Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УТВЕРЖДАЮ
Проректор по учебной работе
и менеджменту качества
_____ Е.Н. Живицкая

22.03.2016г.
Регистрационный № УД -6-491/уч.

«ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ»

Учебная программа учреждения высшего образования по учебной дисциплине
для специальности
1-98 01 02 Защита информации в телекоммуникациях

2016 г.

Учебная программа учреждения высшего образования составлена на основе образовательного стандарта ОСВО 1-98 01 02-2013 и учебного плана специальности 1-98 01 02 Защита информации в телекоммуникациях.

Составители:
Т.В.Борботько, профессор кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор;
О.В.Бойправ, ассистент кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Рецензенты:
П.В.Кучинский, директор Научно-исследовательского учреждения «Институт прикладных физических проблем имени А.Н.Севченко» Белорусского государственного университета, доктор физико-математических наук;
В.К.Конопелько, заведующий кафедрой сетей и устройств телекоммуникаций учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», доктор технических наук, профессор.

Рассмотрена и рекомендована к утверждению:
Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 7 от 12.11.2015);
Научно-методическим советом учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 5 от 18.03.2016).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа рассчитана на 372 учебных часа (10,5 з.е.)

План учебной дисциплины в дневной форме обучения:

Код специальности (направления специальности)	Название специальности (направления специальности)	Курс	Семестр	Аудиторных часов (в соответствии с учебным планом уво)				Академ. часов на курс. работу	Типовой расчет	Форма текущей аттестации
				Всего	Лекции	Лабораторные занятия	Практические занятия, семинары			
1-98 01 02	Защита информации в телекоммуникациях	3	6	64	32	16	16			Экзамен
		4	7	96	32	32	32			Экзамен

Место учебной дисциплины.

Банковская система любой страны обеспечивает не только стабильность цен, национальной валюты, но и проведение платежей, сведения о которых являются информацией ограниченного распространения. В настоящее время широко используются системы дистанционного банковского обслуживания, где процедуры проверки личности клиента банка реализуются без его присутствия в его офисе, что обуславливает проблему компрометации идентификатора пользователя и его неправомерное дальнейшее использование. Кроме того, современные автоматизированные банковские системы имеют подключение к сети Интернет, что обуславливает возможность проведения на них атак. Таким образом, защита банковских автоматизированных систем является весьма актуальной и требует подготовки специалистов с соответствующим уровнем компетентности.

Цель учебной дисциплины: получение знаний о принципах и особенностях построения автоматизированных банковских систем, в том числе обеспечивающих удаленное обслуживание клиентов, методах и способах их защиты от несанкционированного доступа.

Задачи изучения учебной дисциплины:

– изучение особенностей организации банковской деятельности в Республике Беларусь;

– изучение архитектуры и способов построения автоматизированных банковских систем и особенностей обеспечения их информационной безопасности;

– изучение архитектуры и способов построения электронных платежных систем и особенностей обеспечения их информационной безопасности;

– изучение архитектуры и способов построения систем дистанционного банковского обслуживания и особенностей обеспечения их информационной безопасности;

– изучение атак на автоматизированные системы, методов и способов противодействия им;

– изучение особенностей применения технологии межсетевого экранирования для решения задач противодействия атакам и несанкционированного доступа в автоматизированных банковских системах.

В результате изучения учебной дисциплины «Защита информации в банковских технологиях» формируются следующие компетенции:

академические:

1) уметь применять базовые научно-теоретические знания для решения теоретических и практических задач;
2) владеть системным и сравнительным анализом;
3) владеть исследовательскими навыками;
4) уметь работать самостоятельно;
5) быть способным порождать новые идеи (обладать креативностью);
6) владеть междисциплинарным подходом при решении проблем;
7) владеть основными методами, способами и средствами получения, хранения, переработки информации с использованием компьютерной техники;
8) на научной основе организовывать свой труд, самостоятельно оценивать результаты своей деятельности;

социально-личностные:

1) обладать способностью к межличностным коммуникациям;
2) уметь работать в команде;

профессиональные:

1) эксплуатировать средства защиты информации и телекоммуникаций.
2) уметь принимать и осваивать средства защиты информации и телекоммуникаций.
3) настраивать, испытывать и обслуживать аппаратно-программные средства защиты информации.
4) совершенствовать, модернизировать и улучшать технико-экономические показатели средств защиты информации и телекоммуникаций.
5) контролировать качество функционирования систем защиты информации и телекоммуникаций.
6) настраивать и обслуживать операционные системы, базы данных и средства телекоммуникаций.
7) применять методы анализа, синтеза и оптимизации структуры систем защиты информации и телекоммуникаций.

8) анализировать и прогнозировать показатели качества функционирования и другие параметры систем защиты информации и телекоммуникаций.

9) взаимодействовать со специалистами смежных профилей.

10) готовить доклады, материалы к презентациям.

11) владеть современными средствами защиты информации и телекоммуникаций.

В результате изучения учебной дисциплины студент должен:

знать:

– принципы организации банковской деятельности в Республике Беларусь;

– архитектуру автоматизированных банковских систем, методы и способы обеспечения их информационной безопасности;

– архитектуру электронных платежных систем, методы и способы обеспечения их информационной безопасности;

– современные базовые технологии, используемые в системах дистанционного банковского обслуживания, методы и способы обеспечения их информационной безопасности;

– методы и способы защиты автоматизированных банковских систем от атак.

уметь:

- анализировать и классифицировать активы и уязвимости в автоматизированных банковских системах и обоснованно выбирать средства защиты информации;

- анализировать и оценивать риски информационной безопасности, а так же затраты на реализацию мероприятий по защите информации;

- составлять политику безопасности;

- анализировать трафик, передаваемый в информационных системах и обоснованно идентифицировать угрозы информационной безопасности;

- разрабатывать системы защиты автоматизированных банковских систем.

владеть:

- средствами защиты информации.

Перечень учебных дисциплин, усвоение которых необходимо для изучения данной учебной дисциплины

№ п.п.	Название учебной дисциплины	Раздел, темы
1	Компьютерные сети	Все разделы учебной дисциплины

1. Содержание учебной дисциплины

№ тем	Наименование разделов, тем	Содержание тем
1. Организация и автоматизация банковской деятельности в Республике Беларусь		
1	Банковская система Республики Беларусь	Национальная платежная система Основные правовые аспекты функционирования. Принципы банковской деятельности. Платежные услуги, предоставляемые банковской системой.
2	Межбанковские переводы средств и расчеты	Структура системы межбанковских расчетов Республики Беларусь. Система BISS. Клиринговая система. Правила осуществления операции и участники системы. Переводы и расчеты по международным транзакциям.
3	Архитектура автоматизированной банковской системы	Обобщенная структура автоматизированной банковской системы. Основные модули и их функции. Архитектура системы, базирующаяся на общем финансовом ядре.
4	Автоматизированная система межбанковских расчетов	Участники системы. Архитектура автоматизированной системы межбанковских расчетов. Основные модули и их назначение. Особенности функционирования.
5	Автоматизированная информационная система единого расчетного и информационного пространства	Участники системы. Архитектура автоматизированной информационной системы единого расчетного и информационного пространства. Основные модули и их назначение. Особенности функционирования.
6	Обеспечение информационной безопасности автоматизированных банковских систем	Особенности защиты информации. Принципы контроля функционирования. Внешний ресурс (outsourcing). Уязвимости различных степеней критичности. Механизмы защиты автоматизированных банковских систем. Требования стандарта безопасности данных индустрии платежных карт PCI DSS.
7	Системы резервного копирования данных	Назначение. Методы резервного копирования данных. Архитектура систем резервного копирования данных.
2. Электронные платежные системы		
8	Технология электронного обмена данными	Назначение. Основные этапы технологии и сущность. Основные функции программного обеспечения технологии. Компоненты технологии. Архитектура систем электронного обмена данными.
9	Структура электронной платежной системы	Электронная коммерция. История развития систем электронной коммерции. Виды систем электронной коммерции. Архитектура электронной платежной системы. Виды электронных платежных систем. Обзор технологии электронных платежных карт. Система Белкарт. Система MasterCard. Система Visa.
10	Технология электронных денег	Дематериализованные платежные средства. Платежная система на основе электронных кошельков. Угрозы безопасности электронных платежных систем. Обеспечение информационной безопасности.

№ тем	Наименование разделов, тем	Содержание тем
11	Международная платежная система SWIFT	Назначение. Архитектура. Маршрутизация. Обеспечение безопасности.
3. Системы дистанционного банковского обслуживания		
12	Основы построения систем дистанционного банковского обслуживания	Назначение и особенности построения систем дистанционного банковского обслуживания. Данные платежных карт и элементы критичных данных авторизации подлежащих защите. Классификация типов мошенничества. Способы аутентификации в системах дистанционного банковского обслуживания. Персональный идентификатор.
13	Архитектура типовых систем дистанционного банковского обслуживания	Архитектура системы Интернет-банкинга и обеспечение информационной безопасности. Протокол TLS. Архитектура системы мобильного банкинга (М-банкинг) и обеспечение информационной безопасности. Архитектура системы SMS банкинга и обеспечение информационной безопасности. Обобщенная архитектура системы fraud-мониторинга.
14	Системы дистанционного банковского обслуживания на основе АТМ и POS терминалов	Назначение и режимы работы автоматических кассовых аппаратов (АТМ). Разделяемые сети АТМ. Классификация мошенничества и методы противодействия ему. Системы обеспечения расчета в точке продажи (POS). Система mPOS. Обеспечение информационной безопасности. Системы видеоконтроля АТМ и POS терминалов.
4. Защита автоматизированных систем от атак		
15	Общие сведения об атаках	Основные этапы атаки и особенности их реализации. Объекты защиты от атак в автоматизированных системах. Понятие подчиненных вычислительных систем (ботнет). Способы удаленного управления ботнетом. Архитектура ботнетов.
16	Классификация атак	Сетевая разведка. Анализ сетевого трафика. Спуфинг. Атаки отказ в обслуживании (DoS). Атаки на уровне приложений. Парольные атаки. Атака “Man in the middle”. Атака Митника.
17	Основы построения систем противодействия атакам	Состав комплекса противодействия атакам. Организационно-правовые мероприятия. Способы обнаружения атак. Классификация систем обнаружения вторжений. Типы датчиков и примеры размещения. Системы-ловушки (honeypots). Сканеры уязвимостей. Алгоритмы распознавания атак. Способы противодействия сетевой разведке, анализу сетевого траффика, DoS атакам, атакам на уровне приложений и парольным атакам. Обнаружение снифферов.
18	Системы противодействия утечки данных (DLP)	Назначение. Архитектура. Основные модули и особенности их функционирования.
19	Программно-аппаратные средства защиты информации от несанкциониро-	Программно-аппаратный комплекс "Аккорд". Архитектура. Основные модули и реализуемые функции. Построение системы защиты информации с использованием программно-аппаратного комплекса "Аккорд".

№ тем	Наименование разделов, тем	Содержание тем
	ванного доступа	
5. Применение межсетевых экранов в автоматизированных системах		
20	Основные компоненты архитектуры межсетевых экранов	Архитектура межсетевого экрана. База правил. Журнал событий. Модуль управления. Модуль мониторинга и оповещения. Модуль создания отчетов. Способы реализации. Типы межсетевых экранов. Особенности межсетевого экранирования на различных уровнях модели OSI.
21	Основные схемы подключения межсетевых экранов	Концепция демилитаризованной зоны. Схема подключения межсетевых экранов с несколькими сетевыми адаптерами. Применение межсетевых экранов с одним сетевым адаптером.
22	Трансляция сетевых адресов (NAT)	Сущность концепции трансляции сетевых адресов. Статическая трансляция сетевых адресов. Динамическая трансляция сетевых адресов. Трансляция портов.
23	Аутентификация в автоматизированных системах	Методы аутентификации. Аутентификация пользователей. Аутентификация клиентов. Аутентификация сессии.
24	Виртуальные частные сети	Сущность концепции виртуальных частных сетей. Архитектура виртуальных частных сетей.
25	Противодействие спаму	Способы организации массовых рассылок. Основные виды спама и методы его обнаружения. Защита от спама на стороне сервера. Защита от спама на стороне клиента.
26	Противодействие вредоносным программам	Классификация вредоносных программ. Жизненный цикл вредоносных программ. Методы обнаружения вредоносных программ. Способы противодействия вредоносным программам.
27	Применение методов и средств защиты информации в автоматизированных системах	Аутентификация пользователя. Обеспечение конфиденциальности передаваемых данных. Применение концепции демилитаризованной зоны. Обеспечение информационной безопасности подсистемы “Интернет-клиент”.

2. Информационно-методический раздел

2.1 Литература

2.1.1 Основная

1. Банкаускі Веснік. – 2001. – № 31. – С. 7–51.

2. Пупликов С.И., Коноплицкая М.А., Шмарловская С.С. Банковские операции: Учеб. пособие / Под общ. ред. Пупликова С.И. – Минск.: Выш. шк., 2003. – 351 с.

3. Лыньков Л.М., Борботько Т.В., Мухуров Н.И., Беляев Б.И., Катковский Л.В. Защита информации в банковских технологиях. – Учебн. - метод. пособие. Минск: БГУИР, 2008. – 194 с.

4. Деднев М.А., Дыльнов Д.В., Иванов М.А. Защита информации в банковском деле и электронном бизнесе. М.: Кудиц-образ, 2004. – 512 с.

5. Обеспечение информационной безопасности бизнеса / Под ред. Курило А.П. – М.: Издательская группа БДЦ-Пресс, 2005. – 512 с.

6. Мартынов, В.Г. Электронные деньги и мобильные платежи / В.Г. Мартынов [и др.]. – М: КНОРУС: ЦИПСиР, 2009. – 368 с.

7. Бил Джей. Snort 2.1. Обнаружение вторжений. – М.: Бином, 2011. – 656 с.

8. Шаньгин В. Информационная безопасность компьютерных систем и сетей. – М.: Форум, 2011. – 416 с.

9. Джуди Новак, Стивен Норткатт, Дональд Маклахлен. Как обнаружить вторжение в сеть (Network intrusion detection an analyst’s handbook).– М.: Лори, 2012. – 384 с.

10. Лапонина О.Р. Межсетевое экранирование. М. : Бином, 2007. – 344 с.

2.1.2 Дополнительная

11. Голдовский И. Безопасность платежей в Интернете. – СПб.: Питер, 2001. – 240 с.

12. Курило А.П. Аудит информационной безопасности. М. : Издательская группа «БДЦ-пресс», 2006. – 304 с.

13. Касперски К. Записки исследователя компьютерных вирусов. Санкт-Петербург : Питер, 2005. – 316 с.

2.2 Перечень компьютерных программ, наглядных и других пособий, методических указаний и материалов, технических средств обучения, оборудования для выполнения лабораторных работ

1. Стандарт безопасности данных индустрии платежных карт (PCI DSS). Требования и процедуры аудита безопасности. Версия 3.0. – Введ. ноябрь 2013. – PCI Security Standards Council, LLC, 2013. – 143 с.

2. Технологии применения программно-аппаратных комплексов средств защиты информации от несанкционированного доступа семейств АККОРД и ШИПКА: практикум / В.А. Конявский [и др.]. – М : РФК-Имидж Лаб, 2009. – 308 с.

3. Защита информации в банковских технологиях: Лабораторный практикум: учеб.-метод. пособие / Б. И. Беляев [и др.]. – Минск : БГУИР, 2010. – 126 с.

4. Защита информации в компьютерных сетях: Практический курс: учеб. пособие / А. Н. Андрончик [и др.]. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.

5. Обнаружение нарушений безопасности в сетях / Стивен Норткат, Джуди Новак. – М : Издательский дом «Вильямс», 2003. – 448 с.

6. Буянов В.П., Уфимцев Ю.С., Ерофеев Е.А. Методика информационной безопасности. М.: Экзамен, 2004. – 544 с.

7. Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи, 2006. – 400 с.

8. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК Пресс, 2005. – 485 с.

9. Международная телекоммуникационная сеть SWIFT: Метод. руководство к лабораторно-практическим занятиям по курсу "Телекоммуникационные системы в банковских технологиях" / Л.М. Лыньков, Н.А. Маслакова, Г.В. Подельщикова, А.М. Прудник. — Минск : БГУИР, 2002. — 56 с.

10. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – 304 с.

11. Программа Acronis True Image.

12. Программа «Защита систем электронного обмена данными».

13. Программа «Защита удаленных банковских транзакций».

14. Программа «Защита автоматических кассовых аппаратов».

15. Программа Ethereal.

16. Программа Single-honeypot.

17. Программа DLP система SearchInform.

18. Программно-аппаратный комплекс «Аккорд».

19. Программа L0phtcrack.

20. Программа «Защита автоматизированных систем от атак».

21. Ивановский В. DLP: Как защитить секреты от утечки. Цифровой журнал «Компьютерра». – 2011. – № 86.

22. Яремчук С.А. Защита Вашего компьютера / С.А. Яремчук. – СПб: Питер, 2008. – 288 с.

23. Джеймс Л. Фишинг: техника компьютерных преступлений / Л. Джеймс. – М. : НТ Пресс, 2008. – 320 с.

2.3. Перечень тем практических занятий, их название

Целью практических занятий является закрепление теоретического курса, приобретение навыков решения задач, активизация самостоятельной работы студентов.

№ темы по п.1	Название практического занятия	Обеспеченность по пункту 2.2
1	Требования и процедуры аудита безопасности индустрии платежных карт	1
2	Методика описания информационной системы предприятия	6
3	Методика оценки необходимости защиты информации на предприятии	6
3	Оценка затрат на реализацию мероприятий по защите информации на предприятии	6
6	Методика оценки рисков CRAMM	8
6	Политика информационной безопасности	7
6	Аудит информационной безопасности предприятия	8
11	Международная платежная система SWIFT. Структура сообщений	9
15	Особенности передачи данных в информационных сетях	5
16	Сканирование портов и перехват TCP сессии	5
16	Использование протокола ICMP при сетевой разведке	5
16	Основы анализа трафика с помощью Windump	5
16	Составление правил для системы обнаружения вторжений Snort	5
18	Анализ алгоритмов работы DLP систем	21
20	Анализ доступности сведений на различных уровнях модели OSI	10
21	Построение демилитаризованных зон с помощью межсетевых экранов	10
22	Трансляция сетевых адресов	10
25	Анализ эффективности мероприятий по противодействию спаму и фишинг-атакам	22, 23
27	Планирование мероприятий по обеспечению безопасности автоматизированных систем	5

2.4. Перечень тем лабораторных занятий, их название

Основная цель проведения лабораторных занятий состоит в закреплении теоретического материала курса, приобретении навыков выполнения эксперимента, обработки экспериментальных данных, анализа результатов, грамотного оформления отчетов.

№ темы по п.1	Наименование лабораторной работы	Обеспеченность по пункту 2.2
7	Установка и настройка программ резервного копирования данных	11
8	Обеспечение безопасности систем электронного обмена данными	3, 12

№ темы по п.1	Наименование лабораторной работы	Обеспеченность по пункту 2.2
12	Защита удаленных банковских транзакций	3, 13
14	Защита автоматических кассовых аппаратов	3, 14
16	Анализ и захвата трафика с помощью программы Ethereal	4, 15
17	Установка и настройка Honeypot	16
18	Анализ данных с использованием DLP-систем	17
19	Изучение программно-аппаратного комплекса «Аккорд»	18
23	Оценка стойкости паролей к brute force атакам	19
24	Организация виртуальных частных сетей	4, 25
27	Защита автоматизированных систем от атак	3, 20

3.1 Учебно-методическая карта учебной дисциплины в дневной форме обучения

Номер раздела, темы по п.1	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
6 семестр						
1. Организация и автоматизация банковской деятельности в Республике Беларусь						
1	Банковская система Республики Беларусь	2		2	6	Фронтальный опрос. Защита ПЗ
2	Межбанковские переводы средств и расчеты	2		2	6	Фронтальный опрос. Защита ПЗ
3	Архитектура автоматизированной банковской системы	2		4	6	Фронтальный опрос. Защита ПЗ
4	Автоматизированная система межбанковских расчетов	2			5	Фронтальный опрос
5	Автоматизированная информационная система единого расчетного и информационного пространства	2			5	Фронтальный опрос
6	Обеспечение информационной безопасности автоматизированных банковских систем	2		6	6	Фронтальный опрос. Защита ПЗ
7	Системы резервного копирования данных	2	4		6	Фронтальный опрос. Защита ЛР
2. Электронные платежные системы						
8	Технология электронного обмена данными	2	4		6	Фронтальный опрос. Защита ЛР
9	Структура электронной платежной системы	2			5	Фронтальный опрос

Номер раздела, темы по п.1	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
10	Технология электронных денег	2			6	Фронтальный опрос.
11	Международная платежная система SWIFT	2		2	6	Фронтальный опрос. Защита ПЗ
3. Системы дистанционного банковского обслуживания						
12	Основы построения систем дистанционного банковского обслуживания	2	4		6	Фронтальный опрос. Защита ЛР
13	Архитектура типовых систем дистанционного банковского обслуживания	4			5	Фронтальный опрос
14	Системы дистанционного банковского обслуживания на основе АТМ и POS терминалов	4	4		6	Фронтальный опрос. Защита ЛР
	Всего за 6 семестр	**32**	**16**	**16**	**80**	
	Текущая аттестация					**Экзамен**
7 семестр						
4. Защита автоматизированных систем от атак						
15	Общие сведения об атаках	2		8	10	Фронтальный опрос. Защита ПЗ
16	Классификация атак	2	4	10	10	Фронтальный опрос. Защита ЛР и ПЗ
17	Основы построения систем противодействия атакам	6	4		10	Фронтальный опрос. Защита ЛР
18	Системы противодействия утечки данных (DLP)	2	4	2	10	Фронтальный опрос. Защита ЛР и ПЗ
19	Программно-аппаратные средства защиты информации от несанкционированного доступа	2	8		10	Фронтальный опрос. Защита ЛР
5. Применение межсетевых экранов в автоматизированных системах						
20	Основные компоненты архитектуры межсетевых экранов	4		2	10	Фронтальный опрос. Защита ПЗ
21	Основные схемы подключения межсетевых экранов	2		2	10	Фронтальный опрос.

Номер раздела, темы по п.1	Название раздела, темы	Количество аудиторных часов			Самостоятельная работа, часы	Форма контроля знаний
		ЛК	Лаб. зан.	ПЗ		
						Защита ПЗ
22	Трансляция сетевых адресов	2		2	10	Фронтальный опрос. Защита ПЗ
23	Аутентификация в автоматизированных системах	2	4		10	Фронтальный опрос. Защита ЛР
24	Виртуальные частные сети	2	4		10	Фронтальный опрос. Защита ЛР
25	Противодействие спаму	2		4	10	Фронтальный опрос. Защита ПЗ
26	Противодействие вредоносным программам	2			10	Фронтальный опрос.
27	Применение методов и средств защиты информации в автоматизированных системах	2	4	2	12	Фронтальный опрос. Защита ЛР и ПЗ
	Всего за 7семестр	**32**	**32**	**32**	**132**	
	Текущая аттестация					**Экзамен**
	Итого	**64**	**48**	**48**	**212**	

4. Рейтинг-план

Рейтинг-план дисциплины
Защита информации в банковских технологиях, дневная
(название дисциплины согласно учебному плану, форма обучения)
Специальность 1-98 01 02 Защита информации в телекоммуникациях
курс 3, семестр 6.
Количество часов по учебному плану 144, в т.ч. аудиторная работа 64, самостоятельная работа 80
Преподаватель Борботько Тимофей Валентинович, д.т.н., профессор
(ФИО, ученая степень, ученое звание)
Кафедра защиты информации

Рекомендовано на заседании кафедры
защиты информации
Протокол № 7 от «12» ноября 2015 г.

Зав. кафедрой ЗИ _____ /Л.М. Лыньков/

Преподаватель _____ /Т.В. Борботько/

Выставление отметки по текущей аттестации не допускается по результатам итогового рейтинга студента.

Виды учебной деятельности студентов	Модуль 1 (весовой коэффициент вк1=0,25)		Модуль 2 (весовой коэффициент вк2=0,25)		Модуль 3 (весовой коэффициент вк3=0,25)		Модуль 4 (весовой коэффициент вк4=0,25)		Итоговый контроль по всем модулям
	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	
1. Лекционные занятия		к11=0,3		к12=0,3		к13=0,3		к14=0,3	
Темы 1-3	15.03.								
Темы 4-6			15.04.						
Темы 7-10					15.05.				
Темы 11-14							31.05.		
2. Лабораторные работы		к21=0,35		к22=0,35		к23=0,35		к24=0,35	
1	15.03.								
2			15.04.						
3					15.05.				
4							31.05.		
3. Практические занятия		к31=0,35		к32=0,35		к331=0,35		к34=0,35	
1-2	15.03.								
3-4			15.04.						
5-6					15.05.				
7-8							31.05.		
Модульный контроль		МР1		МР2		МР3		МР4	ИР

Рейтинг-план дисциплины
Защита информации в банковских технологиях, дневная
(название дисциплины согласно учебному плану, форма обучения)
Специальность 1-98 01 02 Защита информации в телекоммуникациях
курс 4, семестр 7 .
Количество часов по учебному плану 228, в т.ч. аудиторная работа 96, самостоятельная работа 132
Преподаватель Борботько Тимофей Валентинович, д.т.н., профессор
(ФИО, ученая степень, ученое звание)
Кафедра защиты информации

Рекомендовано на заседании кафедры
защиты информации
Протокол № 7 от «12» ноября 2015 г.

Зав. кафедрой ЗИ _____ /Л.М. Лыньков/

Преподаватель _____ /Т.В. Борботько/

Выставление отметки по текущей аттестации не допускается по результатам итогового рейтинга студента.

Виды учебной деятельности студентов	Модуль 1 (весовой коэффициент вк1=0,25)		Модуль 2 (весовой коэффициент вк2=0,25)		Модуль 3 (весовой коэффициент вк3=0,25)		Модуль 4 (весовой коэффициент вк4=0,25)		Итоговый контроль по всем модулям
	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	Календарные сроки сдачи	Весовой коэффициент отметки	
1. Лекционные занятия		к11=0,3		к12=0,3		к13=0,3		к14=0,3	
Темы 15-17	15.09.								
Темы 18-21			15.10.						
Темы 22-24					15.11.				
Темы 25-27							31.12.		
2. Лабораторные работы		к21=0,35		к22=0,35		к23=0,35		к24=0,35	
1-2	15.09.								
3-4			15.10.						
4-5					15.11.				
6-7							31.12.		
3. Практические занятия		к31=0,35		к32=0,35		к331=0,35		к34=0,35	
1-4	15.09.								
5-8			15.10.						
9-12					15.11.				
13-16							31.12.		
Модульный контроль		МР1		МР2		МР3		МР4	ИР

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Код и наименование специальности	Выпускающая кафедра	Предложения об изменениях в содержании по изучаемой учебной дисциплине	Подпись заведующего выпускающей кафедрой с указанием номера протокола и даты заседания кафедры
1-98 01 02 Защита информации в телекоммуникациях	Кафедра защиты информации	изменения не требуются	_____ протокол № 7 от 12.11.2015 г.

Заведующий кафедрой защиты информации Л.М. Лыньков