МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г. ШУХОВА»

(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института
экономики и менеджмента
Дорошенко Ю.А.
«16» ноября 2016 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

Информационная безопасность

направление подготовки

38.03.05 «Бизнес-информатика»

Профиль подготовки

Технологическое предпринимательство

Степень

Бакалавр

Форма обучения

Очная

Институт: экономики и менеджмента

Кафедра: экономики и организации производства

Белгород – 2016

Рабочая программа составлена на основании требований:

Федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.05 Бизнес-информатика (уровень бакалавриата), утвержден приказом Министерства образования и науки российской Федерации от 11 августа 2016 г. № 1002

Плана учебного процесса БГТУ им. В.Г. Шухова, введенного в действие в 2016 году.

Составитель: к.э.н., доц. (Л.А. Рябова)

Рабочая программа согласована с выпускающей кафедрой
экономика и организация производства
(название кафедры)

Заведующий кафедрой (Селиверстов Ю.И.)
(подпись) (ФИО)

«31» августа 2016 г.

Рабочая программа обсуждена на заседании кафедры
экономики и организации производства
(наименование кафедры)

«31» августа 2016 г., протокол № 1

Заведующий кафедрой д.э.н., профессор (Ю.И. Селиверстов)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа одобрена методической комиссией института
института экономики и менеджмента
(наименование института)

«13» 09 2016 г., протокол № 1

Председатель к.э.н., профессор (В.Э. Выборнова)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции			Требования к результатам обучения
№	Код компетенции	Компетенция	
Профессиональные			
1	ПК-9	Организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия	В результате освоения дисциплины обучающийся должен **Знать:** - основные понятия и направления в защите компьютерной информации, принципы защиты информации; - принципы классификации и примеры угроз безопасности компьютерным системам, современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности; - состояние и правовые основы информационной безопасности РФ, правовые гарантии информационной безопасности личности; - основные инструменты обеспечения многоуровневой безопасности в информационных системах. **Уметь:** - конфигурировать встроенные средства безопасности в операционной системе, проводить анализ защищенности компьютера и сетевой среды с использованием сканера безопасности; - устанавливать и использовать одно из средств для шифрования информации и организации обмена данными с использованием электронной цифровой подписи; устанавливать и использовать один из межсетевых экранов; - устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; - настроить инструменты резервного копирования и восстановления информации. **Владеть:** - методами аудита безопасности информационных систем, методами системного анализа информационных систем; - методами защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

Наименование дисциплины (модуля)
1. Электронный бизнес

Содержание дисциплины служит основой для изучения следующих дисциплин:

Наименование дисциплины (модуля)
1.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единиц, 144 часов.

Вид учебной работы	Всего часов	Семестр № 8
Общая трудоемкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т.ч.:	54	54
лекции	18	18
лабораторные	36	36
практические		
Самостоятельная работа студентов, в том числе:	90	90
Курсовой проект		
Курсовая работа		
Расчетно-графическое задание		
Индивидуальное домашнее задание	9	9
Другие виды самостоятельной работы	45	45
Промежуточная аттестация (экзамен)	36	36

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Наименование тем, их содержание и объем

Курс 4 Семестр 8

№ п/п	Наименование раздела (модуля)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практич. ческие занятия	Лаборат орные занятия	Самостоя-тельная работа
1	2	3	4	5	6
1	**Предмет, методология и понятийный аппарат курса.** Предмет информационной безопасности. Концепция информационной безопасности, важность и ценность информации, модели информационной безопасности, физические и программные каналы утечки информации, закладки и вирусы как средства атаки на информационные системы, парольная защита, аутентификация, разграничение прав доступа, способы закрытия информации и их значение. Аппаратные и программно-аппаратные средства защиты информационной безопасности.	4		8	8
2	**Разрушающие программные воздействия и средства несанкционированного доступа (НСД).** Технологии защиты от НСД. Защита операционных систем. Безопасность компьютерной сети. Закрытие информации шифрованием, финансовые применения и протоколы.	2		4	8
3	**Инфраструктура открытых ключей. Защищенные протоколы.** Краткая история развития криптологии. Основные понятия и определения. Подстановочные и перестановочные шифры. Американский стандарт шифрования DES: алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования. Асимметричные системы шифрования (системы с открытым ключом).	4		8	8
4	**Межсетевые экраны, классы их защищенности.** Политика безопасности и стратегия создания брандмауэра. Режим	2		4	8

	функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты.				
5	**Обнаружение атак в глобальных сетях.** Виртуальные сети и прозрачные сетевые службы. Построение защищенных ВЧС. Многоуровневая защита информации в компьютерных системах и сетях.	2		4	5
6	**Информационная безопасность банковских систем и систем электронной коммерции.** Общие сведения об электронной цифровой подписи (ЭЦП). Алгоритм ЭЦП в симметричной криптосистеме. Алгоритм ЭЦП в асимметричной криптосистеме. Проблема обмена открытыми ключами при ЭЦП. Сложные математические задачи и алгоритмы ЭЦП с открытыми ключами. Алгоритм DSA. Алгоритм ГОСТ Р34.10–94. Стандарт ЭЦП Р34.10–2001.	4		8	8
	ВСЕГО	**18**		**36**	**45**

4.2. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр №8				
1	Предмет, методология и понятийный аппарат курса.	Федеральный закон «Об информации, информатизации и защите информации». Методы оценки уязвимости информации	4	4
		Место информационной безопасности ЭИС в национальной безопасности страны. Концепция информационной безопасности.	4	4
2	Разрушающие программные воздействия и средства несанкционированного доступа (НСД)	Комплексная система обеспечения информационной безопасности.	4	4
3	Инфраструктура открытых ключей. Защищенные протоколы.	Современные приложения криптографии	2	2
		Изучение ППП систем криптографической защиты	4	4

		информации, классическая криптография и распределение ключей		
		Практическое применение криптографии с открытым ключом. Пакет PGP	2	2
4	Межсетевые экраны, классы их защищенности.	Методы аутентификации	4	4
5	Обнаружение атак в глобальных сетях	Основные технологии построения защищенных ЭИС	4	4
6	Информационная безопасность банковских систем и систем электронной коммерции	Федеральный закон «Об электронной цифровой подписи». Электронная цифровая подпись (ЭЦП)	4	4
		Криптосистема операционной системы Windows. CryptoAPI: шифрование и дешифрование в CryptoAPI, ЭЦП в проектах на CryptoAPI	4	4
ИТОГО:			36	36
ВСЕГО:				72

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1. Перечень контрольных вопросов (типовых заданий)

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Предмет, методология и понятийный аппарат курса.	1.Место информационной безопасности экономических систем в национальной безопасности страны. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Международные стандарты информационного обмена. 2.Основные положения теории информационной безопасности информационных систем. Конфиденциальность. Целостность. Доступность. 3.Основные положения теории информационной

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		безопасности информационных систем. Объект и субъект доступа. Средство работы с информацией. Несанкционированный доступ к информации. 4.Основные положения теории информационной безопасности информационных систем. Идентификация. Аутентификация. 5.Основные положения теории информационной безопасности информационных систем. Принципы распределения прав и ответственности. 6.Модели безопасности и их применение. Модели доступа. Решетчатая модель. Модель Белл-ЛаПадула. Модель безопасности. 7.Модели безопасности и их применение. Модели доступа. Модель Биба. Модель Гогена-Мезигера. Модель безопасности. 8.Модели безопасности и их применение. Модели доступа. Модель Сазерленда. Модель Кларка-Вильсона. Модель безопасности. 9.Модели безопасности и их применение. Модели доступа. Обязательное управление доступом и переназначаемое управление доступом Доступ по правилам и доступ по ролям. Модель безопасности. 10.Таксономия (классификация) нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Нарушения конфиденциальности. 11.Таксономия (классификация) нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Изменения в системе. 12.Таксономия (классификация) нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Три вида возможных нарушений информационной системы. Утрата работоспособности или производительности.
2	Разрушающие программные воздействия и средства несанкционированного доступа (НСД)	13.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Непреднамеренные действия сотрудников. 14.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Преднамеренные действия сотрудников. 15.Анализ способов нарушений информационной безопасности. Виды противников или "нарушителей". Источники и мотивы нарушений. Действия сторонних лиц криминального характера. 16.Понятие угрозы. Классификация угроз

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
		информационной безопасности. Угрозы, не зависящие от человека. 17.Понятие угрозы. Классификация угроз информационной безопасности. Искусственные угрозы. 18.Понятие угрозы. Классификация угроз информационной безопасности. Угрозы информационной безопасности от использования специальных средств. 19.Атака. Локальная и удаленная атака. Хакер. Кракер. Фрикер. 20.Типовая атака на систему. 21.Локальные атаки. Социальная инженерия. 22.Закладки в аппаратном обеспечении. 23.Преодоление ограничений доступа на уровне firmware. 24.Получение доступа на этапе загрузки ОС.
3	Инфраструктура открытых ключей. Защищенные протоколы.	25. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Шифр Цезаря. Привести пример. 26. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Квадрат Полибия (тюремная азбука). Привести пример. 27. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические пример. Квадрат Кардано. Привести пример. 28. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические примеры. Таблица Виженера. Многоалфавитная замена. Привести пример. 29. Методы криптографии. Основные принципы криптографии. Шифрование. История тайнописи. Исторические примеры. Шифрование по книге. Привести пример. 30. Методы криптографии. Практически стойкий шифр. Абсолютная стойкость шифра. Атака на основе шифротекста, на основе известного открытого текста, на основе выбранного открытого текста. Надежный шифр. 31. Методы криптографии. Поточное шифрование. Исключающее ИЛИ (сложение по модулю 2). 32. Методы криптографии. Линейные регистры сдвига. Привести пример. 33. Методы криптографии. Блочное шифрование. 34. Методы криптографии. Симметричное шифрование (шифрование на секретном ключе). Асимметричное шифрование (шифрование на открытом ключе). 35. Методы криптографии. Электронная цифровая подпись. 36.Методы криптографии. Хэш-функция в электронной цифровой подписи.
4	Межсетевые экраны,	37.Защита. Использование защищенных компьютерных

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
	классы их защищенности.	систем. Механизмы защиты. Нормативно-правовые, морально-этические, организационные и физические (технические) средства защиты. 38.Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые при создании ИС. Сертификация программного обеспечения. 39.Основные технологии построения защищенных ЭИС. Контроль жизненного цикла программного обеспечения с точки зрения информационной безопасности. Мероприятия, осуществляемые в процессе эксплуатации ИС. 40.Концепция информационной безопасности. Концепция информационной безопасности предприятия. Управления рисками. Политика информационной безопасности. 41.Защита. Механизмы защиты. Физические средства защиты. 42.Аппаратно-программные средства защиты. Системы идентификации и аутентификации пользователей. Системы шифрования дисковых данных. 43.Аппаратно-программные средства защиты. Системы аутентификации электронных данных. 44.Аппаратно-программные средства защиты. Средства управления криптографическими ключами.
5	Обнаружение атак в глобальных сетях	45.Атаки на средства аутентификации. Биометрические средства аутентификации. 46.Атаки на средства аутентификации. Токены. 47.Атаки на средства аутентификации. Пароли. Способы хранения паролей Системной политики паролей 48.Атаки на средства аутентификации. Пароли. Имитация системного приглашения Атака на слабость паролей. 49.Атаки класса "повышение привилегий". 50.Постороннее программное обеспечение. 51.Удаленные атаки. Зловредные программы. 52.Понятия о видах вирусов. 53.Удаленные атаки. Атаки на отказ в обслуживании. Маскировка. 54.Удаленные атаки. Атаки на маршрутизацию. Переполнение буфера. 55.Удаленные атаки. Атаки на севрверы: *CGI* и *HTTP*. Атаки на клиентов: *ActiveX*, *Java*. 56.Удаленные атаки. Атаки на поток данных. Активные атаки. Атака повтором. 57.Атака "злоумышленник-посредник". Атаки на основе сетевой маршрутизации. Перехват сессии.
6	Информационная безопасность банковских систем и	58.Информационная безопасность при подключении к Internet. Межсетевые экраны. 59.Информационная безопасность при подключении к

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
	систем электронной коммерции	Internet. Управляемые коммутаторы. 60.Информационная безопасность при подключении к Internet. Сетевые фильтры. 61.Информационная безопасность при подключении к Internet. Шлюзы сеансового уровня. Посредники прикладного уровня. 62.Информационная безопасность при подключении к Internet. Инспекторы состояния.

5.2. Перечень тем курсовых проектов, курсовых работ, их краткое содержание и объем

Курсовая работа не предусмотрена учебным планом по направлению.

5.3. Перечень индивидуальных домашних заданий, расчетно-графических заданий

Успешное выполнение ИДЗ во многом зависит от четкого соблюдения установленных сроков и последовательного выполнения отдельных этапов работы:

1. Выбор темы не позднее, чем за 2 месяца до сдачи работы

2. Подбор научной литературы

3. Написание и представление преподавателю работы не позднее, чем за 7 дней до ее сдачи.

Оформление работы

Текстовый материал в работе должен быть изложен согласно правилам оформления студенческих работ.

Объем расчетно-графического заданя 15-25 стр.

Структура и содержание ИДЗ

Структура работы состоит из следующих частей:

- Введение
- Раздел 1. Теоретические основы изучаемой проблемы
- Раздел 2. Анализ рассматриваемой проблемы на конкретном примере
- Заключение
- Список литературы

В работе следует отразить вопросы, касающиеся рассматриваемой проблемы, в соответствии с приведенным ниже содержанием.

Введение. Во вступительной части рассматриваются основные тенденции изучения и развития проблемы, обосновывается актуальность проблемы, а также формируются цель и задачи работы.

Раздел 1. Теоретические основы изучения проблемы. В данном разделе, прежде всего, необходимо охарактеризовать объект и предмет исследования. Затем оценить степень изученности данной проблемы в научной литературе и привести различные точки зрения по данному вопросу. В процессе изучения имеющихся литературных источников по исследуемой проблеме очень важно найти сходство и различия точек зрения разных авторов, дать их анализ и обосновать свою позицию по данному вопросу.

Раздел 2. Анализ рассматриваемой проблемы на конкретном примере

При выполнении этой части работы студенты должны провести анализ состояния дел по данному вопросу, дать характеристику имеющимся особенностям и высказать свое мнение для их корректировки в случае необходимости.

Заключение

В заключении должны быть приведены основные выводы, вытекающие из результатов проведенного исследования.

Порядок выбора темы

Выбор темы определяется в соответствии со следующей схемой.

Номер темы ИДЗ выбирается в зависимости от номера фамилии студента в журнале группы.

Порядок проверки и защиты ИДЗ

Задание представляется преподавателю на проверку не позднее, чем за 7 дней до ее сдачи.

Ознакомившись с работой, преподаватель принимает решение о форме ее приема. Задание либо зачитывается, либо назначается время сдачи.

Замечания о необходимости доработок содержания оформляются преподавателем на титульном листе. Защита предполагает краткий доклад по ключевым вопросам.

Если работа не представлена в срок, то ее сдача производится комиссии, назначаемой зав. кафедрой.

Темы ИДЗ

1. Доктрина информационной безопасности РФ.
2. Информационное обеспечение государственной политики РФ.
3. Развитие современных информационных технологий.

4. Угрозы информационной безопасности РФ.
5. Информационно-психологическое оружие.
6. Информационо-психологическая война.
7. Защита информационных ресурсов от несанкционированного доступа.
8. Информационный терроризм.
9. Международное сотрудничество РФ в области защиты информации.
10. Государственная тайна.
11. Служебная тайна.
12. Коммерческая тайна.
13. Персональные данные.
14. Личная тайна.
15. Семейная тайна.
16. Тайна ЗАГСа.
17. Врачебная (медицинская) тайна.
18. Тайна вероисповедания.
19. Тайна исповеди.
20. Адвокатская тайна.
21. Тайна следствия.
22. Судебная тайна.
23. Тайна нотариата.
24. Налоговая тайна.
25. Банковская тайна.
26. Журналистская тайна (тайна СМИ).
27. Авторское право.

5.4. Перечень контрольных работ

Контрольные работы не предусмотрены учебным планом по направлению.

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

1. Всеобщая декларация прав человека (от 10 декабря 1948 г.). М., 2015.
2. Конституция РФ. М., 2015.
3. Гражданский кодекс РФ. М., 2015.
4. Доктрина информационной безопасности РФ. М., 2015.
5. Федеральный закон «О государственной тайне» от 21 июля 1993 г. № 5485-1. М., 1993.

6. Башлы П.Н. Информационная безопасность: учебно-практическое пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К. - М.: Изд. центр ЕАОИ, 2011. - 376 с. http://www.biblioclub.ru/book/90539/
7. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации и информационной сфере / Н.Н. Куняев. — М.: Логос, 2010. - 348 с. http://www.biblioclub.ru/book/84990/
8. Креопалов В. В. Технические средства и методы защиты информации: учебно-практическое пособие / В.В. Креопалов. - М.: Изд. центр ЕАОИ, 2011.- 278 с. http://www.biblioclub.ru/book/90753/

6.2. Перечень дополнительной литературы

9. Ярочкин В.И. Информационная безопасность [Электронный ресурс]: учебник для вузов/ Ярочкин В.И.— Электрон. текстовые данные.— М.: Академический Проект, 2008.— 544 с.— Режим доступа: http://www.iprbookshop.ru/36331.html.— ЭБС «IPRbooks»

6.3. Перечень интернет ресурсов

1. http:// www.consultantplus.ru/ - нормативно-правовая база
2. http://www.garant.ru/ - нормативно-правовая база
3. http://www.promo.s-director.ru/ – сайт журнала «Директор по безопасности»
4. http://college.ru/UDP/texts/ – учебный курс «Защита информации»;
5. http://www.mirash.ru/doki11.html - нормативная база по защите информации;
6. http://tk.plexor.ru/web-links/info/38-zakon.html - нормативные документы по защите информации.
7. http://www.inattack.ru/ - антивирусное программное обеспечение
8. http://securityvulns.ru/ - нормативные документы по защите информации
9. http://www.glossary.ru/cgi-bin/gl_sch2.cgi?RIt(uwsg.outtg9!hlnuvgxtuxy
10. http://www.gosecure.ru/ - сайт форматов ЭЦП
11. http://z-oleg.com/ - антивирусное программное обеспечение
12. http://www.aladdin.ru/ - сайт производителя средств защиты информации

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Реализация данной учебной дисциплины осуществляется с использованием материально-технической базы, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской работы обучающихся, предусмотренных программой учебной дисциплины и соответствующей действующим санитарным и противопожарным правилам и нормам:

- оборудованные кабинеты и аудитории;
- компьютерные классы;
- аудитории, оборудованные мультимедийными средствами обучения.

Лекционные занятия – Учебная аудитория для проведения лекционных занятий.

Самостоятельная работа – специализированная аудитория, оснащенная специализированной мебелью, мультимедийным проектором, переносным экраном, ноутбуком.

Лабораторные занятия – компьютерные классы с установленным специализированным лицензионным программным обеспечением: Microsoft Office Professional 2013, Google Chrome Свободно распространяемое ПО согласно условиям лицензионного соглашения. Kaspersky Endpoint Center 10.

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений
Рабочая программа без изменений утверждена на 2017/2018 учебный год.
Протокол № 11 заседания кафедры от « 6 » июня 2017г.

Заведующий кафедрой _____ Селиверстов Ю.И.
подпись ФИО

Директор института _____ Дорошенко Ю.А.
подпись ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2018 /2019 учебный год.

Протокол № 9 заседания кафедры от «21» 05 2018 г.

Заведующий кафедрой _____ Ю.И. Селиверстов

подпись, ФИО

Директор института _____ **Ю.А. Дорошенко**

подпись, ФИО

ПРИЛОЖЕНИЯ

Изучив данную дисциплину, студенты должны компетентно обеспечить информационную безопасность предприятия. Поэтому основная задача сформировать у студентов умение ставить цель исследования, находить проблему и использовать различные методы в исследовании.

Первая тема «**Предмет, методология и понятийный аппарат курса**» является вводной. В ней должны найти отражение вопросы, вводящие студентов в проблематику исследования. Поэтому необходимо определить понятие исследование, его целевое назначение.

Студенты должны понимать объект исследования – роль защиты информации в реализации цели функционирования организации. Они должны различать концепцию информационной безопасности, понимать важность и ценность информации, определять модели информационной безопасности.

Изучая эту тему, студенты должны знать физические и программные каналы утечки информации. Студенты должны научиться выделять закладки и вирусы как средства атаки на информационные системы. Завершить данную тему следует рассмотрением парольной защиты, способов аутентификации, разграничений прав доступа, способов закрытия информации и их значение.

Вторая тема «**Разрушающие программные воздействия и средства несанкционированного доступа**» направлена на изучение общих положений и сущности технологий защиты от несанкционированного доступа. Студенты должны получить представление относительно существующих технологий защиты операционных систем и их основных составляющих. Они должны отличать методологию от метода и от методики, получить представление о проблеме. Студенты должны осознать, что безопасность компьютерной сети имеет не только теоретическое, но и выраженное практическое значение. В этой теме необходимо ознакомить

студентов с существующими подходами к закрытию информации шифрованием.

Кроме того, в этой теме студенты должны уяснить понятийную суть финансовых применений шифрования и существующих для этого протоколов, а также уметь их разрабатывать.

Третья тема «**Инфраструктура открытых ключей. Защищенные протоколы**». В этой теме необходимо ознакомить студентов с краткой историей развития криптологии, основными понятиями и определениями, связанными с процессом шифрования информации, классифицировать подстановочные и перестановочные шифры.

Необходимо рассмотреть основные стандарты шифрования, такие как: американский стандарт шифрования DES и отечественный стандарт шифрования данных ГОСТ 28147-89: их алгоритм, скорость работы на различных платформах, режимы пользования, основные результаты по анализу стойкости. На их основе определить основные подходы к созданию асимметричных систем шифрования (системы с открытым ключом). Подходы позволяют определиться с выбором метода или методов исследования.

Четвертая тема «**Межсетевые экраны, классы их защищенности**» посвящена основным этапам анализа политики безопасности и стратегии создания брандмауэра. К ним в первую очередь относятся такие, как: - режим функционирования межсетевых экранов и их основные компоненты; - маршрутизаторы; - шлюзы сетевого уровня; - усиленная аутентификация. Кроме этого в исследовании работ по совершенствованию информационной безопасности объекта важную роль играет применение межсетевых экранов для организации виртуальных корпоративных сетей и программных методов защиты.

В этой теме студенты должны научиться проводить различие между основными схемами сетевой защиты на базе различных межсетевых экранов.

Пятая тема «**Обнаружение атак в глобальных сетях**» посвящена проблемам отслеживания и отражения постоянно усложняющихся угроз в глобальных сетях, том числе Internet, которые требуют не только знаний, умений, навыков, но и достаточно высокой технической аппаратной оснащенности. В этой теме необходимо рассмотреть такие категории, как виртуальные сети и прозрачные сетевые службы. Далее необходимо рассказать студентам о построении защищенных виртуальных частных сетей и ознакомить их с многоуровневой защитой информации в компьютерных системах и сетях, определить основные принципы грамотного сочетания аппаратной и программной защиты, научить правильно организовывать системы хранения и накопления данных, позволяющие при минимальных затратах обеспечить безопасное пользование информацией.

Шестая тема «**Информационная безопасность банковских систем и систем электронной коммерции**» дает возможность ознакомиться с практической точки зрения с проблемами защиты информации в корпоративных информационных и банковских системах.

Студенты должны изучить общие сведения об электронной цифровой подписи, понять принципы использования алгоритмов ЭЦП в симметричной и асимметричной криптосистеме. К основным базовым понятиям данной группы относятся: алгоритм DSA, алгоритм ГОСТ Р34.10–94, стандарт ЭЦП Р34.10–2001.

Цель этой темы – рассмотреть использование сложных математических задач и алгоритмы ЭЦП с открытыми ключами в корпоративных информационных системах управления, а также выявить основные проблемы при использовании обмена открытыми ключами электронной цифровой подписи в системах банковских платежей и защите персональных данных.