Қазақстан Республикасының
Білім және ғылым
Министрлігі

Министерство
образования и науки
Республики Казахстан

Д. Серікбаев атындағы
ШҚМТУ

ВКГТУ
им. Д. Серикбаева

УТВЕРЖДАЮ
Декан ШИТиЭ

Денисова Н.Ф.
_____2017 г.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ АҚПАРАТТЫ ҚОРҒАУ
Жұмыс модульдік оқубағдарламасы және силлабус

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ
Рабочая модульная учебная программа и силлабус

Специальность: 5В070400 «Вычислительная техника и программное обеспечение»

Количество кредитов дисциплины: 3

Өскемен
Усть-Каменогорск
2017

Рабочая модульная учебная программа и силлабус разработаны на кафедре «Информационные технологии» на основании Рабочего учебного плана, Каталога элективных дисциплин и Модульной образовательной программы специальности.

Одобрено учебно-методическим советом школы ИТиЭ

Председатель Г.Уазырханова
Протокол №____ от_____г.

Обсуждено на заседании кафедры «ИТ»
Зав. кафедрой С.Кумаргажанова
Протокол №1 от29.08.2017г.

Разработал

Ст.преподаватель И. Котлярова

1 ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ, ЕЕ МЕСТО В УЧЕБНОМ ПРОЦЕССЕ

1.1 Краткое содержание изучаемой дисциплины

Дисциплина «Информационная безопасность и защита информации» относится к модулю «Теория информации, надежность и информационная безопасность», содержащему профильные дисциплины образовательной программы «Вычислительная техника и программное обеспечение». Предметом её изучения являются: основные понятия информационной безопасности, угрозы информационной безопасности, методы и средства безопасности, средства обнаружения и защиты от вирусов, программные средства криптографической защиты информации, технологии обеспечения информационной безопасности.

1.2 Цели и задачи изучения дисциплины

Целью изучения дисциплины «Информационная безопасность и защита информации» является подготовка специалистов, обладающих знаниями в области технологий обеспечения информационной безопасности и способных применять свои знания для обеспечения безопасности информации в системах обработки данных.

Курс должен помочь сформировать у студентов знания по выбору методов и средств защиты информации для обеспечения безопасности современных информационных систем.

Для достижения поставленной цели в рамках изучения дисциплины требуется решить следующие задачи:

- ознакомить с основными понятиями и проблемами информационной безопасности, с основными технологиями обеспечения информационной безопасности;
- сформировать представление о принципах построения систем защиты, о современных методах и средствах защиты информации;
- обеспечить знания и умения, достаточные для обеспечения информационной безопасности в современных операционных и информационных системах.

1.3Результаты изучения дисциплины

Результаты обучения определяются на основе Дублинских дескрипторов соответствующего уровня образования и выражаются через компетенции.

В результате изучения дисциплины обучающийся должен:

знать:

- основные понятия и виды угроз информации в информационных системах;
- современные методы и средства защиты информации;

уметь применять знания и понимания:

- применять на практике различные методы и средства защиты информации, в том числе: средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя; методы криптографической защиты информации; средства обнаружения и защиты от вирусов;
- использовать технологии защиты информации операционных систем;

быть готовым формировать суждения:

- по вопросам применения технологий обеспечения информационной безопасности;
- о практической значимости методов и средств защиты информации; о перспективах развития механизмов информационной безопасности;

развивать коммуникативные способности, в том числе:

- быть способным работать в команде, применять практические навыки работы для защиты информации;
- предлагать новые решения по обеспечению защиты данных в операционных и информационных системах;

развивать навыки обучения, способствующие:

- профессиональному и личностному развитию, повышению квалификации в области защиты информации;
- самостоятельному приобретению и использованию в практической деятельности новых знаний и умений по защите информации.

1.4 Пререквизиты

Для успешного освоения дисциплины «Информационная безопасность и защита информации» необходимы знания по дисциплине «Технология программирования».

1.5 Постреквизиты

Дипломное проектирование.

2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Тематический план

№ модуля, темы	Наименование темы, ее содержание	Ссылка на литературу и другие источники	Трудоемкость в кредитах
1	2	3	4
	Модуль 1 «Методы и средства информационной безопасности»		
	Лекционные занятия		
1	Основные понятия и потенциальные угрозы информационной безопасности.	1, 3, 4, 6	
2	Политика безопасности. Стандарты информационной безопасности.	1, 3, 4	
3	Методы и средства обеспечения информационной безопасности. Модели защиты.	1, 3, 4, 5	
4	Технические средства обеспечения безопасности.	3, 10, 11	
5	Программные средства обеспечения безопасности.	2, 5, 12, 14	
6	Криптографические средства обеспечения безопасности. Основные понятия криптологии. Симметричные криптоалгоритмы.	2, 5, 12, 14	
7	Организационное и правовое обеспечение информационной безопасности. Принципы построения систем защиты.	3, 10, 11	
	Итого		**0,5**

1	2	3	4
	Лабораторные занятия		
1	Шифрование методами перестановки. Подстановка степени n.	2, 12, 14	
2	Шифрование методами перестановки. Маршрутная перестановка.	2, 12, 14	
3	Шифрование методами перестановки. Перестановка тасовкой.	2, 12, 14	
4	Шифрование методами замены. Простая замена	2, 12, 14	
5	Шифрование методами замены. Шифр Цезаря.	2, 12, 14	
	Итого		**1**
	Самостоятельная работа обучающегося под руководством преподавателя (СРОП)		
1	Изучение лекционного материала		
2	Освоение теоретического материала по темам лабораторных работ		
3	Выполнение индивидуальных заданий к лабораторным работам		
4	Защита лабораторных работ		
5	Подготовка к рубежному контролю		
	Самостоятельная работа обучающегося (СРО)		
1	Роль и место системы защиты и безопасности информации в современном информационном процессе.	4, 11, 15, 16, 17	
2	Стандарты информационной безопасности.	4, 11, 15-17, стандарты РК	
3	Симметричные криптоалгоритмы. Шифр Цезаря, шифр Атбаш.	2, 12, 14	
4	Шифрование гаммированием.	2, 12, 14	
5	Моноалфавитные и полиалфавитные шифры. Шифр Плейфейера, Хилла.	2, 12, 14	
	Итого по модулю 1		**1,5**
	Модуль 2 «Технологии обеспечения информационной безопасности и защиты информации»		
	Лекционные занятия		
1	Криптографические средства безопасности. Асимметричные криптоалгоритмы (RSA, Эль-Гамаля).	5, 12, 14	
2	Технология цифровых подписей. Стандарты цифровой подписи DSS и ГОСТ Р34.10-94. Алгоритмы формирования хеш-функций.	5, 12, 14	
3	Механизмы распределения ключей. Прямой обмен ключами. Алгоритм Диффи-Хеллмана.	5, 12, 14	

1	2	3	4
4	Методы идентификации и установления подлинности объекта и субъекта. Парольные системы аутентификации.	1, 6-8	
5	Компьютерные вирусы. Структура и принцип действия компьютерных вирусов.	1, 6-8, 13	
6	Технологии обеспечения информационной безопасности в современных информационных системах и сетях. Технологии защиты информации в Windows.	5, 6, 8, 18,19	
	Итого		**0,5**
	Лабораторные занятия		
1	Шифрование методами замены. Квадрат Вижинера.	2, 12, 14	
2	Шифрование методами замены. Шифрование с использованием алгебры матриц.	2, 12, 14	
3	Алгоритмы шифрования с открытым ключом (RSA, Эль-Гамаля).	5, 12, 14	
4	Изучение персональных средств защиты информации на примере программного средства криптозащиты PGP Desktop Professional 10.2.0.	9	
5	Шифрование дисков при помощи технологии BitLocker	18, 19	
6	Создание и использование правил в брэндмауэре Windows	18, 19	
	Итого		**1**
	Самостоятельная работа обучающегося под руководством преподавателя (СРОП)		
1	Изучение лекционного материала		
2	Освоение теоретического материала по темам лабораторных работ		
3	Выполнение индивидуальных заданий к лабораторным работам		
4	Защита лабораторных работ		
5	Подготовка к рубежному контролю		
	Самостоятельная работа обучающегося (СРО)		
1	Ассиметричный алгоритм RSA.	2, 12, 14	
2	Ассиметричный алгоритм Эль-Гамаля.	2, 12, 14	
3	Стандарты цифровой подписи DSS и ГОСТ Р34.10-94.	2, 12, 14	
4	Механизмы распределения ключей. Алгоритм Диффи-Хеллмана.	2, 12, 14	
5	Шаблоны безопасности.	18, 19	
6	Ограничение использования программного обеспечения с помощью технологии AppLocker	18, 19	

1	2	3	4
	Итого по модулю 2		**1,5**
	Итого по дисциплине, кредит РК		**3**

2.2 Задания для самостоятельной работы (СРОП, СРО)

Тема	Цель и содержание задания	Продолжительность выполнения	Форма контроля	Срок сдачи
1	2	3	4	5
Роль и место системы защиты и безопасности информации в современном информационном процессе.	Ознакомиться и определить роль системы безопасности	4	тест	8
Стандарты информационной безопасности	Ознакомиться со стандартами ИБ, в том числе со стандартами РК	4	тест	8
Симметричные криптоалгоритмы. Шифр Атбаш.	Изучить симметричные криптоалгоритмы	8	Индивидуальное задание	8
Шифрование гаммированием.	Ознакомиться с шифрованием методом гаммирования	4	Индивидуальное задание	8
Моноалфавитные и полиалфавитные шифры. Шифр Плейфейера, Хилла.	Изучить моноалфавитные и полиалфавитные шифры	10	Индивидуальное задание	8
Ассиметричный алгоритм RSA.	Ознакомиться с алгоритмом RSA	5	Индивидуальное задание	12
Ассиметричный алгоритм Эль-Гамаля.	Ознакомиться с алгоритмом Эль-Гамаля	5	Индивидуальное задание	12
Стандарты цифровой подписи DSS и ГОСТ Р34.10-94.	Ознакомиться со стандартами цифровой подписи	5	Индивидуальное задание	12
Механизмы распределения ключей. Алгоритм Диффи-Хеллмана.	Ознакомиться с алгоритмом Диффи-Хеллмана.	5	Индивидуальное задание	12
Компьютерные вирусы. Программные средства защиты от вирусов.	Рассмотреть программные средства защиты от вирусов	5	тест	15

1	2	3	4	5
Технологии обеспечения безопасности операционных систем	Рассмотреть технологии обеспечения безопасности ОС	5	тест	15

2.3 График выполнения и сдачи заданий по дисциплине

Вид контроля	Академический период обучения, неделя														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Защита лабораторных работ	*		*		*	*	*		*	*	*		*	*	*
Инд.задание								*				*			
Рубежный контроль								*							*
Всего	1		1		1	1	1	2	1	1		1	1	1	2

3 СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная литература

1 Зегджа Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия линия-Телеком, 2004. – 452с.

2 Домашев А.В., Попов В.О., Правиков Д.И. и др. Программирование алгоритмов защиты информации. Учебное пособие. М.: «Нолидж», 2004. – 288 с.

3 Хореев А.А. Способы и средства защиты информации. Учебное пособие. – М., 2004. – 316с.

4 Голиков А.М. Основы информационной безопасности: учеб. пособие для практических и семинарских занятий. – Томск : Томск. гос. ун-т систем упр. и радиоэлектроники, 2007. – 214 с.

5 Информационная безопасность и защита информации: учеб. пособие для студ. высш. учеб. заведений / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. – 3-е издание. – М.: Издательский центр «Академия», 2008. – 336 с.

6 Завгородний В.И. Комплексная защита информации в компьютерных системах: учеб. пособие. – М.: ЛОГОС:ПБОЮЛ Н.А. Егоров, 2004.

7 Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.

8 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.

9 PGP Desktop for Windows. User's Guide. (http://www.symantec.com)

Дополнительная литература

10 Галатенко В.А.Основы информационной безопасности: Курс лекций. – М.: ИНТУИТ. РУ, 2006. – 205 с.

11 Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с.

12 Панасенко С.П. Алгоритмы шифрования. Специальный справочник.- СПб.: БХВ-Петербург, 2009.- 576 с.: ил.

13 Глушков С.В., Бабенко М.И., Тесленко Н.С. Секреты хакера: защита и атака. – М.: АСТ: АСТ МОСКВА: ХРАНИТЕЛЬ, 2008. -544 с. (Учебный курс).

14 Бабаш А.В., Шанкин Г.П. Криптография. / под редакцией В.П. Шерстюка, Э.А. Применко/. М.: СОЛОН-ПРЕСС, 2007. – 512 с.

15 Семененко В.А. Информационная безопасность: Учебное пособие. 2-е изд., стереот. - М.: МГИУ, 2005. - 215 с.

16 Корнюшин П.Н., Костерин С.С. Информационная безопасность: Учебное пособие. – Владивосток: ДВГУ, 2003. – 155 с.

17 Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект; Гаудеамус, 2-е изд.- 2004.- 544 с .

18 Пол Мак-Федрис. Windows 7. Полное руководство, Изд. Вильямс, 2011. – 800 с.

19 Карп Д. Хитрости Windows 7. Для профессионалов, Питер, 2011. – 512 с.

12 ОЦЕНКА ЗНАНИЙ

4.1 Требования преподавателя

Требования преподавателя:

- посещение лекционных и практических занятий по расписанию;
- присутствие студентов на занятиях проверяется в начале занятий. В случае опоздания студент должен бесшумно войти в аудиторию и включиться в работу;
- оцениваемые в баллах работы следует сдавать в установленные сроки. За несвоевременную сдачу работ количество баллов снижается;
- повторное прохождение студентом рубежного контроля, в случае получения неудовлетворительной оценки, не допускается;
- студенты, получившие средний рейтинг Рср = (Р 1 + Р2)/2 менее 50%, к сдаче экзамена не допускаются;
- в течение занятий мобильные телефоны должны быть отключены;
- студент обязан приходить на занятия в деловой одежде.

4.2 Критерии оценки

Текущий контроль проводится согласно пункту 2.3.

Рубежный контроль знаний проводится на 7 и 15 неделях семестра в форме тестирования. Рейтинг складывается, исходя из видов контроля, представленных в таблице.

Согласно учебному плану итоговым контролем является сдача экзамена. Экзамен проводится в форме компьютерного тестирования.

Итоговая оценка знаний студента по дисциплине включает:

- 40% результата, полученного на экзамене;
- 60% результатов текущей успеваемости.

Аттестационный период	Вид контроля, удельный вес, %															
	Защита 1 лаб. работы	Защита 2 лаб. работы	Защита 3 лаб. работы	Защита 4 лаб. работы	Защита 5лаб. работы	Индивидуальное задание	**Рубежное тестирование**	Защита 6 лаб. работы	Защита 7 лаб. работы	Защита 8 лаб. работы	Индивидуальное задание	Защита 9 лаб. работы	Защита 10 лаб. работы	Защита 11 лаб. работы	**Рубежное тестирование**	**Всего**
Рейтинг 1	100	100	100	100	100	100	100									100
Рейтинг 2								100	100	100	100	100	100	100	100	100

Формула подсчета итоговой оценки:

$$И = 0{,}6\frac{P_1 + P_2}{2} + 0{,}4Э$$

где Р1, Р2 – цифровые эквиваленты оценок первого, второго рейтингов соответственно;
Э – цифровой эквивалент оценки на экзамене.
Итоговая буквенная оценка и ее цифровой эквивалент в баллах:

Оценка по буквенной системе	Цифровой эквивалент баллов	Процентное содержание	Оценка по традиционной системе
1	2	3	4
A	4,0	95 – 100	Отлично
A-	3,67	90 – 94	
B+	3,33	85 – 89	Хорошо
B	3,0	80 – 84	
B-	2,67	75 – 79	
C+	2,33	70 – 74	Удовлетворительно
C	2,0	65 – 69	
C-	1,67	60 – 64	
D+	1,33	55 – 59	
D	1,0	50 – 54	
F	0	0 – 49	Неудовлетворительно

4.3 Материалы для рубежных и итогового контролей

Под безопасностью информации в системах обработки данных понимается:

А) Регулярное использование средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения требуемого уровня безопасности информации.

В) Способность системы обеспечить в заданный промежуток времени выполнение заданных требований по величине вероятности наступления событий, выражающихся в утечке, модификации или утрате данных.

С) Мера сохранения данных от нежелательных последствий, которые неумышленно или преднамеренно ведут к их модификации, раскрытию или разрушению.

D) Мера возможности возникновения на каком-либо этапе функционирования системы какого-либо явления или события, следствием которого могут быть нежелательные воздействия на защищаемую информацию.

E) Защита данных и программ от несанкционированного доступа.

Конфиденциальность информации – это свойство информации

A) сохранять определенный вид и качество, то есть быть корректной по форме и содержанию

B) быть известной только тем, кому она предназначена

C) находиться в нужном виде и месте для использования санкционированными субъектами в любое время

D) быть неизвестной до определенного момента

E) быть известной только ее владельцу

В каком из следующих шифров символ исходного текста заменяется на ранее определенный символ?

A) Потоковый

B) Полиалфавитный

C) Блочный

D) Моноалфавитный

E) Шифр перестановки

Отказ – это:

A) нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций

B) неправильное выполнение элементом одной или нескольких своих функций, происходящее вследствие специфического его состояния

C) временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции

D) негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде

E) негативное явление, происхождение которого обусловлено спонтанными, не зависящими от намерений людей, обстоятельствами

Модель элементарной защиты предполагает, что

A) защитный контур состоит только из технических средств

B) защитный контур состоит из нескольких преград с одинаковой прочностью

C) предмет защиты помещен в замкнутую и однородную оболочку, называемую преградой

D) защитный контур состоит из нескольких, соединенных между собой преград с различной прочностью

E) преграда может дублироваться еще одной и более преградами

При определении прочности преграды в каком из следующих случаев организация защиты информации вообще теряет свой смысл (если Робх – вероятность обхода преграды нарушителем):

A) Робх = 0

B) Робх = 1

C) Робх> 1
D) Робх< 1
E) Робх> 0

Какой из следующих методов использования паролей заключается в запросе системы определенных символов пароля, выбираемых случайным образом?

A) Метод простого пароля
B) Метод выборки символов
C) Метод паролей однократного использования
D) Метод групп паролей
E) Метод функционального преобразования

Чем характеризуется шифр замены (подстановки)?

A) Отдельные части сообщения (буквы, слова) заменяются на какие-либо другие буквы, числа, символы и т.д.

B) Запись исходного текста сообщения вписывается обычным способом в некоторую матрицу (по строкам слева направо). Выписываются буквы по вертикали, а столбцы при этом берутся в порядке, определяемом ключом

C) для зашифровки и расшифровки сообщения используется один и тот же блок информации - ключ, который должен храниться в тайне и передаваться способом, исключающим его перехват

D) Используются величины, выраженные бесконечным рядом чисел

E) Преобразования информации используют электрические цепи, по которым она передается параллельным способом

Односторонние функции обладают следующим свойством:

A) при заданном значении аргумента x сложно вычислить значение функции f(x), и если известно только значение f(x), то нет простого пути для вычисления аргумента x

B) при заданном значении аргумента x сложно вычислить значение функции f(x)

C) при заданном значении аргумента x относительно просто вычислить значение функции f(x), но если известно только значение f(x), то нет простого пути для вычисления аргумента x

D) при заданном значении аргумента x относительно просто вычислить значение функции f(x), и если известно только значение f(x), то легко вычислить аргумент x

E) при заданном значении аргумента x сложно вычислить значение функции f(x), но если известно только значение f(x), то легко вычислить x

Последовательность электронных цифровых символов, известная владельцу подписи и предназначенная для создания ЭЦП называется:

A) Электронной цифровой подписью
B) Закрытым ключом ЭЦП
C) Открытым ключом ЭЦП
D) Сеансовым ключом ЭЦП
E) Дайджестом сообщения (messagedigest)

Идентификация – это:

A) процедура проверки подлинности заявленного пользователя, процесса или устройства

B) процедура предоставления субъекту определенных полномочий и ресурсов в данной системе

C) регистрация действий пользователя в сети, включая его попытки доступа к ресурсам

D) процедура распознавания пользователя по его идентификатору

E) процедура распознавания субъекта по его биометрическим характеристикам

По особенностям алгоритма вирусы делятся на:

A) файловые, загрузочные, сетевые, макровирусы

B) вирусы-спутники, вирусы-черви, стелс-вирусы, полиморфик-вирусы

C) троянские кони, конструкторы

D) резидентные и нерезидентные

E) сегментированные и несегментированные

Какая часть PGP содержит средства необратимого удаления файлов?

A) PGPZip

B) PGPkeys

C) PGP Shredder и PGP Wipe

D) PGPDisk

E) PGP Net Share

Абоненты некоторой сети применяют цифровую подпись по стандарту ГОСТ Р34.10-94 с общими параметрами p = 17, q = 11, a = 3. Найдите параметры u1 и u2, необходимые для проверки подписи, если известно, что пользователь получил сообщение H(m)=11 вместе с подписью (5,5).

A) u1=10, u2=1

B) u1=8, u2=1

C) u1=6, u2=5

D) u1=5, u2=2

E) u1=6, u2=1

Выберите неверное утверждение:

A) Основные параметры DES: размер блока 64 бита, длина ключа 56 бит, количество раундов – 16

B) DES является классической сетью Фейштеля с двумя ветвями

C) DES является ассиметричным алгоритмом

D) AES (AdvancedEncryptionStandard) – Алгоритм шифрования, действующий в качестве государственного стандарта в области шифрования данных в США с 2001 года

E) Стандарт DES построен на комбинированном использовании перестановки, замены и гаммирования

Какой из алгоритмов не относится к алгоритмам с открытым ключом:

A) Алгоритм RSA

B) Алгоритм Диффи-Хеллмана

C) Алгоритм Эль-Гамаля

D) Алгоритм DES

E) Алгоритм с использованием эллиптических кривых.

4 ОСНОВНЫЕ ФОРМЫ И МЕТОДЫ ОБУЧЕНИЯ

Лекционные занятия проводятся в традиционной форме, с использованием ПК и мультимедийного проектора. На лекциях проводятся экспресс-опросы по пройденному материалу и дискуссии на тему, предложенную для самостоятельного изучения.

Информационно-развивающие: лекция, объяснение, самостоятельная работа с рекомендуемой литературой; проблемно-поисковые и исследовательские – самостоятельная проработка проблемных вопросов по дисциплине, поиск и исследование материала по темам.

Методы (технологии) обучения, используемые в ходе преподавания дисциплины, приведены в таблице:

Методы обучения	Лекции	Лабораторные работы	СРО, СРОП
ИТ-методы	+	+	+
Обучение на основе опыта	+	+	+
Исследовательский метод	+	+	+
Метод активного диалога (дискуссии)	+		+
Поисковый метод			+

6 ВРЕМЯ КОНСУЛЬТАЦИЙ

- по графику работы преподавателя.