Приложение №11

УТВЕРЖДЕНА
приказом АО «ГНИВЦ»
от _____ № ____

Образовательная программа повышения квалификации «Руководителю о безопасности предприятия»
(дистанционная форма обучения)

Москва, 2016 г.

Цель обучения: Повышение квалификации специалистов по информационной безопасности, руководителей и сотрудников служб безопасности предприятия (далее также – Слушатели, обучающиеся) по основным направлениям деятельности и компетенциям с учетом изменений в законодательстве, нормативных актах в целях совершенствования и (или) получения новой компетенции, необходимой для профессиональной деятельности, и (или) повышения профессионального уровня в рамках имеющейся квалификации.

Планируемые результаты обучения/ перечень профессиональных компетенций:

В результате освоения программы обучающийся должен знать:

- как мотивировать сотрудников службы безопасности
- как оценивать деятельность службы безопасности
- законодательство Российской Федерации в области корпоративной безопасности
- как определять внешние и внутренние угрозы для предприятия
- как оценивать защищенность организационной структуры бизнеса и основных бизнес-процессов

В результате освоения (программы) обучающийся должен уметь:

- построить систему защиты организации от внешних и внутренних угроз бизнеса
- выстраивать отношения с акционерами, владельцами, генеральным директором и иными директорами
- распределять полномочия и зоны ответственности между службой безопасностью и иными подразделениями предприятия
- получать сведения с сайта контрагента
- оценивать возможность кризисных ситуаций в деятельности компании на основе статистических методов

В результате освоения (программы) обучающийся должен иметь навыки:

- построения системы корпоративной безопасности
- разработки локально-правовых актов по обеспечению безопасности предприятия
- использования информационных ресурсов Интернета для задач конкурентной разведки
- применения на практике эмпирических законов
- прогнозирования надежности организаций на основе «растровых признаков опасности»
- применения элементов НЛП в процессе переговоров с должниками

Методика освоения программы:

Повышение квалификации специалистов по информационной безопасности, руководителей и сотрудников служб безопасности предприятия по образовательной программе «Руководителю о безопасности предприятия» проводится с использованием дистанционных образовательных технологий.

Обучение проводится в течении 5 (пяти) учебных дней.

Обучение проходит в форме лекционно-практических занятий по следующей схеме:

- лекции проводятся преподавателем (изложение нового материала, повторение пройденного: устный опрос), разбор ошибок, допущенных при решении практических задач и т.д);

- Слушатели самостоятельно выполняют лабораторные работы и иные практические задания.

В течение всего периода обучения в помощь Слушателям АО «ГНИВЦ» организует:

- «горячую линию» по технической и организационной поддержке процесса обучения;

- консультационную поддержку по организационным опросам, связанным с реализацией процесса обучения;

- консультационную поддержку Слушателей по вопросам освоения образовательной программы.

Организационно-педагогические условия

Слушатели, направленные на обучение, зачисляются на курсы повышения квалификации приказом Генерального директора АО «ГНИВЦ».

Повышение квалификации специалистов по информационной безопасности, руководителей, а также сотрудников служб безопасности предприятия осуществляется с использованием дистанционных телекоммуникационных и интернет-технологий.

Теоретическое обучение осуществляется:

Путем проведения лекционных занятий в форме вебинаров (не менее 60% объема лекционных занятий, установленного учебным планом образовательной программы, продолжительность каждого вебинара – не менее 2 (двух) учебных часов) по основным темам программы.

Перед началом занятий для настройки системы проводится пробный вебинар.

Технология вебинаров обеспечивает лекционную работу преподавателя со Слушателями в виртуальном классе.

Обеспечивается видеозапись всех вебинаров, а также:

- не позднее 6 часов после завершения вебинара - размещение на сайте АО «ГНИВЦ» видеозаписей вебинаров для просмотра Слушателями;

- не позднее 24 часов после завершения вебинара - размещение на сайте АО «ГНИВЦ» видеозаписей вебинаров для скачивания Слушателями.

Запись проведенных вебинаров доступна для скачивания Слушателями с сайта АО «ГНИВЦ» в течение всего периода обучения по образовательной программе.

Путем самостоятельного изучения Слушателями, дополнительно к вебинарам, учебных материалов учебно-методического комплекса и учебных материалов, размещенных на сайте АО «ГНИВЦ».

Практические занятия представлены лабораторными работами (практическими заданиями) и выполняются Слушателями. Лабораторные работы (практические задания) входят в состав учебно-методического комплекса.

В состав учебно-методического комплекса входит курс лекций в текстовом формате по всем темам учебного плана и практические материалы курса (практическое пособие) в текстовом формате, аудио- и видеоматериалы по отдельным темам учебного плана. Видеоматериалы имеют качество разрешения видео не ниже 640x480 пикселей (4:3), 640x360 пикселей (16:9) и могут быть воспроизведены на автоматизированных рабочих местах Слушателей, с аппаратно-техническими характеристиками согласно Приложению № 1.

Все предлагаемые текстовые и графические материалы открываются в среде продуктов Microsoft Office 2003.

Услуги «горячей линии» по технической и организационной поддержке процесса обучения, пользованию сервисами сайта АО «ГНИВЦ» и СДО ГНИВЦ оказываются АО «ГНИВЦ»:

- в период за 1 час до начала вебинаров, во время вебинаров и в течение 1 часа после окончания вебинаров, согласно расписанию вебинаров, а также в период проведения итогового тестирования - по телефону, электронной почте, в интернет-форуме и службе обмена мгновенными сообщениями через сеть «интернет». Время реагирования на запросы Слушателей не более 20 (двадцать) минут с момента обращения;

- в круглосуточном режиме - по адресу электронной почты и в интернет-форуме. При этом время реагирования на запросы Слушателей не более 24 (двадцати четырех) часов с момента обращения

Кроме того, консультационная поддержка по организационным вопросам, связанным с реализацией процесса обучения, осуществляется представителями ФГУП ГНИВЦФНС России, ответственными за организацию процесса обучения, по электронной почте или телефону, указанному на сайте АО «ГНИВЦ» (в рабочее время АО «ГНИВЦ»).

Консультационная поддержка Слушателей по вопросам освоения образовательной программы осуществляется АО «ГНИВЦ» по рабочим дням, в течение всего срока обучения по телефону, электронной почте, в интернет-форуме и службе обмена мгновенными сообщениями через сеть «интернет».

Время реагирования на запросы Слушателей по вопросам освоения образовательной программы не более 24 (двадцати четырех) часов с момента обращения.

Консультационная поддержка по вопросам освоения образовательной программы оказывается при участии преподавателей, подготовивших учебные и контрольные (тестовые) материалы по соответствующим дисциплинам (тематикам).

АО «ГНИВЦ» также могут проводиться дополнительные консультации преподавателей по дисциплинам (тематикам), входящим в образовательную программу. Информация о проведении таких консультаций будет публиковаться на сайте АО «ГНИВЦ» не позднее, чем за 1 (один) рабочий (учебный) день до проведения консультации.

Педагогический состав.

В штате Предприятия состоят сотрудники, совмещающие практическую работу и педагогическую деятельность.

Кроме того, для удовлетворения потребностей в квалифицированных специалистах Предприятие заключило соглашения о сотрудничестве с ведущими высшими учебными заведениями г. Москвы.

Форма и методика итоговой аттестации, оценочные материалы:

Опорными точками контроля участия Слушателя в процессе обучения по программе являются:

- участие в вебинаре;
- выполнение практических заданий;
- сдача итогового тестирования.

Освоение программы завершается итоговой аттестацией (экзаменом), которая направлена на определение теоретической и практической подготовленности обучающихся к выполнению профессиональных задач.

Приказом Генерального директора АО «ГНИВЦ» формируется аттестационная комиссия по программе повышения квалификации «Управление проектами в области информационных технологий», в состав которой входят руководство АО «ГНИВЦ», ведущие специалисты Центра организации и координации учебно-методической работы.

Регистрация Слушателей в СДО ГНИВЦ осуществляется куратором группы в начале обучения. Каждому Слушателю предоставляются персональные логин и пароль для входа в СДО ГНИВЦ по электронной почте, указанной в заявке.

К итоговой аттестации (экзамену) допускаются слушатели, не имеющие задолженности и в полном объеме выполнившие программу повышения квалификации «Руководителю о безопасности предприятия».

Слушатели сдают экзамен (проходят итоговую аттестацию) в форме электронного итогового тестирования в СДО ГНИВЦ.

Сеанс сдачи итогового теста назначается в последний день обучения.

Для сдачи итогового теста Слушателю отводится 40 минут (20 вопросов по 2 минуты времени на каждый). Вопросы выбираются случайным образом из общей базы вопросов объемом не менее 40 вопросов. Вопросы равномерно распределены по всем темам программы обучения. При сдаче итогового теста каждый Слушатель имеет право на 3 попытки.

Результаты тестирования фиксируются в базе данных СДО ГНИВЦ и не могут быть подвергнуты корректировке участниками процесса обучения и тестирования. Лучший результат тестирования считается результатом итоговой аттестации Слушателя.

Тест признается успешно сданным, если количество правильных ответов превышает определенный порог (70%).

Методические материалы:

- Учебно-методический комплекс, включающий:
  - учебный план;

- учебно-тематический план;
- рабочую программу;
- курс лекций в текстовом формате по всем темам учебного плана;
- аудио-, видеоматериалы по темам учебного плана;
- практические материалы курса (практическое пособие);
- тестовые материалы для контроля качества усвоения материала;
- методические рекомендации по освоению образовательной программы с описанием и указанием последовательности её изучения (календарный график освоения образовательной программы);
- рекомендации для Слушателей по порядку работы с сайтом АО «ГНИВЦ» и обучающими ресурсами (вебинарами, сервисами для организации и проведения обучения, электронными учебниками и пр.);
- методические рекомендации по организации самоконтроля и текущего контроля, методика проверки (контроля) практических занятий, методика итоговой аттестации;

➢ расписание вебинаров;
➢ технические рекомендации для слушателей на выполнение настроек рабочего места
➢ информация о службе «горячей линии» по технической и организационной и консультационной поддержке дистанционного обучения (ФИО, телефон, адрес электронной почты, адрес интернет-форума и контакты службы обмена мгновенными сообщениями в информационно-телекоммуникационной сети «Интернет»;

Данные материалы размещаются на сайте АО «ГНИВЦ» и доступны для скачивания и распечатывания Слушателями круглосуточно за 2 дня до начала обучения и до окончания обучения.

Литература представлена в Рабочей программе.

УЧЕБНЫЙ ПЛАН

Руководителю о безопасности предприятия

(наименование программы повышения квалификации)

Цель:	Повышение квалификации специалистов по информационной безопасности, руководителей и сотрудников служб безопасности предприятия (далее также – Слушатели, обучающиеся) по основным направлениям деятельности и компетенциям с учетом изменений в законодательстве, нормативных актах в целях совершенствования и (или) получения новой компетенции, необходимой для профессиональной деятельности, и (или) повышения профессионального уровня в рамках имеющейся квалификации.
Категория, группа должностей	Директора предприятий, руководители подразделений и бизнес-единиц; заместители руководителей предприятий по безопасности, директора по безопасности; руководители и сотрудники служб безопасности предприятия; специалисты по экономической безопасности; специалисты по информационной безопасности; сотрудники подразделений внутреннего контроля и аудита; специалисты по HR безопасности; корпоративные юристы
Продолжительность обучения:	40 часов
Форма обучения:	С использованием дистанционных образовательных технологий
Режим занятий:	8 часов в день

№ п/п	Наименование разделов и дисциплин	Количество часов			Формы аттестации и контроля знаний
		всего	по видам занятий		
			лекции	практические занятия	
1.	**Политика экономической безопасности. Определение экономических рисков и построение корпоративной защиты**	**8**	**8**	**-**	**Контрольные вопросы**
2.	**Конкурентная разведка. Анализ надежности компаний и безопасности коммерческих предложений.**	**8**	**2**	**6**	**Контрольные вопросы/ Практические задания в виде кейса**
3.	**Внешнее мошенничество. Управление дебиторской задолженностью. Защита от рейдерства**	**8**	**4**	**4**	**Контрольные вопросы/ Практические задания в виде кейса**
4.	**Политика кадровой безопасности. Проведение внутренних проверок и финансовых расследований (форензик)**	**6**	**3**	**3**	**Контрольные вопросы/ Практические задания в виде кейса**
5.	**Политика информационной безопасности. Создание режима коммерческой тайны. Защита персональных данных своими силами**	**8**	**2**	**6**	**Контрольные вопросы/ Практические задания в виде кейса**
6.	**Подготовка и проведение итоговой аттестации.**	**2**	**-**	**2**	**Экзамен в форме тестирования**

	Итого:	**40**	**19**	**21**	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

Руководителю о безопасности предприятия

(наименование программы повышения квалификации)

Базовое образование:	Высшее
Продолжительность программы:	40 часов
Форма контроля:	Электронное итоговое тестирование, проверка выполнения практических заданий и лабораторных работ, контрольные вопросы по темам
По окончании выдается:	Удостоверение о повышении квалификации установленного образца или Справка об обучении по программе повышения квалификации

№ п/п	Наименование разделов и дисциплин	Количество часов			Формы аттестации и контроля знаний
		всего	по видам занятий		
			лекции	практические занятия	
1.	**Политика экономической безопасности. Определение экономических рисков и построение корпоративной защиты**	**8**	**8**	**-**	**Контрольные вопросы**
1.1.	международные акты в сфере безопасности бизнеса. Законодательство Российской Федерации в области корпоративной безопасности. Ведомственные и отраслевые требования и стандарты в области защиты бизнеса	1	1	-	х
1.2.	международный опыт и корпоративные стандарты по защите компаний от экономических преступлений. Международные акты по борьбе с мошенничеством	1	1	-	х
1.3.	понятие безопасность в российском бизнесе. Постановочные вопросы перед созданием системы защиты бизнеса. Определение объектов защиты. Построение системы корпоративной безопасности	1	1	-	х
1.4	особенность обеспечения корпоративной безопасности в представительствах иностранных компаний, действующих на территории России, в холдингах, в дочерних компаниях, в компаниях, имеющих сложную организационную (терри-	0,5	0,5	-	х

	ториально разделенную) структуру				
1.5	корпоративная безопасность как элемент риск-менеджмента. Определение внешних и внутренних угроз для предприятия. Составление карты экономических рисков. Участие «безопасника» в управлении рисками на предприятии	0,5	0,5	-	х
1.6	методика проведения аудита безопасности предприятия. Составление плана аудита на основе карты экономических рисков и формирования моделей угроз. Определение видов экономических рисков и вероятности их наступления. Оценка защищенности организационной структуры бизнеса и основных бизнес процессов	0,5	0,5	-	х
1.7	экспертные системы оценки защищенности предприятия. Оценка возможности защиты предприятия от внештатных ситуаций. Создание кризисных планов. Наличие мониторинга безопасности предприятия	0,5	0,5	-	х
1.8	определение субъектов корпоративной безопасности. Своя служба безопасности (СБ) или аутсорсинговое обслуживание. Плюсы и минусы обоих вариантов. Распределение полномочий и зон ответственности между СБ и иными подразделениями предприятия	1	1	-	х
1.9	юридические тонкости договорных отношений с аутсорсинговыми организациями, предлагающими услуги по защите бизнеса. Правовое обеспечение взаимодействия с частными охранными организациями и субъектами детективной деятельности	0,5	0,5	-	х

1.10	правовая сторона деятельности СБ. Закон и этика в работе. Подчинение, финансирование и оценка эффективности работы СБ. Взаимодействие с акционерами, владельцами и руководителями. Начальник СБ. Какие требования к нему предъявлять, какими чертами характера и профессиональными качествами он должен обладать. Какой образовательный уровень и опыт в прошлой жизни	0,5	0,5	-	х
1.11	корпоративные стандарты безопасности предприятия (КСБ). Совместимость КСБ с иными стандартами, действующими на предприятии. Включение процесс защиты бизнеса в процесс менеджмента непрерывности бизнеса	0,5	0,5	-	х
1.12	разработка локальных актов по обеспечению безопасности предприятия (концепция безопасности, политики, инструкции, регламенты и т.д.). Создание сводов правил и поведений сотрудников	0,5	0,5	-	х
2.	**Конкурентная разведка. Анализ надежности компаний и безопасности коммерческих предложений.**	**8**	**2**	**6**	**Контрольные вопросы/ Практические задания в виде кейса**
2.1	основные задачи конкурентной разведки	1	-	1	Практические задания в виде кейса
2.2	способы сбора информации	1	-	1	Практические задания в виде кейса
2.3	получение официальной информации из государственных органов и регистрационных организаций	1	1	-	Контрольные вопросы
2.4	получение неофициальной информации	0,5	-	0,5	Практические задания в виде кейса
2.5	международные информационные ресурсы для сбора и анализа информации по контрагенту	0,5	-	0,5	Практические задания в виде кейса
2.6	сбор сведений оперативными методами	0,5	-	0,5	Практические задания в виде кейса
2.7	методы анализа информации	0,5	-	0,5	Практические

					задания в виде кейса
2.8	алгоритм определения надежности контрагентов – юридических и физических лиц	0,5	-	0,5	Практические задания в виде кейса
2.9	оценка контрагента с позиции налоговых рисков	1	-	1	Практические задания в виде кейса
2.10	анализ учредительных документов организации с позиции безопасности	0,5	-	0,5	Практические задания в виде кейса
2.11	типы компаний, преследующие противоправные цели	1	1	-	Контрольные вопросы
3.	**Внешнее мошенничество. Управление дебиторской задолженностью. Защита от рейдерства**	**8**	**4**	**4**	**Контрольные вопросы/ Практические задания в виде кейса**
3.1	общая характеристика и виды преступлений против собственности	1	1	-	Контрольные вопросы
3.2	мошенники и их мотивация, психологические приемы, применяемые мошенниками	1	1	-	Контрольные вопросы
3.3	типы компаний, преследующие мошеннические цели.	1	1	-	Контрольные вопросы
3.4	создание на предприятии системы предупреждения и защиты от мошеннических операций	1	1	-	Контрольные вопросы
3.5	причины образования дебиторской задолженности	1	-	1	Практические задания в виде кейса
3.6	формирование комплекса мер по минимизации угроз, связанных с дебиторской задолженностью.	1	-	1	Практические задания в виде кейса
3.7	коллекторская деятельность.	0,5	-	0,5	Практические задания в виде кейса
3.8	порядок взаимоотношений между подразделениями на предприятии по взысканию задолженности	0,5	-	0,5	Практические задания в виде кейса
3.9	проведение переговоров с должниками	1	-	1	Практические задания в виде кейса
4.	**Политика кадровой безопасности. Проведение внутренних проверок и финансовых расследований (форензик)**	**6**	**3**	**3**	**Контрольные вопросы/ Практические задания в виде кейса**
4.1.	виды угроз, исходящих от сотрудников предприятия, варианты их реализации и возможные направления защиты	1	-	1	Практические задания в виде кейса

4.2.	проверка персонала при приеме на работу	1	-	1	Практические задания в виде кейса
4.3.	комплаенс-контроль сотрудников, занимающих должности с коррупционными (мошенническими) рисками.	1	-	1	Практические задания в виде кейса
4.4	особенность проведения внутрикорпоративного расследования (проверки) по наиболее характерным противоправным действиям сотрудников	1	1	-	Контрольные вопросы
4.5	использование полиграфа (детектора лжи) при проведении внутрикорпоративных расследований (проверок).	0,5	0,5	-	Контрольные вопросы
4.6	документальное оформление результатов внутрикорпоративного расследования (проверки	0,5	0,5	-	Контрольные вопросы
4.7	процедуры увольнения сотрудников с позиции безопасности	1	1	-	Контрольные вопросы
5.	**Политика информационной безопасности. Создание режима коммерческой тайны. Защита персональных данных своими силами**	**8**	**2**	**6**	**Контрольные вопросы/ Практические задания в виде кейса**
5.1	законодательство Российской Федерации в области защиты информации.	1	1	-	Контрольные вопросы
5.2	служба информационной безопасности (СИБ) на предприятии. Разделение функций между СИБ, СБ и ИТ-подразделением.	1	1	-	Контрольные вопросы
5.3	основные направления защиты конфиденциальной информации.	1	-	1	Практические задания в виде кейса
5.4	правовые, организационные, режимные и инженерно-технические мероприятия по защите конфиденциальной информации.	1	-	1	Практические задания в виде кейса
5.5	ИТ мероприятия по защите	1	-	1	Практические

	конфиденциальной информации.				задания в виде кейса
5.6	виды юридической ответственности за разглашение коммерческой тайны,	1	-	1	Практические задания в виде кейса
5.7	организационные, правовые и технические требования по обработке персональных данных	1	-	1	Практические задания в виде кейса
5.8	особенности обработки персональных данных, осуществляемой в информационных системах персональных данных.	1	-	1	Практические задания в виде кейса
6.	**Подготовка и проведение итоговой аттестации.**	**2**	**-**	**2**	**Экзамен в форме тестирования**
	Итого:	**40**	**19**	**21**	

РАБОЧАЯ ПРОГРАММА

Руководителю о безопасности предприятия

(наименование учебной (учебных) предметов, дисциплин (модулей))

Введение: Образовательная программа повышения квалификации «Руководителю о безопасности предприятия» подготовлена для совершенствования компетенций, необходимых для качественной профессиональной деятельности, повышения квалификации с целью профессионального роста, обеспечения соответствия их квалификации, понимания слушателями законных действий со стороны бухгалтера (руководителя, учредителя), направленных на защиту бизнеса от внешних и внутренних угроз, а также минимизации личной ответственности в случаях конфликтов внутри организации.

Перечень тем:

№ п/п	Наименование тем	Количество часов
1.	**Политика экономической безопасности. Определение экономических рисков и построение корпоративной защиты**	**8**
1.1.	международные акты в сфере безопасности бизнеса. Законодательство Российской Федерации в области корпоративной безопасности. Ведомственные и отраслевые требования и стандарты в области защиты бизнеса	1
1.2.	международный опыт и корпоративные стандарты по защите компаний от экономических преступлений. Международные акты по борьбе с мошенничеством	1
1.3.	понятие безопасность в российском бизнесе. Постановочные вопросы перед созданием системы защиты бизнеса. Определение объектов защиты. Построение системы корпоративной безопасности	1
1.4	особенность обеспечения корпоративной безопасности в представительствах иностранных компаний, действующих на территории России, в холдингах, в дочерних компаниях, в компаниях, имеющих сложную организационную (территориально разделенную) структуру	0,5
1.5	корпоративная безопасность как элемент риск-менеджмента. Определение внешних и внутренних угроз для предприятия. Составление карты экономических рисков. Участие «безопасника» в управлении рисками на предприятии	0,5
1.6	методика проведения аудита безопасности предприятия. Составление плана аудита на основе карты экономических рисков и формирования моделей угроз. Определение видов экономических рисков и вероятности их наступления. Оценка защищенности организационной структуры бизнеса и основных бизнес процессов	0,5
1.7	экспертные системы оценки защищенности предприятия. Оценка возможности защиты предприятия от внештатных ситуаций. Создание кризисных планов. Наличие монито-	0,5

	ринга безопасности предприятия	
1.8	определение субъектов корпоративной безопасности. Своя служба безопасности (СБ) или аутсорсинговое обслуживание. Плюсы и минусы обоих вариантов. Распределение полномочий и зон ответственности между СБ и иными подразделениями предприятия	1
1.9	юридические тонкости договорных отношений с аутсорсинговыми организациями, предлагающими услуги по защите бизнеса. Правовое обеспечение взаимодействия с частными охранными организациями и субъектами детективной деятельности	0,5
1.10	правовая сторона деятельности СБ. Закон и этика в работе. Подчинение, финансирование и оценка эффективности работы СБ. Взаимодействие с акционерами, владельцами и руководителями. Начальник СБ. Какие требования к нему предъявлять, какими чертами характера и профессиональными качествами он должен обладать. Какой образовательный уровень и опыт в прошлой жизни	0,5
1.11	корпоративные стандарты безопасности предприятия (КСБ). Совместимость КСБ с иными стандартами, действующими на предприятии. Включение процесс защиты бизнеса в процесс менеджмента непрерывности бизнеса	0,5
1.12	разработка локальных актов по обеспечению безопасности предприятия (концепция безопасности, политики, инструкции, регламенты и т.д.). Создание сводов правил и поведений сотрудников	0,5
2.	**Конкурентная разведка. Анализ надежности компаний и безопасности коммерческих предложений.**	**8**
2.1	основные задачи конкурентной разведки	1
2.2	способы сбора информации	1
2.3	получение официальной информации из государственных органов и регистрационных организаций	1
2.4	получение неофициальной информации	0,5
2.5	международные информационные ресурсы для сбора и анализа информации по контрагенту	0,5
2.6	сбор сведений оперативными методами	0,5
2.7	методы анализа информации	0,5
2.8	алгоритм определения надежности контрагентов – юридических и физических лиц	0,5
2.9	оценка контрагента с позиции налоговых рисков	1
2.10	анализ учредительных документов организации с позиции безопасности	0,5
2.11	типы компаний, преследующие противоправные цели	1
3.	**Внешнее мошенничество. Управление дебиторской задолженностью. Защита от рейдерства**	**8**
3.1	общая характеристика и виды преступлений против собственности	1
3.2	мошенники и их мотивация, психологические приемы, применяемые мошенниками	1
3.3	типы компаний, преследующие мошеннические цели.	1

3.4	создание на предприятии системы предупреждения и защиты от мошеннических операций	1
3.5	причины образования дебиторской задолженности	1
3.6	формирование комплекса мер по минимизации угроз, связанных с дебиторской задолженностью.	1
3.7	коллекторская деятельность.	0,5
3.8	порядок взаимоотношений между подразделениями на предприятии по взысканию задолженности	0,5
3.9	проведение переговоров с должниками	1
4.	**Политика кадровой безопасности. Проведение внутренних проверок и финансовых расследований (форензик)**	**6**
4.1.	виды угроз, исходящих от сотрудников предприятия, варианты их реализации и возможные направления защиты	1
4.2.	проверка персонала при приеме на работу	1
4.3.	комплаенс-контроль сотрудников, занимающих должности с коррупционными (мошенническими) рисками.	1
4.4	особенность проведения внутрикорпоративного расследования (проверки) по наиболее характерным противоправным действиям сотрудников	1
4.5	использование полиграфа (детектора лжи) при проведении внутрикорпоративных расследований (проверок).	0,5
4.6	документальное оформление результатов внутрикорпоративного расследования (проверки	0,5
4.7	процедуры увольнения сотрудников с позиции безопасности	1
5.	**Политика информационной безопасности. Создание режима коммерческой тайны. Защита персональных данных своими силами**	**8**
5.1	законодательство Российской Федерации в области защиты информации.	1
5.2	служба информационной безопасности (СИБ) на предприятии. Разделение функций между СИБ, СБ и ИТ-подразделением.	1
5.3	основные направления защиты конфиденциальной информации.	1
5.4	правовые, организационные, режимные и инженерно-технические мероприятия по защите конфиденциальной информации.	1
5.5	ИТ мероприятия по защите конфиденциальной информации.	1
5.6	виды юридической ответственности за разглашение ком-	1

	мерческой тайны,	
5.7	организационные, правовые и технические требования по обработке персональных данных	1
5.8	особенности обработки персональных данных, осуществляемой в информационных системах персональных данных.	1
6.	**Подготовка и проведение итоговой аттестации.**	**2**

Реферативное описание тем:

1. Политика экономической безопасности. Определение экономических рисков и построение корпоративной защиты

- международные акты в сфере безопасности бизнеса. Законодательство Российской Федерации в области корпоративной безопасности. Ведомственные и отраслевые требования и стандарты в области защиты бизнеса;
- международный опыт и корпоративные стандарты по защите компаний от экономических преступлений. Международные акты по борьбе с мошенничеством (UK Bribery Act, Foreign Corrupt Practices Act, Закон Сарбейнза — Оксли);
- понятие безопасность в российском бизнесе. Постановочные вопросы перед созданием системы защиты бизнеса. Определение объектов защиты. Построение системы корпоративной безопасности;
- особенность обеспечения корпоративной безопасности в представительствах иностранных компаний, действующих на территории России, в холдингах, в дочерних компаниях, в компаниях, имеющих сложную организационную (территориально разделенную) структуру;
- корпоративная безопасность как элемент риск-менеджмента. Определение внешних и внутренних угроз для предприятия. Составление карты экономических рисков. Участие «безопасника» в управлении рисками на предприятии;
- методика проведения аудита безопасности предприятия. Составление плана аудита на основе карты экономических рисков и формирования моделей угроз. Определение видов экономических рисков и вероятности их наступления. Оценка защищенности организационной структуры бизнеса и основных бизнес процессов;
- экспертные системы оценки защищенности предприятия. Оценка возможности защиты предприятия от внештатных ситуаций. Создание кризисных планов. Наличие мониторинга безопасности предприятия;
- определение субъектов корпоративной безопасности. Своя служба безопасности (СБ) или аутсорсинговое обслуживание. Плюсы и минусы обоих вариантов. Распределение полномочий и зон ответственности между СБ и иными подразделениями предприятия;
- юридические тонкости договорных отношений с аутсорсинговыми организациями, предлагающими услуги по защите бизнеса. Правовое обеспечение взаимодействия с частными охранными организациями и субъектами детективной деятельности;
- правовая сторона деятельности СБ. Закон и этика в работе. Подчинение, финансирование и оценка эффективности работы СБ. Взаимодействие с акционерами, владельцами и руководителями. Начальник СБ. Какие требования к нему предъявлять, какими чертами

характера и профессиональными качествами он должен обладать. Какой образовательный уровень и опыт в прошлой жизни;

- корпоративные стандарты безопасности предприятия (КСБ). Совместимость КСБ с иными стандартами, действующими на предприятии. Включение процесс защиты бизнеса в процесс менеджмента непрерывности бизнеса;
- разработка локальных актов по обеспечению безопасности предприятия (концепция безопасности, политики, инструкции, регламенты и т.д.). Создание сводов правил и поведений сотрудников;

2. Конкурентная разведка. Анализ надежности компаний и безопасности коммерческих предложений.

- основные задачи конкурентной разведки. Законодательство Российской Федерации об информации, информационных технологиях и защите информации. Констиуционное право на сбор информации любыми законными способами. Аутсорсинг информационно-аналитических услуг. Получение сведений из средств массовой информации. Особенности получение информации из детективных агентств;
- способы сбора информации. Систематизация работы по сбору информации о контрагенте. Информация, представляемая самим контрагентом. Получение информации с сайта контрагента;
- получение официальной информации из государственных органов и регистрационных организаций. Обзор официальных сайтов государственных органов и представленных на них информационных ресурсов. Использование программных комплексов для сбора и анализа информации (СПАРК, Интегрум и т.д.);
- получение неофициальной информации. Серые базы данных. Специализированные ресурсы по отраслям бизнеса и территориям. Использование информационных ресурсов Интернета для задач конкурентной разведки. Работа в чатах, блогах, живых журналах и иных информационных массивах. Работа с невидимой частью Интернета (интернет разведка);
- международные информационные ресурсы для сбора и анализа информации по контрагенту. Сбор информации по оффшорам. Способы вычисление конечного бенефициара;
- сбор сведений оперативными методами. Беседы с сотрудниками и иные способы получение информации, используя «человеческий фактор». Мотивация человека на передачу (разглашение) информации. Визуальное наблюдение, осмотр помещений и местности.
- методы анализа информации. Обзор автоматизированных информационных систем (АИС), применяемых на предприятиях. Что может и для чего используются АИС. Применение АИС для финансового анализа компании. Формирование корпоративных баз данных;
- алгоритм определения надежности контрагентов – юридических и физических лиц. Формирование матрицы проверки организации в зависимости от суммы сделки, предоплате и иных условий. Применение метода Due Diligence при оценке компании;
- оценка контрагента с позиции налоговых рисков. Понятие «должная осмотрительность» при взаимоотношениях с контрагентами. Коррупционные риски. Угроза конфликта интересов и аффилированности сотрудников с представителями контрагента;
- анализ учредительных документов организации с позиции безопасности. Анализ атрибутов и фирменного стиля. Оценка возможности кризисных ситуаций в деятельности компании на основе статистических методов. Применение на практике эмпирических законов;
- типы компаний, преследующие противоправные цели. Прогнозирование надежности организаций на основе «растровых признаков опасности». Формирование рейтингов надежности партнеров;
- анализ безопасности коммерческих предложений и договоров. Изучение инициаторов проекта, их интересы и деловую репутацию. Верификация представителей. Изучение механизма получения прибыли. Анализ первого контакта. Поведенческие аспекты при выявлении ненадежного партнера.

3. Внешнее мошенничество. Управление дебиторской задолженностью. Защита от рейдерства

- общая характеристика и виды преступлений против собственности. Понятие и признаки мошенничества. Отличие мошенничества от иных видов преступлений против собственности. Новое в законодательстве РФ в части ответственности за мошенничество;
- мошенники и их мотивация, психологические приемы, применяемые мошенниками. Структура мошеннической операции. Формы мошенничества в различных видах бизнеса. Некоторые сценарии проведения мошеннических операций;
- типы компаний, преследующие мошеннические цели. Прогнозирование надежности организации на основе «растровых признаков опасности». Формирование рейтингов надежности партнеров;
- создание на предприятии системы предупреждения и защиты от мошеннических операций.
- причины образования дебиторской задолженности. Типы компаний – должников, их мотивация, способы работы с каждым из них. Особенности работы с организациями, находящимися в стадии банкротства;
- формирование комплекса мер по минимизации угроз, связанных с дебиторской задолженностью. Перечень превентивных мер по недопущению дебиторской задолженности. Организация проведения договорной работы. Мониторинг неплатежей и финансовых рисков в договорной работе. Основные способы возврата долга, плюсы и минусы каждого из них. Переуступка долга;
- коллекторская деятельность. Правовая основа деятельности коллекторских агентств. Особенности досудебного урегулирования конфликтов. Обзор международных и российских коллекторских агентств. Понятие антиколлектор. Обвинение в вымогательстве, как метод работы антиколлекторских агентств;
- медиация, как вид посреднических услуг по досудебному решению вопросов взыскания долга. Правовая основа деятельности медиаторов. Некоторые особенности работы с медиаторами;
- порядок взаимоотношений между подразделениями на предприятии по взысканию задолженности. Судебные иски, арбитражное судебное производство и работа судебных приставов по взысканию дебиторской задолженности. Взаимоотношения с государственными правоохранительными органами;
- проведение переговоров с должниками. Психологические приемы, применяемы в процессе переговоров с должниками. Применение элементов НЛП в процессе переговоров с должниками;
- имиджевые приемы воздействия, применяемые при работе с должниками. Законные способы формирования отрицательного имиджа компании-должника. Некоторые приемы черного PR, применяемые на практике. Реестры ненадежных партнеров, существующие в Интернете.
- определение рейдерства (враждебного поглощения) в законодательстве РФ. Виды рейдерства. Внутреннее и внешнее враждебное поглощение. Цели (причины, мотивы) рейдерства. Типы организаций, наиболее подверженных возможному рейдерскому захвату;
- типы и стратегии деятельности компаний – агрессоров и их возможности. Сценарии рейдерских захватов. Белые, серые и черные схемы враждебного поглощения;
- классификация превентивных мер по защите от враждебного поглощения Создание организационно защищенной структуры бизнеса. Организация охранных мероприятий. Защита реестра акционеров. Применение технологий «отравленных пилюль» и «золотых парашютов» в трудовых отношениях;
- защита предприятия от начавшегося враждебного поглощения. Признаки начавшегося враждебного поглощения. Правовые и организационные способы защиты. Защита бухгалтерских и иных документов на предприятии. Ведение информационной войны с компанией – агрессором. Судебная защита;
- гринмейл или корпоративный шантаж. Что это такое? Сценарии действий гринмейлера. Права гринмейлера в зависимости от количества принадлежащих ему акций.

4. Политика кадровой безопасности. Проведение внутренних проверок и финансовых расследований (форензик)

- виды угроз, исходящих от сотрудников предприятия, варианты их реализации и возможные направления защиты. Противоправные действия сотрудников, ответственность за которые предусмотрена УК РФ, КОАП, ТК РФ и основные способы защиты от них;
- проверка персонала при приеме на работу. Какая информация собирается о кандидате. Сбор и анализ информации о физическом лице по методу SMICE. Порядок анализа резюме. На что обращать внимание при изучении трудовой книжки, дипломов, характеристик и иных официальных документов. Анкеты для кандидатов на работу;
- «растровые признаки опасности» у кандидата на работу. На что обратить внимание в «проверочных мероприятиях». Формирование модели потенциального правонарушителя, применительно к различным должностям;
- формирование корпоративного кодекса поведения сотрудников. Создание стимулов и мотивационных факторов, направленных на усиление лояльности сотрудников;
- «оперативная психология». Анализ личности человека и формирование моделей его поведения. Методы выявления лжи в процессе коммуникаций (профайлинг). Анализ языка тела. Манипуляции в общении и технологии убеждения.
- комплаенс-контроль сотрудников, занимающих должности с коррупционными (мошенническими) рисками. Анализ полномочий и результатов работы сотрудника в организации. Политика кадровой безопасности по минимизации комплаенс-рисков;
- система внутренних проверок (Internal Investigation), финансовых расследований и иные комплаенс процедуры. Методики проведения Forensic accounting (форензик). Вычисление фрода и иных мошеннических сделок. Обеспечение достоверности отчетности организации;
- особенность проведения внутрикорпоративного расследования (проверки) по наиболее характерным противоправным действиям сотрудников (хищение, коммерческий подкуп, мошенничество, разглашение информации, увод клиентов и т.д.);
- использование полиграфа (детектора лжи) при проведении внутрикорпоративных расследований (проверок). Контактный или бесконтактный полиграф, что лучше? Правовая и организационная сторона вопроса. Возможно ли обмануть полиграф?;
- документальное оформление результатов внутрикорпоративного расследования (проверки). Возможность использования результатов в качестве доказательства вины сотрудника;
- процедуры увольнения сотрудников с позиции безопасности. Как лучше расстаться с «нехорошими людьми». Правила проведения индивидуальных бесед с увольняющимися сотрудниками. Имиджевые и репутационные аспекты воздействия на увольняющегося сотрудника. Алгоритм передачи «дел и должности». Что сделать, чтобы увольняющийся сотрудник не увел клиентов.

5. Политика информационной безопасности. Создание режима коммерческой тайны. Защита персональных данных своими силами

- законодательство Российской Федерации в области защиты информации. Международные стандарты безопасности информационных систем. Американская концепция системного подхода к обеспечению защиты конфиденциальной информации (OPSEC Operation Security);
- служба информационной безопасности (СИБ) на предприятии. Разделение функций между СИБ, СБ и ИТ-подразделением. Менеджмент информационной безопасности. Порядок проведения аудита информационной безопасности в организации;
- основные направления защиты конфиденциальной информации. Системный подход к защите информации. Методика разработки политики информационной безопасности предприятия;
- правовые, организационные, режимные и инженерно-технические мероприятия по защите конфиденциальной информа-

ции. Создание внутриобъектового и контрольно-пропускного режимов на предприятии. Физическая защита охраняемых информационных ресурсов;

- ИТ мероприятия по защите конфиденциальной информации. Защита компьютерных сетей. Применение средств криптографической защиты информации;
- законодательство РФ о коммерческой тайны. Понятие режима коммерческой тайны. Формирование перечня сведений, составляющих коммерческую тайну. Создание конфиденциального делопроизводства.
- правовые, режимные, технические и ИТ мероприятия по защите коммерческой тайны. Создание корпоративной правовой базы для функционирования режима коммерческой тайны;
- виды юридической ответственности за разглашение коммерческой тайны, а также за незаконное получение этой информации. Необходимые и достаточные условия для ее наступления;
- законодательство РФ о защите персональных данных. Основные требования федерального закона «О персональных данных» и правовых актов регуляторов в части защиты персональных данных;
- организационные, правовые и технические требования по обработке персональных данных. Алгоритмы и пошаговые действия предприятия по выполнению требований законодательства в области обработки персональных данных;
- особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Подготовка организационно-распорядительной документации на предприятии по защите персональных данных;
- особенности обработки персональных данных, осуществляемой в информационных системах персональных данных. Требования к уровню защиты персональных данных в зависимости от типа угроз;
- государственный контроль за обработкой в компаниях персональных данных. Административный регламент государственной функции. Права и обязанности должностных лиц, осуществляющих государственный контроль и лиц, в отношении которых осуществляются мероприятия по контролю. Психологические приемы общения с проверяющими.

Наименование видов занятий по каждой теме:

№ п/п	Наименование тем	Вид занятия
1.	**Политика экономической безопасности. Определение экономических рисков и построение корпоративной защиты**	**Лекционно-практические занятия**
1.1.	международные акты в сфере безопасности бизнеса. Законодательство Российской Федерации в области корпоративной безопасности. Ведомственные и отраслевые требования и стандарты в области защиты бизнеса	Лекционно-практические занятия
1.2.	международный опыт и корпоративные стандарты по защите компаний от экономических преступлений. Международные акты по борьбе с мошенничеством	Лекционно-практические занятия
1.3.	понятие безопасность в российском бизнесе. Постановочные вопросы перед созданием системы защиты бизнеса. Определение объектов защиты. Построение системы корпоративной безопасности	Лекционно-практические занятия
1.4	особенность обеспечения корпоративной безопасности в представительствах иностранных компаний, действующих на территории России, в холдингах, в дочерних компаниях, в компаниях, имеющих сложную организационную (территориально разделенную) структуру	Лекционно-практические занятия

1.5	корпоративная безопасность как элемент риск-менеджмента. Определение внешних и внутренних угроз для предприятия. Составление карты экономических рисков. Участие «безопасника» в управлении рисками на предприятии	Лекционно-практические занятия
1.6	методика проведения аудита безопасности предприятия. Составление плана аудита на основе карты экономических рисков и формирования моделей угроз. Определение видов экономических рисков и вероятности их наступления. Оценка защищенности организационной структуры бизнеса и основных бизнес процессов	Лекционно-практические занятия
1.7	экспертные системы оценки защищенности предприятия. Оценка возможности защиты предприятия от внештатных ситуаций. Создание кризисных планов. Наличие мониторинга безопасности предприятия	Лекционно-практические занятия
1.8	определение субъектов корпоративной безопасности. Своя служба безопасности (СБ) или аутсорсинговое обслуживание. Плюсы и минусы обоих вариантов. Распределение полномочий и зон ответственности между СБ и иными подразделениями предприятия	Лекционно-практические занятия
1.9	юридические тонкости договорных отношений с аутсорсинговыми организациями, предлагающими услуги по защите бизнеса. Правовое обеспечение взаимодействия с частными охранными организациями и субъектами детективной деятельности	Лекционно-практические занятия
1.10	правовая сторона деятельности СБ. Закон и этика в работе. Подчинение, финансирование и оценка эффективности работы СБ. Взаимодействие с акционерами, владельцами и руководителями. Начальник СБ. Какие требования к нему предъявлять, какими чертами характера и профессиональными качествами он должен обладать. Какой образовательный уровень и опыт в прошлой жизни	Лекционно-практические занятия
1.11	корпоративные стандарты безопасности предприятия (КСБ). Совместимость КСБ с иными стандартами, действующими на предприятии. Включение процесс защиты бизнеса в процесс менеджмента непрерывности бизнеса	Лекционно-практические занятия
1.12	разработка локальных актов по обеспечению безопасности предприятия (концепция безопасности, политики, инструкции, регламенты и т.д.). Создание сводов правил и поведений сотрудников	Лекционно-практические занятия
2.	**Конкурентная разведка. Анализ надежности компаний и безопасности коммерческих предложений.**	**Лекционно-практические занятия**
2.1	получение официальной информации из государственных органов и регистрационных организаций	Лекционно-практические занятия
2.2	типы компаний, преследующие противоправные цели	Лекционно-практические

		занятия
3.	**Внешнее мошенничество. Управление дебиторской задолженностью. Защита от рейдерства**	**Лекционно-практические занятия**
3.1	общая характеристика и виды преступлений против собственности	Лекционно-практические занятия
3.2	мошенники и их мотивация, психологические приемы, применяемые мошенниками	Лекционно-практические занятия
3.3	типы компаний, преследующие мошеннические цели.	Лекционно-практические занятия
3.4	создание на предприятии системы предупреждения и защиты от мошеннических операций	Лекционно-практические занятия
4.	**Политика кадровой безопасности. Проведение внутренних проверок и финансовых расследований (форензик)**	**Лекционно-практические занятия**
4.1	особенность проведения внутрикорпоративного расследования (проверки) по наиболее характерным противоправным действиям сотрудников	Лекционно-практические занятия
4.2	использование полиграфа (детектора лжи) при проведении внутрикорпоративных расследований (проверок).	Лекционно-практические занятия
4.3	документальное оформление результатов внутрикорпоративного расследования (проверки	Лекционно-практические занятия
4.4	процедуры увольнения сотрудников с позиции безопасности	Лекционно-практические занятия
5.	**Политика информационной безопасности. Создание режима коммерческой тайны. Защита персональных данных своими силами**	**Лекционно-практические занятия**
5.1	законодательство Российской Федерации в области защиты информации.	Лекционно-практические занятия
5.2	служба информационной безопасности (СИБ) на предприятии. Разделение функций между СИБ, СБ и ИТ-подразделением.	Лекционно-практические занятия

Планы практических занятий

№ п/п	**Наименование практических занятий**	**Продолжительность, часов**	**Доля практических занятий по отношению к общему объему занятий, в %**
1.	**Конкурентная разведка. Анализ надежности компаний и безопасности коммерческих предложений.**	**6**	**x**
1.1	основные задачи конкурентной	1	x

№ п/п	Наименование практических занятий	Продолжительность, часов	Доля практических занятий по отношению к общему объему занятий, в %
	разведки		
1.2	способы сбора информации	1	х
1.3	получение неофициальной информации	0,5	х
1.4	международные информационные ресурсы для сбора и анализа информации по контрагенту	0,5	х
1.5	сбор сведений оперативными методами	0,5	х
1.6	методы анализа информации	0,5	х
1.7	алгоритм определения надежности контрагентов – юридических и физических лиц	0,5	х
1.8	оценка контрагента с позиции налоговых рисков	1	
1.9	анализ учредительных документов организации с позиции безопасности	0,5	х
2.	**Внешнее мошенничество. Управление дебиторской задолженностью. Защита от рейдерства**	**4**	**х**
2.1	причины образования дебиторской задолженности	1	х
2.2	формирование комплекса мер по минимизации угроз, связанных с дебиторской задолженностью.	1	х
2.3	коллекторская деятельность.	0,5	х
2.4	порядок взаимоотношений между подразделениями на предприятии по взысканию задолженности	0,5	х
2.5	проведение переговоров с должниками	1	х
3.	**Политика кадровой безопасности. Проведение внутренних проверок и финансовых расследований (форензик)**	**3**	**х**
3.1	виды угроз, исходящих от сотрудников предприятия, варианты их реализации и возможные направления защиты	1	х
3.2	проверка персонала при приеме на работу	1	х

№ п/п	Наименование практических занятий	Продолжительность, часов	Доля практических занятий по отношению к общему объему занятий, в %
3.3	комплаенс-контроль сотрудников, занимающих должности с коррупционными (мошенническими) рисками.	1	x
4.	**Политика информационной безопасности. Создание режима коммерческой тайны. Защита персональных данных своими силами**	**6**	**x**
4.1	основные направления защиты конфиденциальной информации.	1	x
4.2	правовые, организационные, режимные и инженерно-технические мероприятия по защите конфиденциальной информации.	1	x
4.3	ИТ мероприятия по защите конфиденциальной информации.	1	x
4.4	виды юридической ответственности за разглашение коммерческой тайны,	1	x
4.5	организационные, правовые и технические требования по обработке персональных данных	1	x
4.6	особенности обработки персональных данных, осуществляемой в информационных системах персональных данных.	1	x
5.	**Подготовка и проведение итоговой аттестации**	**2**	**x**
	Итого:	**21**	**52,5**

Методические рекомендации

Описание процесса обучения

Организация и проведение образовательных мероприятий по повышению квалификации производится с использованием современных дистанционных образовательных технологий в соответствии с требованиями информационной безопасности.

Обучение по программе проводиться в течение пяти учебных дней.

Ежедневный план учебных занятий включает:

- вебинары, которые проводятся преподавателем со Слушателями в виртуальных классах (не менее 2-х учебных часов);

- самостоятельное изучение темы Слушателем;

- практикум, которые Слушатели выполняют самостоятельно под контролем кураторов групп (по 4-6 учебных часов).

По завершению обучения Слушатели сдают экзамен (итоговая аттестация) в форме электронного итогового тестирования.

Слушатели, успешно прошедшие аттестацию по программе «Руководителю о безопасности предприятия», получают Удостоверение о повышении квалификации установленного образца. Слушателям, прослушавшим весь курс обучения, но не прошедшим итоговую аттестацию, выдается соответствующая Справка об обучении.

Методика проведения практических занятий

Формирование у слушателей теоретических знаний и практических навыков в области корпоративной безопасности является основной задачей обучения Слушателей по программе «Руководителю о безопасности предприятия».

Акцент в курсе делается на содержании фактов, методов, подходов в сфере защиты экономических интересов предприятия.

Выводы и доказательства формируются в виде алгоритмов последовательности действий, что позволяет слушателям понять принципы и основы методологии исследования системы экономической безопасности организаций.

В программе «Руководителю о безопасности предприятия» конкретизируются знания и навыки, полученные в процессе изучения базовых и специальных экономических (общепрофессиональных) дисциплин, специализированных курсов для более полного и глубокого понимания деятельности главных бухгалтеров и директоров организаций по защите экономических интересов организации от внешних и внутренних угроз.

Объем практических занятий по выполнению конкретных функций в данной программе подготовки составляет 52,5 % от общего объема занятий.

Последовательность практических занятий по освоению слушателями приемов работы следующая:

1. Демонстрация Преподавателем приемов работы во время проведения вебинаров;
2. Изучение слушателями лекций, иного лекционного материала, входящего в состав учебно-методического комплекса;
3. Выполнение слушателями лабораторных практических работ на компьютере, на котором установлен Microsoft Project.

Последовательное изучение практических примеров во время вебинаров, учебного материала, и, наконец, выполнение практической работы позволяет слушателям совершенствовать и получить новые компетенции, необходимые для профессиональной деятельности, и повысить профессиональный уровень в рамках имеющейся квалификации по программе «Руководителю о безопасности предприятия».

Методика проведения контроля и аттестации

Опорными точками контроля участия слушателя в процессе обучения и выполнения программы подготовки являются:

- посещение вебинаров (пробного и ежедневных учебных);
- выполнение практических работ (лабораторных работ на учебном стенде);
- сдача итогового теста.

Для каждой учебной группы куратором группы совместно с администратором вебинаров ведется Таблица контроля за процессом подготовки и проведения обучения.

По результатам работы в процессе занятий и успешного электронного тестирования Слушателям выдается Удостоверение о повышении квалификации установленного образца, не выполнившим дополнительную профессиональную образовательную программу повышения квалификации - Справка о прохождении курса повышения квалификации.

Список литературы:

1. Аналитический выпуск «Проблемы национальной безопасности – 2» под ред. Кимлацкого О.А. М.: Совет Федерации, Аналитическое управление, www.council.gov.ru

2. Бабаев Н.С., Кузьмин И.И. «Абсолютная» безопасность или приемлемый риск?//Коммунист. — 1989. — №7. — С. 75—81.

3. Бурков В.Н., Щепкин А.В. Моделирование экономических механизмов обеспечения безопасности //Проблемы безопасности при чрезвычайных ситуациях. — 2000. — № 6. С. 55—68.

4. Вахрамеев А. В. Международный терроризм и национальная безопасность // Социально-гуманитарные знания, -2004. -N 1-2

5. Вишняков Я.Д. Безопасность социо-эколого-экономических систем России: состояние и перспективы развития подготовки управленческих кадров //Проблемы безопасности при чрезвычайных ситуациях. — М.:. ВИНИТИ. — 2000. — № 6.

6. Вишняков Я.Д. Колосов А.В., Шемякин В.Л. Оценка и анализ финансовых рисков предприятия в условиях априорно враждебной среды бизнеса.//Менеджмент в России и за рубежом. — 2000. — № 3.

7. Вишняков Я.Д. Лозинский С.В. Бизнес и окружающая среда: коэффициент враждебности окружающей среды развитию бизнеса //Менеджмент в России и за рубежом. — 1998. — №3. — С. 43—53.

8. Вишняков Я.Д. Материаловедение и теория технологии материалов в контексте наук о рисках и безопасности //Материаловедение. — 1998. — № 4, 5.

9. Вишняков Я.Д. Новая парадигма третьего тысячелетия //Экономика и жизнь. — 1994. — № 24. — С. 17.

10. Вишняков Я.Д., Измалков А.В. Управление безопасностью социальных и экономических систем //Вестник университета (ГУУ). — 2000. — №1 (3).

11. Вишняков Я.Д., Харченко С.А. Управление обеспечением безопасности предприятий: экономические подходы // Менеджмент в России и за рубежом , -2004, - №5

12. Гуськов Н.С., Зенякин В.Е., Крюков В.В. Экономическая безопасность регионов России. — М.: Алгоритм, 2000. — 288 с.

13. Дворжев А. Ключ к системе безопасности в гостинице//Гостиничное дело, - 2005, -№7, с.31-39

14. Клейнер Г.Б., Тамбовцев В.Л., Качалов Р.М. Предприятие в нестабильной экономической среде: риски, стратегии, безопасность. — М.: Экономика, 2004. — 288 с.

15. Костров А.В., Ткачев А.А. и др. Корпоративная безопасность.- М.: ВИНИТИ. — 2004. — № 6.