1 Цели и задачи изучения дисциплины

1.1 Цель и задачи дисциплины

Учебная дисциплина «Компьютерная безопасность» ставит своей **целью** формирование теоретических представлений о технологиях, обеспечивающих безопасность компьютерных систем, их функционировании с точки зрения информационной безопасности; а также формирование практических навыков по обеспечению их информационной безопасности.

Задачи освоения дисциплины:

- изучить теоретический базис по компьютерной безопасности и криптографии и принципы обеспечения информационной безопасности в сетях и компьютерных системах;
- научиться решать задачи по защите компьютерных систем и применять системный подход в обеспечении информационной безопасности компьютерных систем и сетей.

1.2 Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерная безопасность» относится к вариативной части учебного плана. Дисциплина логически и содержательно-методически связана с дисциплинами «Математика», «Информатика» бакалавриата, а также дисциплиной «Современные методы алгоритмизации и программирования», предшествующей рассматриваемой в рамках учебной программы. Для освоения данной дисциплины необходимо иметь базовые знания в области информатики, в том числе основ компьютерных сетей.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся общекультурных, профессиональных компетенций: ОК-3, ПК-2, ПК-3.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1	ОК-3	готовностью к саморазвитию, самореализации, использованию творческого потенциала	основы кодирования и декодирования информации	определять области поиска информации для решения поставленных задач	навыками самостоятельного поиска информации

2	ПК-2	способностью обосновывать актуальность, теоретическую и практическую значимость избранной темы научного исследования	методы постановки целей и задач в рамках избранной темы научного исследования	осуществлять поиск информации на русском и иностранном языках в сети интернет	навыками самостоятельного анализа различных источников информации
3	ПК-3	способность проводить самостоятельные исследования в соответствии с разработанной программой	способы проведения тестирования информационных систем на наличие уязвимостей	выполнять анализ конфигураций функциональных модулей информационных систем на наличие уязвимостей	навыками постановки задач с учётом целей исследований

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоемкость дисциплины составляет 4 зач. ед. (144 часа), их распределение по видам работ представлено в таблице

Вид учебной работы	Всего часов	Семестры			
		С	___		
Аудиторные занятия (всего)	28	28	-/-		
В том числе:					
Занятия лекционного типа	-	-	-/-		
Занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	28	28	-/-		
Самостоятельная работа (всего)	89	89	-/-		
В том числе:					
самостоятельное изучение разделов	40	40	-/-		
самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.)	59	59			
Вид промежуточной аттестации (зачет, экзамен)	экзамен	экзамен	-/-		
Общая трудоемкость час	144	144	__		
зач. ед.	4	4	__		

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в С семестре

№ раздела	Наименование разделов	Количество часов		
		Всего	Аудиторная работа	Самостоятельная работа

			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1	Введение в компьютерную безопасность	22	0	2	0	20
2	Основные понятия компьютерной безопасности	25	0	2	2	21
3	Безопасность программного обеспечения	17	0	2	2	13
4	Безопасность в компьютерных сетях	17	0	4	2	11
5	Конфиденциальность	17	0	2	4	11
6	Управление компьютерной безопасностью	19	0	2	4	13
	Итого по дисциплине:	117	0	14	14	89

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

Лекционные занятия – не предусмотрены

2.3.2 Занятия практического типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Введение в компьютерную безопасность	Практическое занятие 1. Развитие информационных систем и их уязвимостей в информационной безопасности. Парадигма уязвимость-угроза-контроль. Классификация угроз. Классификация взломщиков компьютерных систем безопасности. Риски информационной безопасности. Методы контроля и противодействия угрозам информационной безопасности.	Коллоквиум 1, Лабораторная работа № 1, Реферат темы 1-2

2	Основные понятия компьютерной безопасности	Практическое занятие 2 Аутентификация и идентификация пользователей. Пароли и способы их взлома. Способы аутентификации и их надёжность. Биометрическая аутентификация, её точность и эффективность. Аутентификация по токену. Политики методы контроля доступа. Криптография как инструмент обеспечения безопасности информации. Виды шифрования. Ключи. Симметричное шифрование. Способы взлома. Асимметричное шифрование. Области применения. Надежность. Криптография с открытым ключом. Применение. Способы взлома.	Кейс 2, Лабораторная работа № 2, Лабораторная работа № 6
3	Безопасность программного обеспечения	Практическое занятие 3 Вредоносные программы. Виды программ, угрозы. Способы противодействия вредоносным программам. Средства и инструментарий по обеспечению контроля доступа.	Коллоквиум 2, Лабораторная работа № 3, Реферат темы 3-6
4	Безопасность в компьютерных сетях	Практическое занятие 4 Локальная и глобальная сеть. Основные понятия и определения. Угрозы безопасности данных в сети. Модификация или подмена данных в сети. Способы вывода из строя сетевых сервисов и сетевых узлов. Беспроводные сети. Протоколы и физические ограничения. Уязвимости в беспроводных сетях. Уязвимости в беспроводных сетях и способы их нейтрализации. DoS-атаки в сети. DDoS-атаки в сети. Использование ботов и бот-сетей для организации DDoS-атак. Использование криптографии для сетевого обмена информацией. Способы шифрования. Фильтрация трафика и Firewall как средство контроля сетевого доступа. IP-сети. Технология NAT и её применение для обеспечения безопасности сетей.	Коллоквиум 2, Лабораторная работа № 4, Реферат темы 7-9
		Практическое занятие 5 Системы обнаружения сетевых вторжений. Классификация. Системы предотвращения сетевых вторжений. Интернет браузер и виды атак на него. Аутентификация интернет браузеров. Способы атак на пользователей всемирной паутины. Вредоносный контент во Всемирной паутине. Методы получения несанкционированного доступа к данным веб-сервиса. Способы атаки на электронную почту.	

5	Конфиденциальность	Практическое занятие 6 Концепция конфиденциальности пользовательской информации. Проблемы обеспечения конфиденциальности в компьютерных системах. Аутентификация пользователей и конфиденциальность. Конфиденциальность во всемирной паутине. Пути утечки конфиденциальной информации при работе во всемирной паутине. Современные технологии и способы раскрытия личных данных. Технология RFIDи проблема конфиденциальности.	Коллоквиум 3, Кейс 3, Лабораторная работа № 5, Реферат темы 12-13
6	Управление компьютерной безопасностью	Практическое занятие 7 Облачные технологии и информационная безопасность. Организация и планирование мер по обеспечению информационной безопасности в компьютерных системах. Виды рисков компьютерной безопасности и их анализ. Риски техногенного характера и противодействие им. Риски не техногенного характера и противодействие им.	Коллоквиум 3, Кейс 1, Кейс 3, Реферат темы 10-11

2.3.3 Лабораторные занятия

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Введение в компьютерную безопасность	Лабораторное занятие 1 Оценка надежности паролей пользователей	Лабораторная работа № 1
2	Основные понятия компьютерной безопасности	Лабораторное занятие 2 Методы шифрования	Лабораторная работа № 2
3	Безопасность программного обеспечения	Лабораторное занятие 3 Оценка влияния рисков, связанных с компьютерной безопасностью, на активы	Лабораторная работа № 3
4	Безопасность в компьютерных сетях	Лабораторное занятие 4 Практическое использование шифрования и цифровых подписей при передаче информации	Лабораторная работа № 4
5	Конфиденциальность	Лабораторное занятие 5 Шифрование на физических носителях информации	Лабораторная работа № 5
6	Управление компьютерной безопасностью	Лабораторное занятие 6 Управление доступом к информации и контроль доступа пользователей к объектам информационных систем	Лабораторная работа № 6

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Наименование раздела	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Введение в компьютерную безопасность	Bishop M. Computer Security: Art and Science / M. Bishop – Addison-Wesley Professional, 2002. – 1136 p. – ISBN: 978-0201440997 Computer Security Handbook, 6 ed. / [edited by] S. Bosworth, M.E. Kabay, E. Whyne – Wiley, 2014. – 2000 p. – ISBN: 978-1-118-12706-3 Gollmann D. Computer Security / D. Gollmann – Wiley, 2012 – 456 p.–ISBN: 978-1-118-51708-6 Security in computing, 5 ed. / C.P. Pfleeger, S.L. Pfleeger, J. Margulies – Prentice Hall, 2015. – 1948 p. – ISBN: 978-0-13-408504-3 Vacca J.R. Computer and Information Security Handbook, 2 ed. / J.R. Vacca– Morgan Kaufmann, 2013. – 1200 p. –ISBN: 978-0123943972
2	Основные понятия компьютерной безопасности	Bishop M. Computer Security: Art and Science / M. Bishop – Addison-Wesley Professional, 2002. – 1136 p. – ISBN: 978-0201440997 Computer Security Handbook, 6 ed. / [edited by] S. Bosworth, M.E. Kabay, E. Whyne – Wiley, 2014. – 2000 p. – ISBN: 978-1-118-12706-3 Gollmann D. Computer Security / D. Gollmann – Wiley, 2012 – 456 p.–ISBN: 978-1-118-51708-6 Security in computing, 5 ed. / C.P. Pfleeger, S.L. Pfleeger, J. Margulies – Prentice Hall, 2015. – 1948 p. – ISBN: 978-0-13-408504-3 Vacca J.R. Computer and Information Security Handbook, 2 ed. / J.R. Vacca– Morgan Kaufmann, 2013. – 1200 p. –ISBN: 978-0123943972
3	Безопасность программного обеспечения	Bishop M. Computer Security: Art and Science / M. Bishop – Addison-Wesley Professional, 2002. – 1136 p. – ISBN: 978-0201440997 Computer Security Handbook, 6 ed. / [edited by] S. Bosworth, M.E. Kabay, E. Whyne – Wiley, 2014. – 2000 p. – ISBN: 978-1-118-12706-3 Gollmann D. Computer Security / D. Gollmann – Wiley, 2012 – 456 p.–ISBN: 978-1-118-51708-6 Security in computing, 5 ed. / C.P. Pfleeger, S.L. Pfleeger, J. Margulies – Prentice Hall, 2015. – 1948 p. – ISBN: 978-0-13-408504-3 Vacca J.R. Computer and Information Security Handbook, 2 ed. / J.R. Vacca– Morgan Kaufmann, 2013. – 1200 p. –ISBN: 978-0123943972

4	Безопасность в компьютерных сетях	Bishop M. Computer Security: Art and Science / M. Bishop – Addison-Wesley Professional, 2002. – 1136 p. – ISBN: 978-0201440997 Computer Security Handbook, 6 ed. / [edited by] S. Bosworth, M.E. Kabay, E. Whyne – Wiley, 2014. – 2000 p. – ISBN: 978-1-118-12706-3 Gollmann D. Computer Security / D. Gollmann – Wiley, 2012 – 456 p.–ISBN: 978-1-118-51708-6 Security in computing, 5 ed. / C.P. Pfleeger, S.L. Pfleeger, J. Margulies – Prentice Hall, 2015. – 1948 p. – ISBN: 978-0-13-408504-3 Vacca J.R. Computer and Information Security Handbook, 2 ed. / J.R. Vacca– Morgan Kaufmann, 2013. – 1200 p. –ISBN: 978-0123943972
5	Конфиденциальность	Bishop M. Computer Security: Art and Science / M. Bishop – Addison-Wesley Professional, 2002. – 1136 p. – ISBN: 978-0201440997 Computer Security Handbook, 6 ed. / [edited by] S. Bosworth, M.E. Kabay, E. Whyne – Wiley, 2014. – 2000 p. – ISBN: 978-1-118-12706-3 Gollmann D. Computer Security / D. Gollmann – Wiley, 2012 – 456 p.–ISBN: 978-1-118-51708-6 Security in computing, 5 ed. / C.P. Pfleeger, S.L. Pfleeger, J. Margulies – Prentice Hall, 2015. – 1948 p. – ISBN: 978-0-13-408504-3 Vacca J.R. Computer and Information Security Handbook, 2 ed. / J.R. Vacca– Morgan Kaufmann, 2013. – 1200 p. –ISBN: 978-0123943972
6	Управление компьютерной безопасностью	Bishop M. Computer Security: Art and Science / M. Bishop – Addison-Wesley Professional, 2002. – 1136 p. – ISBN: 978-0201440997 Computer Security Handbook, 6 ed. / [edited by] S. Bosworth, M.E. Kabay, E. Whyne – Wiley, 2014. – 2000 p. – ISBN: 978-1-118-12706-3 Gollmann D. Computer Security / D. Gollmann – Wiley, 2012 – 456 p.–ISBN: 978-1-118-51708-6 Security in computing, 5 ed. / C.P. Pfleeger, S.L. Pfleeger, J. Margulies – Prentice Hall, 2015. – 1948 p. – ISBN: 978-0-13-408504-3 Vacca J.R. Computer and Information Security Handbook, 2 ed. / J.R. Vacca– Morgan Kaufmann, 2013. – 1200 p. –ISBN: 978-0123943972

3 Образовательные технологии

При реализации учебной работы по освоению дисциплины «Компьютерная безопасность» используются современные образовательные технологии:

- информационно-коммуникационные технологии в процессе самостоятельной работы при поиске информации в Интернете, подготовке к защите лабораторных работ;
- исследовательские методы в обучении в процессе выполнения лабораторных работ;

- проблемное обучение в процессе обсуждения задач обеспечения компьютерной безопасности в различных ситуациях.

Формы контроля знания и работы со студентами, используемые в процессе преподавания дисциплины:

1. Коллоквиум – форма контроля знаний, предполагающая собеседование преподавателя и студента по заранее определенной теме. Целью коллоквиума является формирование у студентов навыка анализа теоретических проблем на основе изучения литературы и первоисточников.

2. Реферат – результат самостоятельной работы студента, включающий анализ и обзор определенной научной, учебной темы с использованием ряда литературных и научных источников. Целью реферата является формирование у студентов навыка самостоятельной работы с информацией, её анализом и поиском.

3. Метод кейсов это неигровой метод обучения, предполагающий использование проблемно-ситуационного похода. Данный метод направлен на имитационное моделирование реальных задач и ситуаций, возникающих в профессиональной сфере, связанной с изучаемой дисциплиной.

4. Лабораторная работа – форма учебного процесса, направленная на освоение практических навыков посредством выполнения последовательности задач для достижения поставленных целей. Лабораторная работа предполагает освоение инструментария и методологии изучаемой дисциплины.

4 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Текущий контроль: выполнение коллоквиумов, рефератов, кейсов, лабораторных работ.

Коллоквиум

Методические указания:

Коллоквиум – форма контроля знаний, предполагающая собеседование преподавателя и студента по заранее определенной теме. Целью коллоквиума является формирование у студентов навыка анализа теоретических проблем на основе изучения литературы и первоисточников. На коллоквиум выносятся темы, связанные с изученным или изучаемым в данный момент материалом. Проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах. В процессе проведения коллоквиума проводится оценка: владения изученным материалом по рассматриваемой проблеме; содержания как проделанной работы студента в целом, так и отдельных её разделов; умения самостоятельного анализа и поиска информации по рассматриваемым проблемам.

Коллоквиум 1

1 Выделите различия и особенности между уязвимостью, угрозой и контрмерами.

2 Кража, как правило, наносит вред. В случае кражи автомобиля это: финансовые потери, неудобство (отсутствие средства передвижения), моральный ущерб. Приведите список из не менее трёх видов вреда, которые может нанести компании кража её компьютерного оборудования.

Критерии оценки:

Оценка "отлично" выставляется студенту, продемонстрировавшему: всестороннее знание материала по рассматриваемой проблеме; полное, последовательное и грамотное изложение ответов; качественную и аргументированную проработку решения поставленной задачи; способность к самостоятельному поиску и работе с информацией по поставленной задаче.

Оценка "хорошо" выставляется студенту, продемонстрировавшему: знание материала в рамках учебной программы; грамотное изложение ответа на вопрос без существенных неточностей; владение навыками, необходимыми для решения поставленных задач.

Оценка "удовлетворительно" выставляется студенту, продемонстрировавшему: знание основного материала в рамках учебной программы; изложение ответа с неточностями и недостаточно верными формулировками; затруднение при решении поставленных задач.

Оценка "неудовлетворительно" выставляется студенту не справившемуся с поставленной задачей, либо продемонстрировавшему отсутствие теоретических представлений и понимания теоретического материала.

Реферат

Методические указания:

Реферат это результат самостоятельной работы студента, включающий анализ и обзор определенной научной, учебной темы с использованием ряда литературных и научных источников. Целью реферата является формирование у студентов навыка самостоятельной работы с информацией, её анализом и поиском. В процессе подготовки текста реферата студент занимается изучением предметной области, связанной с темой реферата, а также формирует практические навыки, связанные с оформлением и подготовкой аналитических документов.

Темы рефератов

1. Компьютерная система как объект защиты информации. Угрозы информационной безопасности в компьютерной системе. Классификация угроз.
2. Базовые принципы, лежащие в основе моделей политики безопасности в компьютерных системах. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам компьютерной системы.
3. Социальная инженерия и её роль в информационной безопасности компьютерных систем.
4. Технология криптовалют и распределенного реестра.
5. Отечественные и зарубежные стандарты шифрования.
6. Общая характеристика и классификация компьютерных вирусов. Средства, используемые для обнаружения компьютерных вирусов.
7. Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.
8. Задачи, решаемые подсистемой аудита в составе защищенных компьютерных систем.
9. Содержательный смысл понятия комплексной системы защиты информации в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению данных систем.
10. Каналы утечки информации в компьютерных системах.
11. Минимизация ущерба, наносимого компьютерным системам авариями и стихийными бедствиями. Дублирование информации. Технология RAID. Резервирование технических средств.
12. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.
13. Общие понятия, история развития и классификация криптографических средств.

Критерии оценки:

Оценка "зачтено" выставляется, если представленный реферат: в полной мере раскрывает заданную тему исследования; содержит актуальные литературные и научные источники и отражает современное состояние рассматриваемой проблемы; отражает владение автором понятийного аппарата и соответствует требованиям по оформлению

Оценка "не зачтено" выставляется, если представленный реферат: не раскрывает заданную тему исследования; не соответствует требованиям к

оформлению; содержит значительные грамматические и понятийные ошибки.

Кейс

Методические указания:

Метод кейсов это неигровой метод обучения, предполагающий использование проблемно-ситуационного похода. Данный метод направлен на имитационное моделирование реальных задач и ситуаций, возникающих в профессиональной сфере, связанной с изучаемой дисциплиной. При этом обучающиеся должны провести исследование проблемы и выработать оптимальное практическое решение. Такой подход в обучении способствует формированию умения применять полученные теоретические знания при решении практических задач, самостоятельного мышления и умения находить оптимальные профессиональные решения в различных ситуациях.

Кейс 1

В обычном офисе биометрическая аутентификация может быть использована для контроля доступа сотрудников и зарегистрированных посетителей. Например, данная система имеет ложные срабатывания, когда сотрудники получают ложный отказ в доступе. В результате требуется человек, который будет пропускать сотрудников в случае ложного срабатывания системы. Таким образом, при использовании биометрической аутентификации для контроля доступа нужен охранник, плюс дополнительные расходы на оборудования для биометрической системы. Приведите причины и выгоду, которые оправдывают дополнительные расходы на биометрическое оборудование.

Критерии оценки:

Оценка "отлично" выставляется студенту, продемонстрировавшему: исчерпывающее аргументированное решение поставленной задачи с опорой на теоретический материал, освоенный в ходе освоения учебного курса; уверенное знание предметной области в рамках поставленной задачи и свободное владение материалом при ответе на дополнительные вопросы.

Оценка "хорошо" выставляется студенту, продемонстрировавшему: аргументированное решение поставленной задачи, допускающее незначительные неточности в терминологии и изложении теоретического материала; знание базовых понятий предметной области в рамках поставленной задачи и владение материалом при ответе на дополнительные вопросы.

Оценка "удовлетворительно" выставляется студенту, продемонстрировавшему: корректное решение поставленной задачи с недостаточной, поверхностной аргументацией выбранного решения при наличии базовых знаний теоретического материала; не систематизированные знания теоретического и практического материала, а также незначительные ошибки при ответе на дополнительные вопросы и обсуждении проблематики поставленной задачи.

Оценка "неудовлетворительно" выставляется студенту не справившемуся с поставленной задачей, либо продемонстрировавшему отсутствие теоретических представлений и понимания теоретического материала.

Лабораторная работа

Методические указания:

Лабораторная работа – форма учебного процесса, направленная на освоение практических навыков посредством выполнения последовательности задач для достижения поставленных целей. Лабораторная работа предполагает освоение инструментария и методологии изучаемой дисциплины. При этом форма организации данных занятий могут включать проведение эксперимента, выполнение расчётов, решение и моделирование различных задач. Данная форма занятий служит дополнением теоретических занятий и направлена на закрепление полученных ранее знаний.

Лабораторная работа № 1

Оценка надежности паролей пользователей

Краткое описание:

Студенты должны провести оценку времени, необходимого для успешной атаки на пароли, сгенерированные по различным правилам (например, содержит только строчные буквы, содержит комбинацию строчных и заглавных букв и т.д.).

Критерии оценки:

Оценка "отлично" выставляется если: работа выполнена в полном объёме без ошибок и замечаний; работа оформлена в соответствии с требованиями к оформлению лабораторных работ; в процессе защиты работы студент продемонстрировал уверенное знание материала, необходимого для выполнения заданий лабораторной работы.

Оценка "хорошо" выставляется если: работа выполнена в полном объёме, однако присутствуют незначительные ошибки либо замечания; работа

оформлена в соответствии с требованиями к оформлению лабораторных работ; в процессе защиты работы студент продемонстрировал наличие базовых теоретических представлений, необходимых для выполнения заданий лабораторной работы.

Оценка "удовлетворительно" выставляется если: основная часть работы выполнена корректно, однако присутствуют ошибки либо замечания; работа не в полной мере оформлена в соответствии с требованиями к оформлению лабораторных работ; в процессе защиты работы студентом допущены ошибки в изложении теоретических представлений, необходимых для выполнения заданий лабораторной работы.

Оценка "неудовлетворительно" ставится если: работа содержит ошибки и не закончена; оформление не соответствует требованиям; в процессе защиты студент не продемонстрировал знание базовых теоретических представлений по предметной области.

Промежуточный контроль: экзамен.

Экзаменационная оценка выставляется по результатам:
- оценки теоретических знаний, полученных в процессе освоения предмета;
- успешной защиты отчетов по лабораторным работам;
- оценки сданных выполненных практических заданий.

Вопросы к экзамену

1. Развитие информационных систем и их уязвимостей в информационной безопасности.
2. Парадигма уязвимость-угроза-контроль.
3. Классификация угроз.
4. Классификация взломщиков компьютерных систем безопасности.
5. Риски информационной безопасности.
6. Методы контроля и противодействия угрозам информационной безопасности.
7. Аутентификация и идентификация пользователей.
8. Пароли и способы их взлома.
9. Способы аутентификации и их надёжность.
10. Биометрическая аутентификация, её точность и эффективность.
11. Аутентификация по токену.
12. Политики методы контроля доступа.
13. Средства и инструментарий по обеспечению контроля доступа.
14. Криптография как инструмент обеспечения безопасности информации. Виды шифрования. Ключи.
15. Симметричное шифрование. Способы взлома.

16. Асимметричное шифрование. Области применения. Надежность.

17. Криптография с открытым ключом. Применение. Способы взлома.

18. Вредоносные программы. Виды программ, угрозы.

19. Способы противодействия вредоносным программам.

20. Локальная и глобальная сеть. Основные понятия и определения.

21. Угрозы безопасности данных в сети.

22. Модификация или подмена данных в сети.

23. Способы вывода из строя сетевых сервисов и сетевых узлов.

24. Беспроводные сети. Протоколы и физические ограничения. Уязвимости в беспроводных сетях.

25. Уязвимости в беспроводных сетях и способы их нейтрализации.

26. DoS-атаки в сети.

27. DDoS-атаки в сети. Использование ботов и бот-сетей для организации DDoS-атак.

28. Использование криптографии для сетевого обмена информацией. Способы шифрования.

29. Фильтрация трафика и Firewall как средство контроля сетевого доступа.

30. IP-сети. Технология NAT и её применение для обеспечения безопасности сетей.

31. Системы обнаружения сетевых вторжений. Классификация.

32. Системы предотвращения сетевых вторжений.

33. Интернет браузер и виды атак на него.

34. Аутентификация интернет браузеров.

35. Способы атак на пользователей всемирной паутины.

36. Вредоносный контент во Всемирной паутине.

37. Методы получения несанкционированного доступа к данным веб-сервиса.

38. Способы атаки на электронную почту.

39. Концепция конфиденциальности пользовательской информации.

40. Проблемы обеспечения конфиденциальности в компьютерных системах.

41. Аутентификация пользователей и конфиденциальность.

42. Конфиденциальность во всемирной паутине.

43. Пути утечки конфиденциальной информации при работе во всемирной паутине.

44. Современные технологии и способы раскрытия личных данных.

45. Технология RFIDи проблема конфиденциальности.

46. Облачные технологии и информационная безопасность.

47. Организация и планирование мер по обеспечению информационной безопасности в компьютерных системах.

48. Виды рисков компьютерной безопасности и их анализ.

49. Риски техногенного характера и противодействие им.

50. Риски не техногенного характера и противодействие им.

Практические задания к экзаменационным билетам

1. Реализуйте алгоритм шифрования "Шифр Цезаря".
2. Реализуйте алгоритм шифрования "Шифр Гронсфельда".
3. Реализуйте алгоритм шифрования "Шифр Плейфейера".
4. Реализуйте алгоритм шифрования "Шифр Хилла".
5. Реализуйте алгоритм шифрования, выполняющий скремблирование.
6. Реализуйте алгоритм шифрования методом простой перестановки.
7. Реализуйте алгоритм шифрования методов одиночной перестановки по ключу.
8. Реализуйте алгоритм шифрования методом двойной перестановки.
9. Реализуйте алгоритм шифрования "Магический квадрат".
10. Реализуйте алгоритм шифрования "Решётка Кардано".
11. Определите время перебора всех паролей, состоящих из 6 цифр.
12. Определите время перебора всех паролей, которые могут содержать цифры 0-9 и буквы латинского алфавита A-Z, как строчные, так и прописные.
13. Определите время перебора всех паролей, которые могут содержать буквы латинского алфавита A-Z, как строчные, так и прописные.
14. Определите время перебора всех паролей, которые могут содержать цифры 0-9, буквы латинского алфавита A-Z, как строчные, так и прописные, а также различные знаки пунктуации.
15. Опишите алгоритм программы, работающей по модели безопасности Белла-Лападулы. Функции программы: регистрация и авторизация пользователей, создание, редактирование и просмотр текстовых заметок.
16. Опишите алгоритм программы, работающей на основе списка контроля доступа. Функции программы: регистрация и авторизация пользователей, создание, редактирование и просмотр текстовых заметок.
17. Создайте почтовое письмо с цифровой подписью.
18. Используя Truecrypt сохраните и зашифруйте текстовую информацию на сменном носителе.

19. Используя Truecrypt сохраните и зашифруйте аудио- или видеофайл на сменном носителе.
20. Составьте политику информационной безопасности предприятия, занимающегося разработкой программного обеспечения. Опишите его особенности и пользовательские роли.
21. Составьте политику информационной безопасности университета. Опишите его особенности и пользовательские роли.
22. Составьте политику информационной безопасности сети магазинов. Опишите его особенности и пользовательские роли.
23. Составьте политику информационной безопасности банка. Опишите его особенности и пользовательские роли.
24. Составьте политику информационной безопасности социальной сети. Опишите его особенности и пользовательские роли.
25. Составьте политику информационной безопасности исследовательского бюро. Опишите его особенности и пользовательские роли.

Образец экзаменационного билета

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кубанский государственный университет»

Направление 38.04.01 «Экономика»
Магистерская программа «Economics and Management»
Кафедра маркетинга и торгового дела
Дисциплина «Компьютерная безопасность»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Развитие информационных систем и их уязвимостей в информационной безопасности.
2. DoS-атаки в сети.
3. Практическое задание.
Реализуйте алгоритм шифрования "Шифр Цезаря".

Заведующий кафедрой, к. э. н., доцент _____А. Н. Костецкий
(подпись)

(подпись)

Критерии оценки теоретических вопросов экзаменационного билета:

Оценка "отлично" выставляется студенту, ответ которого: содержит полные и точные ответы на вопросы экзаменационного билета; демонстрирует свободное знание программного материала, понятийного аппарата учебной дисциплины; отражает связь теоретических знаний и их практического применения.

Оценка "хорошо" выставляется студенту, ответ которого: содержит полные ответы на вопросы экзаменационного билета с незначительными неточностями; демонстрирует хорошее знание программного материала и понятийного аппарата учебной дисциплины; отражает связь теоретических знаний и их практического применения.

Оценка "удовлетворительно" выставляется студенту, ответ которого: содержит полный ответы на один из вопросов экзаменационного билета и частично верный ответ на другой вопрос; демонстрирует удовлетворительное знание программного материала и понятийного аппарата учебной дисциплины

Оценка "неудовлетворительно" выставляется студенты, ответ которого: содержит ответы на один вопрос экзаменационного билета; отсутствует знание программного материала и понятийного аппарата учебной дисциплины.

Критерии оценки задач экзаменационного билета:

Оценка "отлично" ставится, если задача решена верно.

Оценка "хорошо" ставится, если алгоритм решения задачи корректен, однако имеется незначительная ошибка в реализации.

Оценка "удовлетворительно" ставится, если рассуждения в процессе решения корректны, но ответ и решение отсутствует или содержит принципиальные ошибки

Оценка "неудовлетворительно" ставится, если задача не решена.

5 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

5.1 Основная литература

1. Easton C. Computer Security Fundamentals, 3rd edition / C. Easton – Pearson IT Certification, 2016 – 448 p. – ISBN: 978-0789757463
2. Freud J. Measuring and Managing Information Risk: A FAIR Approach / J. Freud, J. Jones. – Butterworth-Heinemann, 2014. – 408 p. – ISBN: 978-0124202313

5.2 Дополнительная литература

1. Applied Information Security / D. Basin, P. Schaller, M. Schläpfer – Springer, 2011. – 202 p. – ISBN: 978-3-642-24474-2.
2. Bishop M. Computer Security: Art and Science / M. Bishop – Addison-Wesley Professional, 2002. – 1136 p. – ISBN: 978-0201440997
3. Computer Security Handbook, 6 ed. / [edited by] S. Bosworth, M.E. Kabay, E. Whyne – Wiley, 2014. – 2000 p. – ISBN: 978-1-118-12706-3
4. Gollmann D. Computer Security / D. Gollmann – Wiley, 2012 – 456 p.– ISBN: 978-1-118-51708-6
5. Privacy in a Digital, Networked World / [edited by] S. Zeadally, M. Badra – Springer, 2015. – 418p. – ISBN: 978-3319084695
6. Security in computing, 5 ed. / C.P. Pfleeger, S.L. Pfleeger, J. Margulies – Prentice Hall, 2015. – 1948 p. – ISBN: 978-0-13-408504-3
7. Vacca J.R. Computer and Information Security Handbook, 2 ed. / J.R. Vacca– Morgan Kaufmann, 2013. – 1200 p. –ISBN: 978-0123943972

5.3 Периодические издания

1. Computers & Security / ISSN: 0167-4048
2. Journal of Computer Security / ISSN 0926-227X

6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Computer Security https://www.coursera.org/course/security
2. Introduction to Network Security http://learnthat.com/introduction-to-network-security/
3. Network Security tutorial https://training.apnic.net/docs/TSEC01.pdf
4. Software Security https://www.coursera.org/course/softwaresec

7 Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов является неотъемлемой частью процесса подготовки. Под самостоятельной работой понимается часть учебной планируемой работы, которая выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа направлена на усвоение системы научных и профессиональных знаний, формирования умений и навыков, приобретение опыта самостоятельной творческой деятельности. СРС помогает формировать культуру мышления студентов, расширять познавательную деятельность.

8 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1 Перечень необходимого программного обеспечения

1. Microsoft Visual Studio

2. Microsoft Windows Server 2012
3. Ubuntu Linux
4. Oracle Virtualbox

9 Материально-техническое обеспечение дисциплины

Учебно-научные помещения и лаборатории экономического факультета ФБГОУ ВО КубГУ в полной мере обеспечены приборами и оборудованием специального назначения, необходимыми для проведения курса. Обеспеченность учебно-лабораторным оборудованием отвечает требованиям государственного образовательного стандарта и рабочей программе предлагаемого курса.