Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Компьютерная безопасность

Направление подготовки 38.03.05 «Бизнес-информатика»

Профиль подготовки Бизнес-информатика

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоем-кость зач. ед,час.	Лек-ции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
5	4/144	18		18	63	Экзамен (45)
Итого	**4/144**	**18**		**18**	**63**	**Экзамен (45)**

Владимир 2016

ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины является изучение основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению информационной безопасности в сфере экономики.

Задачи изучения дисциплины являются получение обучающимися:

- знаний о современных тенденциях угроз информационной безопасности, о нормативных правовых документах по защите информации, а так же о современных методах и средствах обеспечения информационной безопасности в экономических информационных системах;

- умений выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности;

- навыков владения приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах (СЭИС)

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Компьютерная безопасность» относится к дисциплинам по выбору учебного плана.

Для успешного освоения дисциплины «Компьютерная безопасность» требуются знания, приобретенные в результате освоения дисциплин: «Информатика», «Программирование», «Базы данных», «Информационные процессы и их регулирование», «Информационная инфраструктура предприятия».

В процессе освоения дисциплины создаются предпосылки и теоретические основы для изучения дисциплин: «Управление разработкой и жизненным циклом информационных систем», «Разработка мобильных приложений и облачные сервисы».

2. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В процессе освоения данной дисциплины студент формирует и демонстрирует следующие ***профессиональные компетенции***:

проектная деятельность:

- умение осуществлять планирование и организацию проектной деятельности на основе стандартов управления проектами (ПК-14);

консалтинговая деятельность:

- умение консультировать заказчиков по рациональному выбору ИС и ИКТ управления бизнесом (ПК-23).

В результате освоения дисциплины студент должен демонстрировать следующие результаты образования:

Знать:

- основные стандарты управления проектами, методики планирования и организации проектной деятельности на их основе (ПК-14);

- особенности и критерии выбора ИС и ИКТ управления бизнесом (ПК-23).

Уметь:

формулировать задачи и функции деятельности проектной группы (ПК-14);

обосновывать выбор ИС и ИКТ управления бизнесом, исходя из критерия рациональности (ПК-23).

Владеть:

навыками планирования проектной деятельности и ее организации на основе стандартов управления проектами(ПК-14);

навыками консультирования заказчиков по рациональному выбору ИС и ИКТ управления бизнесом (ПК-23).

3. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)							Объем учебной работы, с применением интерактивных методов (в часах/ %)	Формы текущего контроля успеваемости *(по неделям семестра),* форма промежуточной аттестации *(по семестрам)*
				Лекции	Семинары	Практические занятия	Лабораторные работы	Контрольные работы	СРС	КП / КР		
1.	Раздел 1. Основные положения Тема 1. Компьютерная безопасность в условиях функционирования в России глобальных сетей Тема 2. Виды возможных нарушений ИБ ИС Тема 3. Средства защиты ИС.	5	1-6	6			6		21		6/50	Письменные задания Рейтинг 1

2.	Раздел 2. Теория информационной безопасности Тема 4. Основные положения теории информационной безопасности Тема 5. Модели безопасности и их применение Тема 6. Способы нарушений информационной безопасности	5	7-12	6			6		21		6/50	Письменные задания Рейтинг 2
3.	Раздел 3. Защита информации Тема 7. Защищенные ИС Тема 8. Методы криптографии Тема 9. Технологии построения защищенных систем	5	13-18	6			6		21		6/50	Письменные задания Рейтинг 3
Всего				**18**			**18**		**63**		**18/50**	**Экзамен (45)**

СОДЕРЖАНИЕ КУРСА

Тема 1. Основные положения

Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Три вида возможных нарушений информационной системы. Защита. Современная нормативно-законодательная база обеспечения информационной безопасности.

Тема 2. Теория информационной безопасности

Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Основные положения теории информационной безопасности. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности.

Тема 3. Защита информации

Использование защищенных компьютерных систем. Методы криптографии. Основные технологии построения защищенных систем. Место информационной безопасности экономических систем в национальной безопасности страны.

Темы лекционных занятий

Тема 1. Компьютерная безопасность в условиях функционирования в России глобальных сетей

Тема 2. Виды возможных нарушений ИБ ИС

Тема 3. Средства защиты ИС.

Тема 4. Основные положения теории информационной безопасности

Тема 5. Модели безопасности и их применение

Тема 6. Способы нарушений информационной безопасности

Тема 7. Защищенные ИС

Тема 8. Методы криптографии

Тема 9. Технологии построения защищенных систем

Содержание лабораторных работ

Лабораторная работа №1. Компьютерная безопасность в условиях функционирования в России глобальных сетей (2 часа)

Лабораторная работа №2. Виды противников или «нарушителей». Понятие о видах вирусов (2 часа)

Лабораторная работа №3. Основные нормативные руководящие документы, касающиеся информационной безопасности (2 часа)

Лабораторная работа №4. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства (2 часа)

Лабораторная работа №5. Основные положения теории информационной безопасности. Модели безопасности и их применение (2 часа)

Лабораторная работа №6. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности (2 часа)

Лабораторная работа №8. Методы криптографии. Основные технологии построения защищенных систем (2 часа)

Лабораторная работа №9. Место информационной безопасности экономических систем в национальной безопасности страны (2 часа)

4. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.05 Бизнес-информатика, профиль «Бизнес-информатика» компетентностный подход к изучению дисциплины «Компьютерная безопасность» реализуется путем проведения лекций, а также практических занятий с применением мультимедийных технологий.

Преподавание дисциплины ведется с применением следующих видов образовательных

технологий: информационные технологии — обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам (теоретически к неограниченному объему и скорости доступа), подготовка презентаций учебного материала для совместного обсуждения, увеличения контактного взаимодействия с преподавателем и объективного контроля и мониторинга знаний студентов; разрешение проблем — учебные задания, которые требуют от студентов умения мыслить, творчески усваивать знания и развивать навыки их практического применения. Предполагает совместное последовательное движение студенческой аудитории к выстраиванию пути или путей разрешения возникшей проблемы («Дерево решений», «Мозговой штурм» и др.); проблемное обучение — стимулирование студентов к самостоятельному приобретению знаний, необходимых для решения конкретной проблемы; контекстное обучение — мотивация студентов к усвоению знаний путем выявления связей между конкретным знанием и его применением; обучение на основе опыта — активизация познавательной деятельности студента за счет ассоциации и собственного опыта с предметом изучения; индивидуальное обучение — выстраивание студентом собственной образовательной траектории на основе формирования индивидуальной образовательной программы с учетом интересов студента; междисциплинарное обучение — использование знаний, умений и способностей в практической деятельности из разных областей, их группировка и концентрация в контексте решаемой задачи.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Контроль освоения дисциплины производится в соответствии с Положением о рейтинговой системе комплексной оценки знаний студентов ФБГОУ ВО ВлГУ: рейтинг-контроль № 1 и 2 по 10 баллов, рейтинг контроль № 3 – 15 баллов, самостоятельная работа студентов – 15 баллов, посещаемость – 5 баллов, баллы бонуса – 5 баллов.

Текущий контроль студентов производится в дискретные временные интервалы преподавателем, ведущим локаторные занятия по дисциплине, в следующих формах: письменный опрос, контрольная работа (решение задач); отдельно оцениваются личностные качества студента (аккуратность, исполнительность, инициативность) – работа у доски, своевременная сдача лабораторных работ.

Промежуточная аттестация знаний студентов производится по результатам семестра в форме экзамена, который включает в себя ответы на теоретические вопросы и решение задач.

Задания для рейтинг-контроля

Рейтинг-контроль №1

Ответьте на вопросы теста:

Собственником информации не может быть:

а) государство;

б) юридическое лицо;

в) группа физических лиц;

г) физическое лицо;

д) ответы а – г правильны;

е) нет правильного ответа.

2. Терминология в сфере защиты информации регулируется

а) ГОСТ Р 6.30 – 2003

б) ГОСТ 51141 – 98

в) ГОСТ 50922 – 96

г) Гражданским кодексом.

3. Заранее намеченный результат защиты информации – это

а) замысел защиты информации;

б) цель защиты информации;

в) уровень эффективности защиты информации.

4. Содержание и порядок действий, направленных на обеспечение защиты информации – это

а) мероприятие по защите информации;

б) система защиты информации

в) организация защиты информации.

5. Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и (или) собственником информации – это

а) носитель информации

б) собственник информации

в) владелец информации

д) пользователь информации

6. В настоящее время по степени конфиденциальности можно классифицировать информацию,

а) составляющую коммерческую тайну;

б) составляющую государственную тайну;

в) составляющую служебную тайну;

г) составляющую профессиональную тайну.

7. В каких областях деятельности может быть государственная тайна

а) военной

б) образовательной

в) экономической

г) контрразведывательной

д) внешнеполитической

е) внутриполитической

ж) разведывательной

з) оперативно-розыскной

и) экологической

к) правильны все ответы.

8. Классифицированный список типовой и конкретной ценной информации о выполняемых работах, производимой продукции, научных и деловых идеях, технологических новшествах – это

а) перечень ценных и конфиденциальных документов организации

б) перечень конфиденциальных сведений организации

в) перечень типовых документов, образующихся в деятельности организации.

9. Организацией конфиденциального делопроизводства непосредственно занимаются:

а) все сотрудники организации в меру своих сил и обязанностей

б) служба безопасности

в) сектор конфиденциального делопроизводства в составе службы безопасности

г) первый руководитель организации

д) постоянно действующая экспертная комиссия

е) комиссии по проверке наличия, состояния и учета документов

10. Кто имеет право давать разрешение на ознакомление со всеми видами конфиденциальных документов организации всем категориям сотрудников и другим лицам?

а) руководитель службы безопасности

б) первый руководитель организации

в) руководитель сектора конфиденциального делопроизводства в составе службы безопасности

г) правильны все варианты

11. Для работы сотруднику подразделения понадобились конфиденциальные сведения и документы другого подразделения. Кто должен дать разрешение на ознакомление со сведениями и документами?

а) непосредственный начальник этого сотрудника

б) заместитель руководителя организации, курирующий данное направление

в) начальник подразделения, содержащего необходимые конфиденциальные сведения и документы

г) только первый руководитель организации.

12. Конфиденциальные документы уничтожаются, если

а) они являются исполненными

б) истек срок их конфиденциальности

в) истек срок их хранения

13. Отправка нешифрованного конфиденциального документа по факсу

а) не допускается

б) допускается

в) допускается, если на документе стоит гриф конфиденциальности

14. При проверках наличия конфиденциальных документов:

а) проверяют только документы, не трогая дела и иные носители конфиденциальной информации, т.к. в противном случае проверки будут очень громоздкими и долговременными

б) проверяют документы и дела, не трогая иные носители конфиденциальной информации, т.к. все, что связано с компьютерными технологиями, будет проверено специалистами по компьютерной безопасности

в) проверяют документы и дела, а также иные носители конфиденциальной информации

Дайте письменный ответ на следующие вопросы:

1. Понятие и виды конфиденциальной информации в современном российском законодательстве.

2. Государственная тайна.

3. Правовой режим персональных данных. Общая характеристика Федерального закона «О персональных данных»

4. Понятие коммерческой тайны. Общая характеристика Федерального закона «О коммерческой тайне».

5. Понятие и разновидности служебной и профессиональной тайн.

6. Гражданско-правовая, административная и дисциплинарная ответственность за правонарушения в информационной сфере.

Рейтинг-контроль №2

Дайте письменный ответ на следующие вопросы:

Служба конфиденциального делопроизводства, ее статус в структуре организации.

2. Квалификационные характеристики и требования к сотрудникам службы КД.

3. Цели и задачи, права и обязанности, нормативно-методическая база службы КД

4. Анализ угроз несанкционированного получения документированной информации, хищения или уничтожения документов, их фальсификации или подмены. Предполагаемые рубежи и уровни защиты документопотоков

Рейтинг-контроль №3

Ответьте на вопросы теста:

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется

Выберите один ответ.

a. Компилятор

b. Интернет-черви

c. Вирус

2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется

Выберите один ответ.

a. Воздействием (влиянием)

b. Потерей

c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется

Выберите один ответ.

a. Троянской программой

b. Червем

c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата, называется

Выберите один ответ.

a. Устойчивостью

b. Терпимостью по отношению к риску

c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может

выполнять команды

Выберите один ответ.

a. Две

b. Одну

c. Сколько зададут

6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:

Выберите один ответ.

a. Статическими алгоритмами

b. Алгоритмы RMS

c. Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:

Выберите один ответ.

a. Каталоги

b. Символьные файлы

c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются

Выберите один ответ.

a. Вирусами

b. Руткитами

c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:

Выберите один ответ.

a. Правилами безопасности

b. Требованием безопасности

c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

Выберите один ответ.

a. Управление риском

b. Предупреждением рисков

c. Анализом рисков

11 .Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется

Выберите один ответ.

a. Мультипроцессоры типа «хозяин-подчиненный»

b. Симметричный мультипроцессор

c. Мультипроцессор с общей памятью

Дайте письменный ответ на следующие вопросы:

1. Экспертиза ценности конфиденциальных документов

2. Номенклатура конфиденциальных дел. Установление сроков конфиденциальности при составлении номенклатуры дел.

3. Правила формирования и оформления конфиденциальных дел.

Вопросы к экзамену

1. Что такое Компьютерная безопасность?

2. Какие предпосылки и цели обеспечения информационной безопасности?

3. В чем заключаются национальные интересы РФ в информационной сфере?

4. Что включает в себя информационная борьба?

5. Какие пути решения проблем информационной безопасности РФ существуют?

6. Каковы общие принципы обеспечения защиты информации?

7. Какие имеются виды угроз информационной безопасности предприятия (организации)?

8. Какие источники наиболее распространенных угроз информационной безопасности существуют?

9. Какие виды сетевых атак имеются?

10.Какими способами снизить угрозу сниффинга пакетов?

11.Какие меры по устранению угрозы IP -спуфинга существуют?

12.Что включает борьба с атаками на уровне приложений?

13.Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?

14.В чем заключается распределенное хранение файлов?

15.Что включают в себя требования по обеспечению комплексной системы информационной безопасности?

16.Какие уровни информационной защиты существуют, их основные составляющие?

17.В чем заключаются задачи криптографии?

18.Зачем нужны ключи?

19.Какая схема шифрования называется многоалфавитной подстановкой?

20.Какие системы шифрования вы знаете?

21.Что включает в себя защита информации от несанкционированного доступа?

22.В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?

23.Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?

24.Какие задачи выполняет подсистема управления доступом?

25.Какие требования предъявляются к подсистеме протоколирования аудита?

26.Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?

27.В чем заключается контроль участников взаимодействия?

28.Какие функции выполняет служба регистрации и наблюдения?

29.Что такое информационно-опасные сигналы, их основные параметры?

30.Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?

31.Какой процесс называется аутентификацией пользователя?

32.Какие схемы аутентификации вы знаете?

33.Что такое смарт-карты?

34.Какие требования предъявляются к современным криптографическим системам защиты информации?

35.Что такое симметричная криптосистема?

36.Какие виды симметричных криптосистем существуют?

37.Что такое асимметричная криптосистема?

38.Что понимается под односторонней функцией?

39.Как классифицируются криптографические алгоритмы по стойкости?

40.В чем заключается анализ надежности криптосистем?

41.Что такое дифференциальный криптоанализ?

42.В чем сущность криптоанализа со связанными ключами?

43.В чем сущность линейного криптоанализа?

44.Какие атаки изнутри вы знаете?

45.Какая программа называется логической бомбой?

46.Какими способами можно проверить систему безопасности?

47.Что является основными характеристиками технических средств защиты информации?

48.Какие требования предъявляются к автоматизированным системам защиты третьей группы?

49.Какие требования предъявляются к автоматизированным системам защиты второй группы?

50.Какие требования предъявляются к автоматизированным системам защиты первой группы?

51.Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?

52.Какие требования предъявляются к межсетевым экранам?

53.Какие имеются показатели защищенности межсетевых экранов?

54.Какие атаки системы снаружи вы знаете?

55.Какая программа называется вирусом?

56.Какая атака называется атакой отказа в обслуживании?

57.Какие виды вирусов вы знаете?

58.Какие вирусы называются паразитическими?

59.Как распространяются вирусы?

60.Какие методы обнаружения вирусов вы знаете?

61.Какая программа называется монитором обращения?

62.Что представляет собой домен?

63.Как осуществляется защита при помощи ACL -списков?

64.Какой список называется перечнем возможностей?

65.Какие способы защиты перечней возможностей вы знаете?

66.Из чего состоит высоконадежная вычислительная база (ТСВ)?

67.Какие модели многоуровневой защиты вы знаете?

68.В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?

69.Какие характеристики положены в основу системы классификации информационных систем управления предприятием?

70.Какие задачи решает система компьютерной безопасности?

71.Какие пути защиты информации в локальной сети существуют?

72.Какие задачи решают технические средства противодействия экономическому шпионажу?

73.Какой порядок организации системы видеонаблюдения?

74.Что включает в себя защита информационных систем с помощью планирования?

75.Какие условия работы оцениваются при планировании?

76.Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?

77.Что такое мобильные программы?

78.Что такое концепция потоков?

79.Что представляет собой метод «песочниц»?

80.Что такое интерпретация?

81.Что такое программы с подписями?

82.Что представляет собой безопасность в системе Java ?

83.Назовите несколько примеров политик безопасности пакета JDK 1.2?

84.Какие международные документы регламентируют деятельность по обеспечению защиты информации?

85.Что понимают под политикой информационной безопасности?

86.Что включает в себя политика информационной безопасности РФ?

87.Какие нормативные документы РФ определяют концепцию защиты информации?

Самостоятельная работа студентов

Самостоятельная работа студентов является неотъемлемой частью процесса подготовки бакалавра. Она направлена на усвоение системы научных и профессиональных знаний, формирование умений и навыков, приобретение опыта самостоятельной творческой деятельности. СРС помогает формировать культуру мышления студентов, расширять познавательную деятельность.

Виды самостоятельной работы по курсу:

а) по целям: подготовка к лекционным и лабораторным занятиям, к рейтингам, НИР.

б) по характеру работы: изучение литературы, написание эссе; выполнение заданий и тестов; выполнение лабораторных работ; подготовка доклада, презентаций.

Задания для самостоятельной работы (реферат)

1. Основные понятия и определения информационной безопасности. Особенности защиты информации в социально-экономических информационных системах (СЭИС)

2. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах (КЭИС).

3. Правовые меры обеспечения информационной безопасности в социальноэкономических информационных системах (СЭИС).

4. Законодательные и нормативные акты Российской Федерации в области защиты

информации.

5. Использование электронных ключей для организации информационной безопасности в КЭИС.

6. Организационно-административные методы защиты, применяемые в социально-экономических информационных системах.

7. Формирование политики безопасности предприятия (организации).

8. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).

9. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.

10. Симметричные и асимметричные криптосистемы.

11. Электронная цифровая подпись. Использование ЭЦП в экономических системах.

12. Защита информации в компьютерных сетях. Объекты защиты информации в сети.

13. Потенциальные угрозы безопасности в Интранет. Методы защиты информации в Интранет.

14. Потенциальные угрозы безопасности в Интернет (и в частности в электронной коммерции). Методы защиты информации в сети Интернет.

15. Использование межсетевых экранов для обеспечения информационной безопасности в Интернет.

16. Частные виртуальные сети (VPN). Классификация VPN.

17. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.

18. Методы защиты от вредоносных программ в СЭИС.

19. Аудит информационной безопасности.

20. Управление информационными рисками

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2016. — 239 с. : ил. — (Высшее образование: Бакалавриат).

2. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2016. — 322 с. — (Высшее образование). — ww.dx.doi.org/10.12737/11380

3. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2016. — 432 с. — (Среднее профессиональное образование).

б) дополнительная литература

1. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2015. — 416 с. — (Профессиональное образование).

2. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — М. : ИНФРА-М, 2016. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/13571.

3. Информационная безопасность и защита информации: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2015. - 336 с.: 60x90 1/16. - (Высшее образование) (Переплёт 7БЦ) ISBN 978-5-369-01761-6

в) программное обеспечение и Интернет-ресурсы

http://www.edu.ru – Федеральный образовательный портал

http://msdn.microsoft.com/ru-ru/library/ - каталог API (Microsoft) и справочных материалов

https://www.microsoft.com/en-us/download/details.aspx?id=42299 - Microsoft® SQL Server® 2014 Express

https://www.microsoft.com/en-us/download/office.aspx - Microsoft Office

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий практического/лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Лабораторные работы проводятся в аудиториях, оснащенных мульти-медиа оборудованием, компьютерных классах с доступом в интернет.

Перечень используемого лицензионного программного обеспечения:

- Операционная система семейства MicrosoftWindows.
- Пакет офисных программ MicrosoftOffice.
- Консультант+.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 38.03.05 «Бизнес-информатика» профиль подготовки «Бизнес-информатика»

Рабочую программу составил _____ ст. преподаватель Виноградов Д.В.

Рецензент:

Начальник отдела ИТ ООО «Альянс» _____ Чесалкин Н.Б.

Программа рассмотрена и одобрена на заседании кафедры «Бизнес – информатика и экономика»

Протокол № 1 от 30 08 2016 года

Заведующий кафедрой «Бизнес – информатика и экономика»,

д.э.н., профессор _____ И. Б. Тесленко

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 38.03.05 – Бизнес – информатика

Протокол № 1 от 30 08 2016 года

Председатель комиссии _____ И.Б. Тесленко

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ

РАБОЧЕЙ ПРОГРАММЫ ДИСИЦПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017 - 18 учебный год.

Протокол заседания кафедры № 1 от 28.08.2017 года.

Заведующий кафедрой _____

Рабочая программа одобрена на 2018 - 19 учебный год.

Протокол заседания кафедры № 1 от 30.08.2018 года.

Заведующий кафедрой _____

Рабочая программа одобрена на 2019 - 20 учебный год.

Протокол заседания кафедры № 1 от 30.08.2019 года.

Заведующий кафедрой _____

Рабочая программа одобрена на _____ учебный год.

Протокол заседания кафедры № ____ от _____ года.

Заведующий кафедрой _____