ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ

Цель программы — формирование у слушателей умений и навыков построения системы менеджмента/обеспечения информационной безопасности в банках и небанковских кредитно-финансовых организациях Республики Беларусь с учетом требований национального законодательства и международных стандартов в области защиты информации и обеспечения кибербезопасности.

Выпускники курса получают свидетельство о повышении квалификации в области технической защиты информации государственного образца.

Целевая аудитория:

- руководители и специалисты структурных подразделений, обеспечивающие информационную безопасность и/или кибербезопасность;
- руководители и специалисты структурных подразделений, ответственные за управление рисками информационной безопасности, киберрисками, ИТ-рисками;
- руководители и специалисты структурных подразделений, ответственные за проведение аудита информационной безопасности (ИТ-аудита);
- специалисты IT-подразделений, реализующие мероприятия по защите информации в банковском секторе.

Требуемая предварительная подготовка слушателей:

- общие представления об информационных системах, правовых, организационных и технических аспектах обеспечения информационной безопасности;
- навыки работы в ОС Windows и с офисными приложениями на уровне пользователя.

Форма обучения – очная (дневная).
Стоимость обучения одного слушателя – 990 рублей.

Обучение проводится по адресу: г. Минск, ул. К. Цеткин, 24, 11 этаж в соответствии с графиком учебного процесса.

Продолжительность программы – 36 академических часов.

Учебный план курса

№ п/п	Название тем курса
	Структуры и стандарты построения систем информационной безопасности на основании процессного подхода
1.	Основы процессного подхода в области информационной безопасности. ISO/IEC 2700x. COBIT. ITIL. CIS Critical Security Controls. NIST Special Publication
2.	Технические требования и правила информационной безопасности в банковской деятельности. PCI DSS
3.	Формализация и внедрение процессов управления и обеспечения информационной безопасностью
	Менеджмент риска информационной безопасности (киберриска)
4.	Международные стандарты менеджмента и оценки риска
5.	Постановление правления НБ РБ № 550. Интеграция управления киберриском в общую систему риск-менеджмента
	ТТП ИБ 4.1 – 2020. Менеджмент рисков информационной безопасности. Взаимодействие подразделений банка и распределение обязанностей по управлению киберриском
6.	Основные этапы менеджмента риска ИБ. Процесс менеджмента риска ИБ. Стресс-тестирование риска информационной безопасности (киберриска)
7.	Формат отчета об оценке рисков. Инструментальные средства оценки и анализа риска
8.	Оценка риска нарушения информационной безопасности
	Управление программой аудита информационной безопасности банка
9.	Международные стандарты проведения аудита информационной безопасности. Разработка программы аудита
10.	Сбор и анализ информации о киберугрозах и уязвимостях информационной инфраструктуры банка. Использование специальных инструментов для поиска информации об уязвимостях

11.	Алгоритм проведения аудита информационной безопасности и отчетность. Определение целей, области и критериев аудита. Планирование аудита. Подготовка рабочих документов. Наблюдения и свидетельства аудита
12.	Проведение аудита информационной безопасности
	Разработка (совершенствование) системы менеджмента информационной безопасности в банке (ТТП ИБ 2.1-2020)
13.	Организация функционирования службы информационной безопасности. Определение области действия системы обеспечения информационной безопасности. Разработка документации, регламентирующей вопросы обеспечения информационной безопасности (ТТП ИБ 6.1-2020)
14.	Определение подхода к оценке рисков информационной безопасности и проведение оценки и обработки рисков
15.	Планирование внедрения системы обеспечения информационной безопасности. Реализация программ по обучению и повышению осведомленности в области информационной безопасности. Организация обнаружения и реагирования на инциденты безопасности (ТТП ИБ 7.1-2020)
16.	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний. Мониторинг, анализ функционирования системы обеспечения информационной безопасности и контроль защитных мер. Оценка соответствия требованиям (ТТП ИБ 5.1-2020)
17.	Разработка и планирование внедрения процесса системы менеджмента информационной безопасности
	Защита информации в информационных системах банка
18.	Требования законодательства Республики Беларусь в области защиты информации, распространение и (или) предоставление которой ограничено
19.	Проектирование системы защиты информации информационных систем и ресурсов банка
20.	Создание (внедрение) системы защиты информации информационных систем и ресурсов банка
21.	Аттестация системы защиты информации информационных систем и ресурсов банка
22.	Эксплуатация и модернизация системы защиты информации информационных систем и ресурсов банка
23.	Проект разработки и внедрения системы защиты информации
	Обеспечение кибербезопасности на критически важных объектах информатизации
24.	Требования законодательства Республики Беларусь в области защиты информации, обрабатываемой на критически важных объектах информатизации
25.	Проектирование системы информационной безопасности критически важных объектов информатизации
26.	Создание системы информационной безопасности критически важных объектов информатизации
27.	Аудит системы информационной безопасности критически важных объектов информатизации
28.	Функционирование системы информационной безопасности критически важных объектов информатизации
29.	Проект разработки и внедрения системы информационной безопасности критически важного объекта информатизации