

Министерство образования Республики Беларусь

Учреждение образования
"БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ
И РАДИОЭЛЕКТРОНИКИ"

УТВЕРЖДАЮ
Первый проректор
 С.К. Дик
« _____ » _____ 2018 г.



ПРОГРАММА

дополнительного экзамена по специальности
1-98 80 01 "Методы и системы защиты информации, информационная
безопасность"

Минск, 2018

Программа составлена на основании типовых учебных программ дисциплин:

«Основы защиты информации»

Регистрационный № ТД-1.013 от 27.02.2006г.

«Защита объектов связи от несанкционированного доступа»

Регистрационный № ТД-Р.210/тип.от 03 марта 2010 г.

«Защита информации в банковских технологиях»

Регистрационный № ТД-Р.333/тип.от 14.06.2011 г.

Специальности (ей) 98 01 02 «Защита информации в телекоммуникациях»

Форма экзамена: устный

Составители:

Борботько Т.В. – д.т.н., профессор, зав. кафедрой ЗИ

Лыньков Л.М. – д.т.н., профессор кафедры ЗИ

РЕКОМЕНДОВНА К УТВЕРЖДЕНИЮ

Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
(протокол № 16 от 21 марта 2018 г.)

Заведующий кафедрой ЗИ,
д.т.н., профессор



Т.В.Борботько

Раздел 1. Телекоммуникационные системы в банковском деле и электронном бизнесе

Тема 1.1. Электронная коммерция

Традиционная и электронная коммерция. Виды электронной коммерции. Мобильная коммерция. Технология EDI в системах B2B. Компоненты технологии EDI. Информационная безопасность электронной коммерции.

Тема 1.2. Деньги и платежные системы в электронной коммерции

Механизмы классических денег. Платежные средства. Типы дематериализованных денег. Электронные кошельки. Платежные системы. Угрозы безопасности электронных платежных систем.

Тема 1.3. Персональные платежи и их защита

Автоматические кассовые аппараты (АТМ), методы и средства их защиты. Обеспечение безопасности POS-систем. Персональный идентификатор (PIN). Системы видеоконтроля персональных платежей.

Тема 1.4. Международные платежные системы

Архитектура и обеспечение безопасности в системе SWIFT. Архитектура и обеспечение безопасности в системе CHAPS.

Раздел 2. Управление доступом в телекоммуникационных системах

Тема 2.1. Реализация политики безопасности в телекоммуникационных системах

Модели политики безопасности. Механизмы защиты. Принципы реализации политики безопасности. Механизмы поддержки политики безопасности в телекоммуникационных системах.

Тема 2.2. Организация контроля функционирования и защиты телекоммуникационных систем

Принципы реализации. Особенности защиты информации в автоматизированных банковских системах. Этапы построения защиты автоматизированных банковских систем. Административная группа управления защитой. Управление рисками.

Тема 2.3. Опасные события и их предупреждение

Источники получения информации об угрозах. Локализация угроз. Особенности использования внешнего ресурса.

Раздел 3. Противодействие угрозам безопасности в телекоммуникационных системах

Тема 3.1. Атаки в телекоммуникационных системах

Классификация атак. Сетевая разведка. Анализ сетевого трафика. Спуфинг. Атака man in the middle. Атака отказ в обслуживании (DoS). Атаки на уровне приложений. Парольные атаки. Бот-нет (зомби-сети).

Тема 3.2. Противодействие атакам в телекоммуникационных системах

Состав комплекса противодействия атакам. Системы обнаружения вторжений (IDS).honeypots. Сканеры уязвимостей. Способы обнаружения атак. Корреляция данных об атаках, получаемых из различных источников. Межсетевые экраны. Трансляция сетевых адресов (NAT). Противодействие спаму. Противодействие вредоносным программам. Виртуальные частные сети (VPN).

Тема 3.3. Безопасность платежей в Интернете

Обеспечение безопасности платежей в системах электронной коммерции. Информационная безопасность систем Интернет-банкинга. Информационная безопасность B2C систем. Информационная безопасность B2B систем. Fraud-мониторинг в системах электронных платежей. Протоколы для обеспечения безопасной передачи данных.

Литература

К разделу 1

1. 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.

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

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

4. 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. — Мн.: БГУИР, 2002. – 56 с.

К разделу 2

1. 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.

2. Лыньков Л.М., Голиков В.Ф., Борботько Т.В. Основы защиты информации и управление интеллектуальной собственностью. – Учебн. - метод. пособие. Минск: БГУИР, 2013. – 243 с.

3. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. - М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.