

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»



УТВЕРЖДАЮ:

Проректор по научно-педагогической работе

А.В. Мешков
(подпись) И.О. Фамилия

« 29 » 05 20 17 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Системы банковской безопасности»

(наименование дисциплины согласно учебному плану)

Направление (специальность)
подготовки:

10.03.01 «Информационная безопасность»

(код и наименование направления / специальности)

Направленность:

Информационная безопасность

(наименование профиля / магистерской программы / специализации)

Уровень образования:

бакалавриат

(бакалавриат, магистратура, специалитет)

Форма обучения:

очная

(очная, заочная, очно-заочная)

Семестры	7
Общая трудоёмкость в з.е./часах	2,5/90
Аудиторные занятия (час.), в том числе	34
Лекции (час.)	17
Практические (семинарские) занятия (час.)	-
Лабораторные работы (час.)	17
Самостоятельная работа (час.), в том числе	38
Курсовой проект/работа (сем/кол.)	-
Индивидуальное задание (сем/кол.)	1
Форма промежуточной аттестации (экзамен/зачёт):	Экзамен

Донецк, 2017 г.

Рабочая программа дисциплины «Системы банковской безопасности» составлена в соответствии с учебным планом по направлению подготовки 11.03.01. Информационная безопасность для 2015 года приёма.

Составитель: старший преподаватель кафедры Радиотехники и защиты информации Ванда Н.И.

Рабочая программа **рассмотрена и утверждена** на заседании кафедры Радиотехники и защиты информации

Протокол от «3» 09 2016 года № 2

Заведующий кафедрой _____ (подпись) В.В. Паслен (Ф.И.О.)

Рабочая программа **согласована с выпускающей кафедрой** Радиотехники и защиты информации

Протокол от « » _____ 2017 года № _____

Заведующий кафедрой _____ (подпись) В.В. Паслен (Ф.И.О.)

Рабочая программа **одобрена учебно-методической комиссией** ДонНТУ по направлению (специальности) подготовки 11.03.01. Информационная безопасность

Протокол от «30» 09 2016 года № 2

Председатель _____ (подпись) В.В. Паслен (Ф.И.О.)

Рабочая программа **продлена** для 20 17 года приёма на заседании кафедры Радиотехники и защиты информации.

Протокол от «25» 05 20 17 года № 10
Заведующий кафедрой _____ (подпись) Паслен В.В. (Ф.И.О.)

Согласовано с выпускающей кафедрой Радиотехники и защиты информации.
Заведующий кафедрой _____ (подпись) Паслен В.В. (Ф.И.О.)

Рабочая программа **продлена** для 20 18 года приёма на заседании кафедры Радиотехники и защиты информации.

Протокол от «31» 08 20 18 года № 1
Заведующий кафедрой _____ (подпись) Паслен В.В. (Ф.И.О.)

Согласовано с выпускающей кафедрой Радиотехники и защиты информации.

Заведующий кафедрой _____ (подпись) Паслен В.В. (Ф.И.О.)

Рабочая программа **продлена** для 20 19 года приёма на заседании кафедры Радиотехники и защиты информации.

Протокол от «28» 08 20 19 года № 1
Заведующий кафедрой _____ (подпись) Паслен В.В. (Ф.И.О.)

Согласовано с выпускающей кафедрой Радиотехники и защиты информации
Заведующий кафедрой _____ (подпись) Паслен В.В. (Ф.И.О.)

1. ОБЪЕКТ, ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина рассматривает вопросы: Основы безопасности банковской деятельности. Угрозы банка. Недобросовестная конкуренция и промышленный шпионаж. Охрана и режим в банке. Информационная безопасность банка. Экономическая безопасность банка. Информационно-аналитическое обеспечение деятельности банка. Организация безопасности в работе с персоналом. Действия учреждений банков в экстремальных условиях. Защита компьютерных технологий и систем банка.

Целью дисциплины является: участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов банка на предмет соответствия требованиям защиты информации; сбор и анализ исходных данных для проектирования систем защиты информации; определение требований, сравнительный анализ систем по показателям информационной безопасности; организация работы малых коллективов исполнителей с учетом требований защиты банковских учреждений; изучение и совершенствование систем управления информационной и технической безопасности банка; контроль эффективности реализации политики информационной безопасности объекта.

В результате освоения дисциплины студент должен

знать: концептуальные основы безопасности банка, классификацию угроз безопасности банковской деятельности; правовые и организационные основы противодействия этим угрозам, а также технику обеспечения безопасности банка; наиболее распространенные виды преступлений, посягающих на ведущие элементы безопасности банка; рациональные способы и приемы выявления, предупреждения и пресечения указанных преступных посягательств; принципы организации информационной безопасности на предприятии.

уметь: реализовывать мероприятия для предотвращения угроз в сфере банковской безопасности; использовать полученные знания при проектировании систем технической защиты банковской деятельности; разрабатывать средства и системы защиты информации.

Перечисленные результаты обучения являются основой для формирования следующих компетенций:

общекультурными компетенциями (ОК):

- способностью находить организационно-управленческие решения в нестандартных ситуациях и готовностью нести за них ответственность (ОК - 5);

- способностью осознавать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности, готовностью и способностью к активной созидательной деятельности в условиях информационного противоборства (ОК - 6);

- способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения, владеть культурой мышления (ОК - 7);

общепрофессиональными компетенциями (ОПК):

- способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ОПК - 6);

- способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ОПК - 8);

профессиональными компетенциями (ПК):

- способностью администрировать подсистемы информационной безопасности объекта (ПК - 2); 23, 16,

2. МЕСТО ДИСЦИПЛИНЫ В ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

Дисциплина относится к профессиональному циклу вариативной части дисциплин по выбору вуза учебного плана.

Базируется на знаниях и умениях, которые студент приобрел при освоении предшествующих дисциплин: безопасность информационных и коммуникационных систем, криптография и стеганография, методы и средства защиты информации, схемотехника устройств технической защиты информации, создание и обработка баз данных ПЭВМ.

Знания и умения, приобретенные при освоении данной дисциплины, реализуются студентом при изучении последующих дисциплин (технические средства охраны объектов, управление информационной безопасностью, организационное обеспечение технической защиты информации), прохождении учебной или производственной практики, прохождении государственной итоговой аттестации.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Распределение учебных часов по темам дисциплины и видам занятий

Наименование тем (содержательных модулей)	Количество часов				
	Всего	В том числе			
		Лекции	Практ. (Семина.)	Лабор.	СРС
Тема 1. Основы безопасности банковской деятельности.	10	2		2	8
Тема 2. Угрозы банка.	12	2		2	8
Тема 3. Недобросовестная конкуренция и промышленный шпионаж.	12	2		2	10
Тема 4. Охрана и режим в банке.	12	2		2	10
Тема 5. Информационная безопасность банка.	12	2		2	10
Тема 6. Экономическая безопасность банка.	12	2		2	10

Тема 7. Информационно-аналитическое обеспечение деятельности банка.	10	2		2	10
Тема 8. Организация безопасности в работе с персоналом.	10	2		2	10
Итого:	108	16		16	76

3.2. Лекции

Тема 1. Основы безопасности банковской деятельности.

Содержание темы 1: Введение. Понятие безопасности банка, ее цель и задачи. Виды безопасности и формы ее организации. Силы и средства безопасности банковской деятельности. Деятельность персонала банка по выполнению мер безопасности.

Литература к теме 1: [1, 4]

Тема 2. Угрозы банка.

Содержание темы 2: Внешние и внутренние угрозы, их характеристика и тенденции развития. Банковское мошенничество и злоупотребления служебным положением работников банков. Мероприятия банка по защите от внешних и внутренних угроз.

Литература к теме 2: [1,2,4]

Тема 3. Недобросовестная конкуренция и промышленный шпионаж.

Содержание темы 3: Виды взаимоотношений, отражающих состояние отношений субъектов рынка в процессе их коммерческой деятельности. Определение понятия «конкуренция». Сущность недобросовестной конкуренции и промышленного шпионажа, их проявление в банках. Возможные способы привлечения к работе работников банка промышленными шпионами.

Литература к теме 3: [1, 4, 5]

Тема 4. Охрана и режим в банке.

Содержание темы 4: Оборудование и техническое обеспечение банков. Организация охраны учреждений банков. Режимы охраны

Литература к теме 4: [1, 2, 4]

Тема 5. Информационная безопасность банка.

Содержание темы 5: Неправомерное получение информации и защита от него. «Утечка» информации. Несанкционированный доступ к информации. Каналы утечки и передачи информации. Правовое регулирование защиты тайн банка

Литература к теме 5: [3, 4]

Тема 6. Экономическая безопасность банка.

Содержание темы 6: Защита материальных ценностей, оборудования и технических средств от противоправных действий. Обеспечение безопасности кредитных операций банков. Обеспечение безопасности работы банков на фондовом рынке. Обеспечение безопасности проведения в банках кассовых операций.

Обеспечение безопасности работы банков с пластиковыми платежными средствами. Обеспечение безопасности валютных операций банков. Борьба с легализацией (отмыванием) незаконно полученных средств. Литература к теме 6: [4, 5]

Тема 7. Информационно-аналитическое обеспечение деятельности банка.

Содержание темы 7: Понятие информационного ресурса. Коммерческая разведка: структура, цель, объекты, источники. Структура информационно-аналитической работы. Каналы получения информации.

Литература к теме 7: [1,2,3,4]

Тема 8. Обеспечение безопасности в работе с персоналом банка.

Содержание темы 8: Кадровая политика банка по подбору персонала. Психологическое тестирование. Соционика. Психология недобросовестного работника, клиента, мошенника. Конфликты, их предупреждения и решения.

Литература к теме 7: [1,2,4,5]

3.3. Практические (семинарские) занятия

[illegible]

3.4. Лабораторные работы

№ п/п	Тема работы	Объем, час.	Литера- тура
1	Создание и обработка элементарных таблиц Excel.	2	6
2	Ввод данных и корректировка информации в электронной таблице.	2	6
3	Экономические и математические расчеты с применением табличного редактора Excel.	2	6
4	Простейшее моделирование банковских помещений с соблюдением необходимых технических требований	4	4
5	Разработка типичной инструкции пропускного режима банковских учреждений.	2	1, 4
6	Разработка требований к помещениям охраны и службы безопасности	2	3, 4

7	Организация безопасности кредитных операций банка. Обеспечение безопасности работы банка с ценными бумагами. Защита интересов банка во время проведения кассовых операций.	2	4,5
Итого:		16	

3.5. Самостоятельная работа студента

№ п/п	Виды самостоятельной работы студента	Объем, час.
1	Изучение лекционного материала (не менее 50% от объема лекций)	34
2	Подготовка к практическим занятиям (не менее 50% от объема аудиторных практических занятий)	
3	Подготовка к лабораторным работам (не менее 50% от объема аудиторных лабораторных занятий)	33
4	Выполнение курсового проекта (36 часов)	
5	Выполнение курсовой работы (27 часов)	
6	Выполнение индивидуального задания (не менее 9 часов)	9
Итого:		76

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Текущий контроль знаний студентов производится по результатам выполнения лабораторных работ, во время контрольных опросов в ходе изучения дисциплины.

Промежуточная аттестация по результатам освоения дисциплины в семестре проводится в форме семестрового экзамена в соответствии с «Положением об организации и проведении семестрового контроля знаний студентов в Донецком национальном техническом университете», утвержденном 25.09.2013г. Для определения уровня знаний студентов преподаватель руководствуется критериями оценки знаний, являющимися составляющей учебно-методического комплекса дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Литература:

Основная:

1. Гамза, В.А. Безопасность банковской деятельности [Текст] : учебник / В.А. Гамза, И.Б. Ткачук. - М. : Маркет ДС, 2014.
2. Букин, С. О. Безопасность банковской деятельности: Учебное пособие / С. О. Букин — СПб.: Питер, 2011. — 288 с.: ил.
3. Зубок, М.И. Безопасность банковской деятельности : учебник / М. И. Зубок, С. М. Яременко. — К.: КНЕУ, 2012. — 477с.

Дополнительная:

4. Побережный, С.Н. Модели и методы обеспечения банковской безопасности / Монография / С.Н. Побережный, Б.А. Дадашев, А. Л. Пластун. — Сумы: ГВУЗ «УАБД НБУ», 2010. — 239с.

5. Продукты и технологии современного банковского бизнеса / Под ред. д.э.н., профессора Г.Н. Белоглазовой и д.э.н., профессора Н.П.Радковской.- СПб.: Изд-во СПбГЭУ, 2013. — 295с.

6. Волков В. Б. Понятный самоучитель Excel 2010. / В. Б. Волков— СПб.: Питер, 2010. — 256 с.: ил.

Internet-ресурсы

1. [http:// www.ib-bank.ru](http://www.ib-bank.ru).
2. <http://www.cbr>
3. <http://cbrb-dnr.ru>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

1. Лекционные занятия:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;

2. Практические занятия:

3. Лабораторные работы:

- Оборудование учебного кабинета:
- компьютеры с программным обеспечением.

Составитель рабочей программы: _____ Н. И. Ванда



(подпись)