Наименование дисциплины и код: **Б.3.19. «Информационная безопасность» гр. БИ-1-15**

Лектор	Старший преподаватель Мусаев Б. М.
Контактная информация:	Кафедра «Прикладной информатики» каб. 102. тел.: раб.0312325120
Количество кредитов:	3 кредита (45 часов)
Дата:	2017-18 учебный год, V семестр
Цель и задачи курса	Целью дисциплины «Информационная безопасность» является ознакомление студентов с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей и, конечно, методов их применения. Задачи дисциплины «Информационная безопасность»: ✓ определение целей и принципов защиты информации; ✓ установление факторов, влияющих на защиту информации; ✓ изучение современной доктрины информационной безопасности; ✓ рассмотрение состава защищаемой информации, ее классификацией по видам тайн, материальным носителям, собственникам и владельцам; ✓ установление структуры угроз защищаемой информации; ✓ определение места конфиденциального документооборота в организациях различного типа; ✓ раскрытие принципов, методов и технологии конфиденциального документооборота.
Описание курса	Дисциплина «Информационная безопасность» направлен на развитие информационных компетенций, необходимых будущим специалистам в любой предметной области. В современной рыночной экономике обязательным условием успеха предпринимателя в бизнесе, получения прибыли и сохранения в целостности созданной им организационной структуры является обеспечение экономической безопасности его деятельности. Одна из главных составных частей экономической безопасности – информационная безопасность.
Пре реквизиты	Для качественного изучения дисциплины рекомендуется использовать в ходе учебного процесса интерактивные доски, электронные учебные пособия по данной дисциплине, видеокурсы и Интернет-ресурсы. Дисциплина относится к профессиональному циклу и изучается в течение одного семестра. Изучение дисциплины завершается сдачей экзамена. Для успешного освоения данного курса студент должен иметь элементарные знания по таким дисциплинам как «Информатика и программирование», «Информационные системы и технологии».

Пост реквизиты	Освоение данной дисциплины необходимо обучающемуся для успешного прохождения производственной практики и выполнения выпускной квалификационной работы. Для обеспечения высокой эффективности учебного процесса, обучающий обязан соблюдать следующие правила: • не опаздывать на занятия; • отключить сотовый телефон; • не пропускать занятия, в случае болезни предоставить справку; • своевременно и старательно выполнять лабораторные задания; • быть терпимым и доброжелательным к сокурсникам и преподавателям; • быть пунктуальным и обязательным; • исключить курение в корпусе университета.
Компетенции	***В результате освоения дисциплины бакалавр должен знать:-*** основы организационной защиты информации, ее современные проблемы и терминологию; - концептуальные, информационные, программные, физические, психологические, математические, криптологические, правовые, экономические, системотехнические и практические основы защиты информации; - принципы организации информационных систем в соответствии с требованиями информационной защищенности, в том числе в соответствии с требованиями по защите коммерческой и государственной тайны; - принципы и методы организационной защиты информации в различных сферах деятельности; - принципы построения современных систем защиты информации в компьютерных системах; - принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; - методы проведения анализа надежности системы защиты информации в компьютерных системах; - методы анализа и оценки величины возможного ущерба, наносимого безопасности организации вследствие несанкционированного (противоправного) распространения информации, составляющей коммерческую тайну; - состав компонентов комплексной системы обеспечения информационной безопасности, функциональные и вспомогательные подсистемы, технологию проектирования и оценки надежности системы защиты; - основные организационные меры обеспечения защиты коммерческой тайны в конкретной сфере деятельности; - основные правовые понятия, правовые акты Кыргызской Республики в области защиты коммерческой и государственной тайны; - правовые нормы и стандарты по лицензированию в области обеспечения защиты коммерческой и государственной тайны и сертификации средств защиты

	информации; - правовые акты в области защиты коммерческой тайны в конкретной сфере деятельности; - руководящие документы по оценке защищенности компьютерных систем; - основные руководящие документы по обеспечению режима и секретности (конфиденциальности) в организации; - конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, потенциальные каналы утечки информации, характерные для этих устройств, способы их выявления и методы оценки опасности, основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации, методы и средства инженерно-технической защиты информации; - типовую структуру службы безопасности, ее основные задачи и функции должностных лиц. ***В результате освоения дисциплины бакалавр должен уметь***: - самостоятельно анализировать и оценивать угрозы информации, применяя соответствующие модели; - анализировать основные механизмы, реализованные в современных операционных системах и базах данных, и модифицировать их для решения задач обеспечения информационной безопасности; - проектировать архитектуру системы информационной защиты, ее технологическое и организационное построение; - проектировать базы данных и распределенные системы обработки информации, обладающие требуемыми характеристиками обеспечения безопасности данных; - применять эффективные методы управления информационной безопасностью; - применять системный подход к обеспечению информационной безопасности в различных сферах деятельности, включая комплекс организационных мер, учитывающих особенности функционирования организации и решаемых ею задач; - оценивать состояние организационной защиты информации на объекте (организации); - используя современные методы и средства разрабатывать и оценивать модели и политику информационной безопасности; - реализовывать системы защиты информации в информационных системах в соответствии со стандартами по оценке защищенных систем. ***В результате освоения дисциплины бакалавр должен владеть***: - методами и формами защиты информации; -технологией составления конфиденциальных документов.
Политика курса	1. Посещение лекций, лабораторных и практических

	занятий должно быть обязательным. Самостоятельная работы студентов (СРС) заключается в выполнении заданий в компьютерном классе, работе с учебной литературой, периодическими изданиями, поиске необходимых материалов с сети Интернет, подготовке и написании докладов и рефератов, выполнение самостоятельно разработанных заданий и примеров, работа с ПЭВМ. 2. Задания выдаются по мере проведения лекционных, лабораторных и практических занятий по данной теме и принимаются во время, выделенное для СРСП. Задания, требующие их выполнение на компьютере, оформлены в виде отдельных упражнений и выдаются каждому студенту индивидуально. Студент, не выполнивший задания для лабораторного занятия или СРС, должен отработать и сдать их до перехода к следующей теме. Рубежный контроль проводится каждые пять недель. 3. Студенты, пропустившие занятия, должны отработать его во время СРС и сдать преподавателю. Преподаватель засчитывает только полностью выполненные лабораторные работы. Студенты, пропустившие без уважительной причины 1/3 часть учебных занятий, к экзамену не допускаются. 4. На занятиях не разрешается пользоваться сотовыми телефонами, выходить из класса и опаздывать. Опоздавшие студенты на занятия не допускаются. 5. Время лекций и практических занятий – 90 минут. Во время лекций и лабораторных занятий преподаватель имеет право удалить из учебной аудитории студентов, мешающих проведению занятия и нарушающих дисциплину, на одно занятие. При повторном нарушении порядка студент освобождается от занятий. 6. Итоговые оценки знаний студентов оцениваются по бальной системе. 7. Для рубежного контроля выполняются индивидуальные задания, а также проводятся, блочное тестирование.
Методы преподавания:	- Лекции; - дискуссии; - выполнение лабораторных работ.

Форма контроля знаний	Оценка знаний будет проводиться на основе европейской системы ECTS. Система ECTS изначально делит студентов между группами «зачтено», «не зачтено», а затем оценивает работу этих двух групп по отдельности. Студенты, набравшие более 50 баллов, получают оценку «зачтено». Из групп получившие оценки «зачтено» на основании итогового контроля получают оценки «отлично» (от 85 до 100 баллов), «хорошо» (от 70 до 84 баллов), «удовлетворительно» (от 50 до 69 баллов). *Баллы итоговой оценки распределяются следующим образом:* Текущая контрольная работа – **40%** Рубежная контрольная работа – **40%** Итоговый контроль –**20%** *При выведении итоговой оценки будут учитываться активность студентов в решении задач, предлагаемых на занятиях.* • Текущая контрольная работа (домашние задания) необходимы для закрепления изученного материала, а также для проверки уровня понимания материала. Домашние задания будут содержать примерами, использующие основные факты и положения. Выполнение домашних заданий даст возможность студентам понимать на должном уровне пройденный материал. • Рубежная контрольная работа дается для проверки знаний по текущим материалам. Будут предложены практические и теоретические задания, раскрывающие понимание основных определений Правильное выполнение контрольных работ, даст студентам приобрести высоких зачетных баллов. Одним из основных условий набора высоких баллов является владение студентом пройденного материала на достаточно высоком уровне. Контрольные работы будут проходить в установленное время. Пересдача контрольных работ не предусматривается. Итоговый контроль – это компьютерное тестирование, чтобы студенты могли, надлежащим образом подготовиться к экзамену заранее дается перечень экзаменационных вопросов. Ответ считается наилучшим, если теоретические факты будут иллюстрированы конкретными примерами.
Литература: **Основная** **Дополнительная**	**Основная**: 1. «Информационная безопасность». Учебное пособие. 2. Герасименко В.А., Малюк А.А. «Основы защиты информации». - М.: ППО «Известия», 1997. 3. Мельников В.И. «Защита информации в компьютерных системах». - М.: «Финансы истатистика», 1997. 4. Милославская Н.Г., Толстой А.И. «Интрасети: доступ в Internet, защита». - М.: ООО«ЮНИТИ-ДАНА», 2000. 5. Проскурин В.Г., Крутов СВ. «Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах». - М: «Радио и связь»,2000. 6. Белкин П.Ю. «Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных». - М.: «Радио и связь», 1999. Касперский Е.В. «Компьютерные вирусы: что это такое и как с ними бороться». - М.:«СК Пресс», 1998. Фролов А.В., Фролов Г.В. «Осторожно: компьютерные вирусы». - М.: «Диалог-МИФИ», 1996. Горбатов В.С. Фатьянов А.А. «Правовые основы защиты информации». - М.: МИФИ,1999. **Дополнительная**: 1. Барсуков В.С. Безопасность: технологии, средства, услуги. – М.: Кудиц-Образ, 2001.

	2. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. – М.: Юридическая литература,1991. 3. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006. 4. Маккарти Л. IT-Безопасность: стоит ли рисковать корпорацией. – М.: Кудиц-Образ, 2004. 5. Мельников В.П. Информационная безопасность / В.П. Мельников, С.А. Клеймёнов, А.М. Петраков. – М.: Academia, 2005 6. Сычёв Ю.Н. Информационная безопасность. – М.: МЭСИ, 2001. 7. ГОСТ Р ИСО/МЭК 27001-2006 – Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. 8. ГОСТ Р ИСО/МЭК 17799-2005 – Информационная технология. Практические правила управления информационной безопасностью. 9. ГОСТ Р ИСО/МЭК 15408-1-2002 – Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
СРС	Общие сведения о программе EASY RECOVERY Восстановление удаленной информации Восстановление информации из корзины Восстановление информации с помощью специальных программ Восстановление файлов с помощью EASY RECOVERY Удаление файлов без возможности восстановления Защита папок и файлов Защита папок и файлов с помощью HIDE FOLDERS XP Копирование образа системы и восстановление операционной системы, приложений, личных параметров и файлов на ПК Общие сведения об ACRONIS TRUE IMAGE Создание образа раздела диска Установка программного обеспечение TrueCrypt Создание и использование контейнера TrueCrypt Защита скрытых томов от повреждений Создание скрытой операционной системы.
Примечание.	Самостоятельные работы студента должны быть представлены в точно установленный преподавателем срок. В случае сдачи работ после установленного срока снимается 50% баллов, полученных студентом.

Календарно-тематический план распределения часов с указанием недели, темы

№	Дата	Тема	К. час	Литература	Подготовительные вопросы по модулям

1	07.09.17	Защита файлов от несанкционированного доступа с помощью архиваторов и средств MS OFFICE	2	**Основная**: 1. «Информационная безопасность». Учебное пособие. 2. Герасименко В.А., Малюк А.А. «Основы защиты информации». - М.: ППО «Известия», 1997. 3. Мельников В.И. «Защита информации в компьютерных системах». - М.: «Финансы истатистика», 1997. 4. Милославская Н.Г., Толстой А.И. «Интрасети: доступ в Internet, защита». - М.: ООО«ЮНИТИ-ДАНА», 2000. 5. Проскурин В.Г., Крутов СВ. «Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах». - М: «Радио и связь»,2000. 6. Белкин П.Ю. «Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных». - М.: «Радио и связь», 1999. Касперский Е.В. «Компьютерные вирусы: что это такое и как с ними бороться». - М.:«СК Пресс», 1998. Фролов А.В., Фролов Г.В. «Осторожно: компьютерные вирусы». - М.: «Диалог-МИФИ», 1996. Горбатов В.С. Фатьянов А.А. «Правовые основы защиты информации». - М.: МИФИ,1999. **Дополнительная**: 1. Барсуков В.С. Безопасность: технологии, средства, услуги. – М.: Кудиц-Образ, 2001. 2. Батурин Ю.М.	1. Какая система называется безопасной и какая надежной? 2. Что такое политика безопасности? 3. Каковы основные предметные направления ЗИ? 4. Что такое государственная тайна? 5. Что называется коммерческой тайной? 6. Что такое служебная тайна? 7. Что представляет профессиональная тайна? 8. Что такое персональные данные? 9. Каковы источники права на доступ к информации? 10. Что такое информация ограниченного распространения? 11. Каковы виды доступа к информации? 12. Дайте определение ИБ. 13. Сформулируйте интересы государства, общества и личности в информационной сфере. 14. Что такое доступность информации? 15. Чем определяется ценность информации для владельца? 16. Что такое конфиденциальная
2	08.09.17	Защита файлов с помощью архиватора WINRAR	2		
3	14.09.17	Подбор пароля для файла WORD	2		
4	21.09.17	Подбор пароля для архива WINRAR	2		
5	22.09.17	Криптография	2		
6	28.09.17	Программы шифрования файлов	2		
7	05.10.17	Шифрование файлов с помощью программы Filecrypt 32	2		
8	05.10.17	Шифрование файлов	2		
9	06.10.17	Шифрование и дешифрование папок с файлами файлов	2		
10	19.10.17	Стеганография. Общие сведения BDVDATAHIDER	2		
11	20.10.17	Шифрование и дешифрование информации	2		
12	26.10.17	Сведения об электронной цифровой подписи. Запуск PGP	2		
13	02.11.17	Создание пары ключей. Экспорт ключа. Импорт ключа. Подпись ключа.	2		
14	03.11.17	Шифрование информации	2		
15	09.11.17	Шифрование и дешифрование текста в буфере	2		

		обмена		Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. – М.: Юридическая литература,1991. 3. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006. 4. Маккарти Л. IT-Безопасность: стоит ли рисковать корпорацией. – М.: Кудиц-Образ, 2004. 5. Мельников В.П. Информационная безопасность / В.П. Мельников, С.А. Клеймёнов, А.М. Петраков. – М.: Academia, 2005 6. Сычёв Ю.Н. Информационная безопасность. – М.: МЭСИ, 2001.	информация, государственная и коммерческая тайна? 17. Назовите три степени секретности. 18. Назовите три категории ценности коммерческой информации. 19. Что такое товарная ценность информации и каковы пути ее получения? 20. Назовите основные методы определения количества информации. 21. Что является предметом защиты в компьютерных сетях? Приведите особенности этого предмета. 22. Перечислите основные виды угроз ИБ. 23. В чем заключается комплексное обеспечение ИБ?
16	16.11.17	Шифрование и дешифрование текста в открытом документе	2		
17	17.11.17	Шифрование и дешифрование файла	2		
18	23.11.17	Общие сведения BESTCRYPT	2		
19	30.11.17	Создание файла – контейнера. Работа с виртуальным диском	2		
20	01.12.17	Закрытие виртуального диска по TIME OUT и HOT KEY	2		
21	07.12.17	Скрытые контейнеры. Принцип защиты данных с использованием скрытых контейнеров, создание скрытого контейнера	2		
22	14.12.17	Утилита очистки, запуск утилиты очистки	2		
23	15.12.17	Общие сведения о восстановлении удаленных файлов	2		
ИТОГО			**45 часов**		

График самостоятельной работы студентов

№	Недели Месяцы	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Суммы балов
		ноябрь								декабрь								
1	Текущий контроль	20								20								40 баллов
2	Срок сдачи СРС*.	15.10 - 25.10. 2017г.								14.12 – 19.12 2017г.								