АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ИНСТИТУТ ЭКОНОМИКИ, СТРОИТЕЛЬСТВА, ПРИКЛАДНЫХ ФИНАНСОВ И ПРАВА»

УТВЕРЖДАЮ
Директор АНО ДПО
«Институт ЭСПФ»

к.ю.н, доцент
О.В.Цуканов
01 апреля 2026 г.

ПРОГРАММА

повышения квалификации
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА»

(16 часов)

Москва – 2026

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА»

Общая характеристика программы

1. Цель реализации программы

Цель:

Формирование у слушателей компетенций, необходимых для организации и обеспечения информационной безопасности бизнеса, предотвращения утечек информации, противодействия актуальным киберугрозам, выстраивания безопасных бизнес-процессов и повышения устойчивости организации к инцидентам информационной безопасности.

2. Требования к результатам обучения
Планируемые/ Проектируемые результаты обучения

В результате освоения программы слушатель должен приобрести знания и умения, необходимые для качественного изменения компетенций:

Знать:

- основные угрозы и уязвимости информационной безопасности бизнеса;
- основные нормативно-правовые и организационные требования в сфере защиты информации и обработки данных в организации;
- принципы обеспечения конфиденциальности, целостности и доступности информации в бизнес-среде;
- организационные, кадровые и технические ресурсы, необходимые для построения системы информационной безопасности бизнеса;
- примеры регламентирующих и стандартизирующих документов при обслуживании клиентов

Уметь:

- выявлять критичные информационные активы и определять основные риски их компрометации;
- подбирать организационные и технические меры защиты информации с учетом специфики деятельности организации;
- оценивать уязвимости бизнес-процессов и альтернативные способы минимизации киберрисков;
- анализировать уровень защищенности организации и предлагать меры по его повышению.

Владеть:

- навыками безопасной организации работы с корпоративной информацией и цифровыми ресурсами;
- способностью анализировать инциденты информационной безопасности и их влияние на деятельность организации;
- методами базовой оценки рисков и выработки профилактических мер по защите бизнеса.

3. Содержание программы

УЧЕБНЫЙ ПЛАН
программы повышения квалификации
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА»

Требования к уровню образования слушателей	лица, имеющие среднее профессиональное и (или) высшее образование (бакалавр, специалист, магистр), банковская сфера, страховые агенты, туристическая деятельность, а также иные слушатели с высшим или средним профессиональным образованием в сферах, связанных с обслуживанием клиентов.
Категория слушателей	руководители организаций и подразделений, специалисты по информационной безопасности и ИТ, сотрудники финансовых, кадровых, юридических, административных и операционных служб, а также иные специалисты, работающие с корпоративной информацией и цифровыми ресурсами.
Срок освоения программы	16 часов, 2 недели
Форма обучения	очно-заочная, с применением дистанционных образовательных технологий и электронного обучения
Режим занятий	4 часа в день

№ № п/п	Наименование дисциплины, модуля	Всего часов трудоемкости	В том числе				Форма контроля
			Контактная работа*			Самостоятельная работа*	
			Всего, часов	из них			
				Лекции	Практические занятия		
1	**Тема 1. Основы информационной безопасности бизнеса**	**4**		**2**		**2**	
2	**Тема 2. Основные угрозы, уязвимости и киберриски организации**	**4**		**2**		**2**	
3	**Тема 3. Нормативно-правовая база и комплаенс и организационные аспекты: люди, процессы, управление**	**4**		**2**		**2**	
4	**Тема 4. Реагирование на инциденты и обеспечение устойчивости бизнеса**	**2**				**2**	
5	**Тема5. Культура кибербезопасности и обучение персонала**	**2**				**2**	
6	**Всего:**	**16**		**6**		**10**	
7	**Общая трудоемкость программы:**	**16**					

* С применением электронного обучения и дистанционных образовательных технологий

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ИНСТИТУТ ЭКОНОМИКИ, СТРОИТЕЛЬСТВА, ПРИКЛАДНЫХ ФИНАНСОВ И ПРАВА»

Календарный учебный график
программы повышения квалификации
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА»

Срок освоения программы – 16 часов.
Продолжительность обучения – 2 недели
Форма обучения – очно-заочная, с применением дистанционных образовательных технологий

№ п\п	Наименование дисциплин (модулей), тем	1 неделя	2 неделя	КР	СР	С	ПА	ИА	Всего
1	**Тема 1. Основы информационной безопасности бизнеса** Понятие информационной безопасности бизнеса. Информационные активы организации и их значение для устойчивости деятельности. Базовые принципы защиты информации: конфиденциальность, целостность, доступность. Роль информационной безопасности в системе корпоративного управления и обеспечения непрерывности бизнес-процессов.	2							2

2	**Тема 2. Основные угрозы, уязвимости и киберриски организации** Классификация актуальных угроз информационной безопасности бизнеса. Внешние и внутренние угрозы: фишинг, вредоносное программное обеспечение, компрометация учетных данных, утечки данных, ошибки персонала, социальная инженерия. Основы выявления уязвимостей и оценки киберрисков.	2	2						4
3	**Тема 3. Нормативно-правовая база и комплаенс и организационные аспекты: люди, процессы, управление** Законодательство РФ в области ИБ для бизнеса. Стандарты и требования отраслевых регуляторов Международные стандарты и корпоративные политики. Построение Службы информационной безопасности (СИБ). Управление инцидентами (IRP). Создание SOC (Security Operations Center): in-house, outsource, MDR.	2	2						4
4	**Тема 4. Реагирование на инциденты и обеспечение устойчивости бизнеса** Подходы к выявлению, классификации и локализации инцидентов информационной безопасности. Порядок действий сотрудников при выявлении нарушений безопасности. Эскалация инцидентов, минимизация ущерба, восстановление процессов и обеспечение	2							2

	устойчивости бизнеса.								
5	**Тема 5. Культура кибербезопасности и обучение персонала** Формирование культуры кибербезопасности в организации. Повышение осведомленности персонала, профилактика социальной инженерии, обучение безопасной работе с корпоративными данными и цифровыми ресурсами. Внутренние коммуникации, контроль соблюдения правил и развитие ответственного поведения сотрудников.		2						2
6	Итоговая аттестация		2						2
7	Итого	8	8						16

Условные обозначения: КР – контактная работа; СР – самостоятельная работа; ПА – промежуточная аттестация; С – стажировка; ИА – итоговая аттестация, П- практика

4. Содержание тем

Тема 1. Основы информационной безопасности бизнеса

Понятие информационной безопасности бизнеса. Информационные активы организации и их значение для устойчивости деятельности. Базовые принципы защиты информации: конфиденциальность, целостность, доступность. Роль информационной безопасности в системе корпоративного управления и обеспечения непрерывности бизнес-процессов.

Тема 2. Основные угрозы, уязвимости и киберриски организации

Классификация актуальных угроз информационной безопасности бизнеса. Внешние и внутренние угрозы: фишинг, вредоносное программное обеспечение, компрометация учетных данных, утечки данных, ошибки персонала, социальная инженерия. Основы выявления уязвимостей и оценки киберрисков..

Тема 3. Нормативно-правовая база и комплаенс и организационные аспекты: люди, процессы, управление

Законодательство РФ в области ИБ для бизнеса.152-ФЗ «О персональных данных»: практика применения, штрафы, уведомления об утечках.187-ФЗ «О безопасности КИИ»: категорирование, создание ГосСОПКА, отчетность. 99-ФЗ (приказ №239) о лицензировании ГИС и ГИС. Стандарты и требования отраслевых регуляторов. ЦБ РФ (Положение 682-П, 716-П, СТО БР ИББС) для финансового сектора. Требования для операторов связи, ГИС, АСУ ТП. Международные стандарты и корпоративные политики. Внедрение ISO/IEC 27001. Построение СУИБ (системы управления информационной безопасностью) «под бизнес».

Построение Службы информационной безопасности (СИБ). Модели подчинения: CISO (директор по ИБ), функции, взаимодействие с IT, юристами, службой безопасности. KPI службы ИБ: как измерить эффективность, не мешая бизнесу. Управление инцидентами (IRP). Жизненный цикл инцидента: обнаружение, сдерживание, расследование, восстановление. Создание SOC (Security Operations Center): in-house, outsource, MDR. Коммуникации при утечке: раскрытие информации, работа с репутацией (PR в кризис). Управление доступом и идентификация. IGA (Identity Governance), PAM (Privileged Access Management). Внедрение безпарольной аутентификации и MFA как базовый стандарт.

Тема 4. Реагирование на инциденты и обеспечение устойчивости бизнеса

Подходы к выявлению, классификации и локализации инцидентов информационной безопасности. Порядок действий сотрудников при выявлении

нарушений безопасности. Эскалация инцидентов, минимизация ущерба, восстановление процессов и обеспечение устойчивости бизнеса.

Тема 5. Культура кибербезопасности и обучение персонала

Формирование культуры кибербезопасности в организации. Повышение осведомленности персонала, профилактика социальной инженерии, обучение безопасной работе с корпоративными данными и цифровыми ресурсами. Внутренние коммуникации, контроль соблюдения правил и развитие ответственного поведения сотрудников.

5. Материально-технические условия, необходимые для осуществления образовательного процесса

Наименование специализированных учебных помещений	**Вид занятий**	**Наименование оборудования, программного обеспечения**
Учебный интерактивный класс	Все виды контактной работы	Мультимедийное оборудование, компьютеры. Компьютер, подключенный к сети Интернет, интернет-браузер. Прикладные программы для просмотра текстовых и видеоматериалов.

Материально-технические условия соответствуют действующим санитарным и противопожарным правилам и нормам.

Примечание. *В случае проведения учебных занятий с применением электронного обучения (ЭО) и дистанционных образовательных технологий (ДОТ) у слушателя должен быть персональный компьютер, оснащенный аудиоколонками, с доступом в сеть интернет и установленным видеоплеером, способным воспроизводить видеофайлы.*

2. Перечень информационных технологий и учебно-методических условий, используемых при осуществлении образовательного процесса

При проведении занятий с применением ЭО и ДОТ проведение вебинаров для слушателей осуществляется в удаленном доступе. Преподавателями используются компьютерные презентации, работа в чате, индивидуальное консультирование слушателей.

Условия для функционирования электронной информационно-образовательной среды

Электронные информационные ресурсы	Вид занятий	Наименование оборудования, программного обеспечения

Система дистанционного обучения, система видеоконференцсвязи	Все виды контактной работы Промежуточная аттестация Итоговая аттестация	Компьютер, подключенный к сети Интернет; интернет-браузер; Прикладные программы для просмотра текстовых и видеоматериалов

6. Организация образовательного процесса

В образовательном процессе используются разнообразные формы работы со слушателями.

- лекция (видеолекция) с мультимедийным сопровождением по наиболее сложным вопросам программы;
- лекция-вебинар с использованием современных технических средств обучения;
- практические занятия и самостоятельная работа с использованием современных технических средств обучения;
- кейс-стади (в том числе видео-кейсы) – изучение конкретных ситуаций из практики информационной безопасности бизнеса (утечки данных, фишинговые атаки, компрометация учетных записей, ошибки персонала, инциденты удаленного доступа), для выполнения данного вида заданий обучающимся предоставляется описание реальной или моделируемой профессиональной ситуации и ставятся задачи по выявлению угроз, оценке рисков, анализу причин инцидента и выработке мер реагирования и профилактики;
- тестирование метод оценки знаний, умений, навыков обучающихся и др.

Обучение проводится, в том числе с использованием ЭО и ДОТ, реализуемых посредством информационно-телекоммуникационных сетей при опосредованном взаимодействии слушателей и педагогических работников.

В процессе обучения слушатели обеспечиваются необходимыми для эффективного прохождения обучения учебно-методическими материалами и информационными ресурсами в объеме изучаемого курса, которые могут быть объединены в учебно-методический комплекс. Материалы учебно-методического комплекса доводятся до всех слушателей курса.

Итоговая аттестация проводится на образовательном портале Финансового университета посредством информационно-телекоммуникационных сетей.

7. Кадровое обеспечение образовательного процесса

Учебный процесс со слушателями обеспечивают квалифицированные сотрудники института, а также приглашенные специалисты и действующие практики других организаций.

8. Оценка качества освоения программы

Оценка качества освоения программы осуществляется в виде прохождения итогового тестирования на основе системы зачет/незачет по всей программе.