высоких стандартов знаний
B-	2,67	75-79	Более, чем достаточные знания, приближающиеся к высоким стандартам
C+	2,33	70-74	Достаточные знания, соответствующие общим стандартам
C	2	65-69	Удовлетворяет и соответствует большинству общих стандартов знаний
C-	1,67	60-64	Удовлетворяет, но по некоторым знаниям не соответствует стандартам
D+	1,33	55-59	Минимально удовлетворяет, но по большому спектру знаний не соответствует стандартам
D	1	50-54	Минимально удовлетворительный проходной балл с сомнительным соответствием стандартам
FX	0,5	25-49	Временная оценка: Неудовлетворительные низкие показатели, требуется пересдача экзамена
F	0	0-49	Не пытался освоить дисциплину. Выставляется также при попытке студента получить оценку на экзамене обманом
I	0	0	Временная оценка: Студент, завершивший большую часть курса успешно, не завершивший итоговые контрольные мероприятия в силу уважительных обстоятельств
W	0	0	Студент добровольно снялся с дисциплины и ее не освоил до 6-ой учебной недели
AW	0	0	студент снят с дисциплины преподавателем за систематические нарушения академического порядка и правил

10 Критерии оценивания

Каждая работа кроме тестов оценивается по 4 критериям:

– аккуратность и точность (А) – 30% (как точно и аккуратно рассчитана работа);

– творчество и креативность (Т) – 30% (как и каким образом представлена работа);

– полнота и зрелость (З) – 40% (как глубоко, логично и структурно решена работа);

– оригинальность (О) – используется специальный коэффициент 1.0; 0.5 или 0.

Критерии	**Отлично (0.9-1.0)**	**Хорошо (0.7-0.9)**	**Удовлетворительно (0.4-0.7)**	**Неудовлетворительно (0-0.4)**
Аккуратность и точность				
Творчество и креативность				
Полнота и зрелость				
Оригинальность				

Общая оценка будет рассчитана по формуле:
Оценка = (А + Т + З)×О

Максимальная оценка знаний по видам заданий

Тесты и активность	
Самостоятельная работа студента (СРС)	
Практические занятия и бонус	
Лабораторные занятия	
1-я промежуточная аттестация (Midterm)	
Курсовой проект	
2-я финальная аттестация (Endterm)	
Итоговый экзамен	**40**
Итого	**100**

11 Политика поздней сдачи работ

Студент должен прийти подготовленным к лекционным и практическим(лабораторным) занятиям. Требуется своевременная защита и полное выполнение всех видов работ (практических, и самостоятельных). Студент не должен опаздывать и пропускать занятия, быть пунктуальным и обязательным. Предусматривается уменьшение максимального балла на 10% за несвоевременно сданные работы. Если Вы вынуждены пропустить промежуточную аттестацию по уважительным причинам, Вы должны предупредить преподавателя заранее до нее, чтобы была возможность сдать пройти рубежный контроль заранее. Пропуск экзамена по неуважительной причине лишает Вас права на его сдачу. При пропуске экзамена по уважительной причине оформляется специальное разрешение и назначается дата, время и место сдачи экзамена.

12 Политика академического поведения и этики

Будьте толерантны, уважайте чужое мнение. Возражения формулируйте в корректной форме. Плагиат и другие формы нечестной работы недопустимы. Недопустимы подсказывание и списывание во время экзаменов, сдача экзамена за другого студента. Студент, уличенный в фальсификации любой информации курса, получит итоговую оценку «F».

Активность на лекционных и практических занятиях обязательна и является одной из составляющих Вашего итогового балла / оценки. Многие теоретические вопросы, подкрепляющие лекционный материал, будут представлены лишь на лекциях. Следовательно, пропуск занятия может повлиять на Вашу успеваемость и итоговую оценку. Однако посещение занятий само по себе еще не означает увеличение баллов. Необходимо Ваше постоянное активное участие на занятиях. Обязательным требованием курса является подготовка к каждому занятию. Необходимо просматривать

указанные разделы учебника и дополнительный материал не только при подготовке к практическим занятиям, но и перед посещением соответствующей лекции. Такая подготовка облегчит восприятие Вами нового материала и будет содействовать Вашему активному приобретению знаний в стенах университета.

Помощь: За консультациями по выполнению самостоятельных работ, их сдачей и защитой, а также за дополнительной информацией по пройденному материалу и всеми другими возникающими вопросами по читаемому курсу обращайтесь к преподавателю в период его офис часов или через электронные средства связи в рабочее время.

При обучении

Обязательное участие на учебных занятиях согласно расписанию, которая определяет готовность к занятию. В случае отсутствия на занятии студент обязан в течение суток известить преподавателя и объяснить план самостоятельного изучения занятия:

- обязательное прочтение представленных материалов до занятия;
- сдача заданий вовремя;
- 20% неучастия в аудиториях (по уважительной причине с подтверждающими документами) - оценка «F (Fail)»;
- плагиатизм и списывание при выполнении задания не допустимы;
- обязательное использование электронных гаджетов на занятии, что приветствуется, но недопустимо использование на экзамене.

В рамках обучения по дисциплине недопустимы любые коррупционные проявления в любой форме. Организатор таких действий (преподаватель, студенты или третьи лица по их поручению) несут полную ответственность за нарушение законов РК.

Рассмотрено и одобрено на заседании кафедры КИБОиХИ протокол № 1 от «23» августа 2022 г.

Заведующий кафедрой _____ **Сатыбалдиева Р.Ж.**
(*подпись)*

Составитель:

Ассоциированный профессор _____ **Батыргалиев А.Б.**
(подпись)