

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А. Е. Тарутина

КАДРОВАЯ БЕЗОПАСНОСТЬ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности 38.05.01 «Экономическая безопасность»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 658.8

Рецензент

кандидат экономических наук, доцент кафедры экономики и финансов
ИНОТЭКУ ФГБОУ ВО «КГТУ» И. А. Крамаренко

Тарутина, А. Е.

Кадровая безопасность: учеб.-метод. пособие по изучению дисциплины
для студентов специальности 38.05.01 «Экономическая безопасность» /
А. Е. Тарутина. – Калининград: Локальный электронный методический
материал, 2025. – 61 с.

В учебно-методическом пособии приведен тематический план по дисциплине и даны методические указания по её изучению, подготовке к практическим занятиям, к промежуточной аттестации, а также по выполнению самостоятельной работы. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы Профессионального модуля специальности 38.05.01 «Экономическая безопасность», в состав которого входит дисциплина «Кадровая безопасность».

Рис. 2, табл. 17, список лит. – 6 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой экономической безопасности ФГБОУ ВО «КГТУ» 27.03.2025г., протокол № 8

Учебно-методическое пособие по изучению дисциплины рекомендовано в качестве локального электронного методического материала для использования в учебном процессе методической комиссией ИНОТЭКУ ФГБОУ ВО «КГТУ» 25.04.2025 г., протокол № 4

УДК 658.8

© Федеральное государственное
бюджетное образовательное
учреждение высшего образования
«Калининградский государственный
технический университет», 2025 г.
© Тарутина А. Е., 2025 г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	4
1 Тематический план по дисциплине и методические указания по её самостоятельному изучению	9
Тема 1. Кадровая безопасность организации: понятие и сущность.....	9
Тема 2. Система управления кадровой безопасностью в организации.....	14
Тема 3. Технология обеспечения кадровой безопасности	18
Тема 4. Противодействие угрозам безопасности персонала организации.....	24
Тема 5. Противодействие угрозам информационной безопасности организации со стороны собственного персонала	27
Тема 6. Противодействие угрозам имущественной безопасности организации с участием персонала	29
2 Методические указания для подготовки к практическим занятиям.....	31
Тема 1. Кадровая безопасность организации: понятие и сущность.....	31
Тема 2. Система управления кадровой безопасностью в организации.....	35
Тема 3. Технология обеспечения кадровой безопасности	38
Тема 4. Противодействие угрозам безопасности персонала организации.....	42
Тема 5. Противодействие угрозам информационной безопасности организации со стороны собственного персонала	45
Тема 6. Противодействие угрозам имущественной безопасности организации	49
3 Методические указания по подготовке к промежуточной аттестации.....	52
4 Методические указания по выполнению самостоятельной работы по дисциплине	58
СПИСОК ЛИТЕРАТУРЫ.....	60

ВВЕДЕНИЕ

Учебно-методическое пособие составлено в соответствии с требованиями утвержденной рабочей программы дисциплины «Кадровая безопасность» Профессионального модуля, части, формируемой участниками образовательной программы специалитета по специальности 38.05.01 Экономическая безопасность.

Целью освоения дисциплины «Кадровая безопасность» является формирование у будущих специалистов теоретических знаний и практических навыков в области разработки и реализации стратегии обеспечения стабильного функционирования кадровой составляющей системы экономической безопасности организации

Планируемые результаты освоения дисциплины «Кадровая безопасность» заключаются в том, что студент должен:

знать:

- методы оценки и управления рисками кадровой безопасности, внутрикорпоративных злоупотреблений;
- основы построения и функционирования системы управления кадровой безопасностью;
- полномочия и обязательства менеджмента организации по противодействию кадровым рискам, требования к обеспечению сохранения коммерческой тайны;

уметь:

- анализировать законодательные и локальные нормативные акты по управлению кадровыми рисками и выработать рекомендации по их актуализации;
- принимать организационно-управленческие решения, которые должны привести к повышению уровня кадровой безопасности;
- ставить задачи в рамках обеспечения кадровой составляющей экономической безопасности и контролировать их выполнение;

владеть:

- навыками формирования анализа и оценки информации, необходимой для принятия решений в области обеспечения кадровой безопасности компании;
- умениями проведения внутреннего аудита деятельности организации с целью выявления рисков и угроз кадровой безопасности, формировать интегрированную систему управления рисками;
- приемами разработки и реализации стратегии обеспечения стабильного функционирования системы кадровой составляющей экономической безопасности;

– способностью планирования, организации и координации деятельности службы безопасности и внутреннего аудита в ходе обеспечения кадровой безопасности.

К видам текущего контроля результатов освоения дисциплины «Кадровая безопасность» относятся задания, выполняемые студентами на учебных занятиях и во время самостоятельной работы, а именно:

1) Тестовые задания.

Критерии оценки результатов теста:

- «отлично» – 90–100 % правильных ответов в тесте;
- «хорошо» – 70–90 % правильных ответов в тесте;
- «удовлетворительно» – 50–70 % правильных ответов в тесте;
- «неудовлетворительно» – менее 50 % правильных ответов в тесте.

2) Задания по темам практических (семинарских) занятий.

Критерии и шкала оценивания практических (семинарских) занятий:

– «отлично» – полное раскрытие вопроса; указание точных названий и определений; правильная формулировка понятий и категорий; самостоятельность ответа, умение вводить и использовать собственные классификации и квалификации, анализировать и делать собственные выводы по рассматриваемой теме; использование дополнительной литературы и иных материалов и др.;

– «хорошо» – недостаточно полное, по мнению преподавателя, раскрытие темы; несущественные ошибки в определении понятий, категорий и т. п., кардинально не меняющих суть изложения; использование устаревшей учебной литературы и других источников;

– «удовлетворительно» – отражение лишь общего направления изложения лекционного материала и материала современных учебников; наличие достаточного количества несущественных или одной-двух существенных ошибок в определении понятий и категорий и т. п.; использование устаревшей учебной литературы и других источников; неспособность осветить проблематику учебной дисциплины и др.

– «неудовлетворительно» – нераскрытие темы; большое количество существенных ошибок; отсутствие умений и навыков, обозначенных выше в качестве критериев выставления положительных оценок др.

3) Задания (задачи) по темам практических занятий;

Критерии и шкала оценки результатов:

– «отлично» – выставляется при безошибочно решенной задаче;

– «хорошо» – выставляется, если задача, в основном, решена верно;

– «удовлетворительно» – выставляется при незначительных замечаниях и неточностях по задаче;

– «неудовлетворительно» – выставляется при ответах, не удовлетворяющих критериям, указанным в предыдущих пунктах.

Промежуточная аттестация по дисциплине осуществляется в форме экзамена. К экзамену допускаются студенты, имеющие положительные результаты прохождения текущего контроля.

К оценочным средствам промежуточной аттестации результатов освоения дисциплины «Кадровая безопасность» относятся:

– экзаменационные задания по дисциплине, представленные в виде контрольных вопросов и тестовых заданий закрытого и открытого типов.

Более подробно виды и примеры оценочных средств представлены в приложении к рабочей программе дисциплины – фонде оценочных средств (ФОС), размещенном в ЭИОС КГТУ.

Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41–100 % правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» – менее 40 % правильных ответов; оценка «удовлетворительно» – от 41 до 60 % правильных ответов; оценка «хорошо» – от 61 до 80 % правильных ответов; оценка «отлично» – от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100-балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 1).

Таблица 1 – Система оценок и критерии выставления оценки

Система оценок Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить	Может найти необходимую информацию в рамках	Может найти, интерпретировать и систематизировать	Может найти, систематизировать необходимую

Система оценок Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
	отдельные фрагменты информации в рамках поставленной задачи	поставленной задачи	вать необходимую информацию в рамках поставленной задачи	информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно-корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

Структура учебно-методического пособия по изучению дисциплины включает четыре раздела.

В первом разделе представлен тематический план по дисциплине и методические указания по изучению тем курса, приводятся выдержки наиболее важного при изучении тем материала, а также указаны источники для самостоятельного изучения.

Второй раздел содержит методические указания по подготовке к практическим занятиям согласно тематическому плану, тестовые вопросы и задания.

В третьем разделе учебно-методического пособия представлены методические указания по подготовке к промежуточной аттестации по дисциплине.

В четвертом разделе даны методические указания по выполнению самостоятельной работы по дисциплине. В библиографическом списке указаны рекомендуемые для изучения дисциплины источники литературы.

При необходимости для обучающихся инвалидов или обучающихся с ОВЗ предоставляется дополнительное время для подготовки ответа с учетом его индивидуальных психофизических особенностей.

1 ТЕМАТИЧЕСКИЙ ПЛАН ПО ДИСЦИПЛИНЕ И МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ЕЁ САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ

Тематический план лекционных занятий представлен в таблице 2.

Таблица 2 – Тематический план лекционных занятий (ЛЗ)

Номер темы ЛЗ	Содержание темы ЛЗ
1	Кадровая безопасность: понятие и сущность
2	Система управления кадровой безопасностью организации
3	Технология обеспечения кадровой безопасности
4	Противодействие угрозам безопасности персонала организации
5	Противодействие угрозам информационной безопасности организации со стороны собственного персонала
6	Противодействие угрозам имущественной безопасности организации

Тема 1. Кадровая безопасность: понятие и сущность

Форма занятий – лекция.

Вопросы для изучения

Вопрос 1. Кадровая безопасность организации в современных условиях

Вопрос 2. Риски и угрозы кадровой безопасности

Вопрос 3. Противоправное поведение персонала

Методические указания по изучению темы 1

Вопрос 1. Кадровая безопасность организации в современных условиях

Корпоративная БС – состояние корпорации как системы (ее основных подсистем), при котором вероятность актуализации факторов угрозы ее существованию минимизирована.

Объектами корпоративной безопасности (безопасности организации) выступают:

- финансовые средства, материальные ценности, технологии;
- имущество и информационные ресурсы компании;
- персонал корпорации.

Под *системой корпоративной безопасности* принято понимать организованную совокупность специальных органов, методов, средств и

мероприятий, посредством которых обеспечивается защита корпорации как от внешних угроз, так и внутренних. Ее *элементы*:

- информационная безопасность;
- экономическая безопасность;
- личная безопасность;
- инженерно-техническая и техническая безопасность;
- ИТ-безопасность;
- правовая безопасность;
- кадровая безопасность.

Кадровая безопасность (далее КБ) – это процесс минимизации рисков негативных воздействий на безопасность компании за счет устранения угроз, связанных с персоналом, его деструктивным потенциалом и негативными аспектами трудовых отношений в целом.

Цели КБ:

- формирование целостного представления о КБ и ее взаимосвязи с другими элементами безопасности организации;
- определение путей реализации мероприятий, которые обеспечивают необходимый уровень кадровой безопасности.

Задачи обеспечения КБ:

- своевременное выявление реальных и потенциальных угроз жизненно важным интересам компании со стороны персонала;
- эффективное противодействие и борьба с факторами, препятствующими реализации законных интересов компании и ее сотрудников;
- сохранение интеллектуальной и материальной собственности фирмы;
- разработка и реализация механизма оперативного реагирования на возникающие негативные условия и тенденции развития компании;
- сбор информации, анализ, оценка и предотвращение нежелательных и неправомерных действий сотрудников в отношении компании;
- предотвращение проникновения в организацию криминальных элементов и субъектов противоправной деятельности;
- формирование требований к сотрудникам относительно кадровой безопасности;
- составление нормативной документации, проведение информационно-разъяснительной работы, мониторинг системы кадровой безопасности.

Структура КБ представлена на рисунке 1.

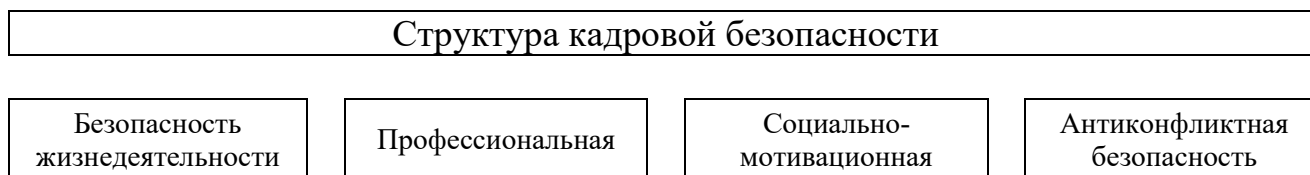


Рисунок 1 – Структура кадровой безопасности организации

Субъект КБ – активный участник процессов в деятельности обеспечения КБ, воздействующий на объект КБ независимо от характера этого воздействия: наносящего ущерб, разрушение или противодействующего этому.

К ним относятся:

- система управления персоналом (СУП) и менеджеры по персоналу;
- служба безопасности (СБ) и менеджеры по безопасности;
- охранники;
- сотрудники информационно-аналитических отделов;
- системные администраторы и другой технический персонал, обслуживающий системы коммуникаций и линии связи компании.

Объектами КБ являются СУП, СБ, персонал в целом и кандидаты на вакансии организации.

Вопрос 2. Риски и угрозы кадровой безопасности

Суть мероприятий по обеспечению КБ – защита деятельности организации от вероятных угроз и рисков, вызванных человеческим фактором.

Кадровый риск – ситуация, отражающая опасность нежелательного развития событий, которые напрямую или косвенно затрагивают функционирование и развитие организации, персонала, общества в целом и наступление которых связано с объективно существующей неопределенностью, обусловленной рядом причин.

Риски КБ делятся на три группы (таблица 3):

Таблица 3 – Классификация кадровых рисков

Группа рисков	Состав
Риски КБ при работе с персоналом на входе в организацию	– риск неправильного выбора источника поиска кандидатов; – риск отсутствия формализованных компетенций должности или нечеткого формирования требований к кандидату на должность; – риск неправильной оценки кандидата на этапе подбора; – риск принятия кандидата с прямыми угрозами кадровой и экономической безопасности организации.
Риски КБ при работе с персоналом внутри организации	– риск неудачной адаптации работника в коллективе или невосприятие коллективом; – риск снижения и потери работником мотивации и стимулов к эффективной работе; – риск оттока профессионалов к конкурентам через предложение лучших

Группа рисков	Состав
	условий работы (переманивание); – риск снижения темпов развития и потеря кадрового потенциала работниками организации; – риск возникновения неконструктивных внутренних конфликтов между работниками организации; – риск прямых злоупотреблений работника, наносящий экономический ущерб организации; – риск создания отрицательного имиджа организации на рынке.
Риски КБ при работе с персоналом на выходе из организации	– риск финансовых претензий работника к организации; – риск формирования отрицательного имиджа организации как работодателя через распространение отрицательной информации о нем; – риск распространения работником информации, являющейся коммерческой тайной, среди его конкурентов.

Угрозы КБ – негативное воздействие кадровой функциональной составляющей на экономическую безопасность предприятия.

Классификация угроз КБ по основным признакам:

- 1) *по источнику возникновения:* внешние и внутренние;
- 2) *по целевой направленности:* угрозы БС сотрудникам организации и угрозы БС организации со стороны ее собственных сотрудников;
- 3) *по характеру потерь:* угрозы информационной и угрозы имущественной безопасности;
- 4) *по субъекту реализации:* со стороны конкурентов, со стороны криминальных структур и отдельных злоумышленников; со стороны государства; со стороны сотрудников организации;
- 5) *по экономическому содержанию:* материального характера и нематериального характера;
- 6) *по вероятности реализации:* потенциальные, реализуемые и реализованные.

Методы противодействия рискам и угрозам классифицируются по следующим признакам:

1. По времени реализации: профилактические (превентивные), пресекающие (отражающие), карающие (репрессивные);
2. По характеру действия: методы административного характера, экономического характера и психологического характера;
3. По степени легитимности: методы легитимного характера, нелегитимного характера, криминальные методы.

Вопрос 3. Типы противоправного поведения персонала

Можно выделить несколько типов поведения сотрудников, которые представляют потенциальную или реальную угрозу безопасности организации (таблица4).

При аддиктивном поведении различают следующие виды зависимостей: фармакологические (химические); субстанциональные; пищевые. Основные группы риска: члены религиозных новообразований, алкоголики, наркоманы, игроки.

В организации, как правило, в той или иной степени присутствуют все из вышеперечисленных деструктивных форм поведения. Однако наибольшую опасность, в том числе и финансовую, представляет девиантное поведение, существующее в виде различных типов мошенничества.

Мошенничество представляет собой незаконное, путем обмана, подтасовки, манипуляций, присвоения чужой собственности, активов компании поведение.

Таблица 4 – Типы противоправного поведения сотрудников организации

Тип поведения	Особенности
Аддиктивное поведение	Уход от реальности путем изменения своего психического состояния с помощью наркотиков, алкоголя или постоянной фиксации внимания на определенных предметах или видах деятельности (карты, бега) для получения интенсивных эмоций. Эти процессы управляют жизнью человека, лишают воли. Для достижения своих целей аддикт может пожертвовать, чем угодно
Антисоциальное девиантное поведение	Совершение действий, противоречащих этике и морали, безответственность, игнорирование законов и прав других людей
Суицидное поведение	Подвергающее свою (и рядом находящихся людей) жизнь риску
Конформистское поведение	Исполнение воли «авторитета», приспособленчество, отсутствие критичности, неспособность принимать решения, брать на себя ответственность
Нарцисстическое поведение	Повышенная чувствительность к оценкам других людей, отсутствие достаточного чувства сопереживания, дистанцирование от коллектива, неприятие его норм и требований
Эгоистическое, индивидуально-целевое деструктивное поведение	Основа – достижения личных целей за чужой счет; сопровождается, имитационным поведением, когда истинные эгоистические цели камуфлируются псевдо-активностью, псевдо-исполнительностью, демагогией, ошибками восприятия (сделал задания так, как понял, а понял неверно)
Фанатическое поведение	Слепая приверженность какой-либо идее, нетерпимости к другим взглядам, что может сопровождаться действиями насильственного характера. Нейтральные или дружеские поступки других людей часто оцениваются как враждебные или заслуживающие презрения
Аутистическое поведение	Затруднение социальных контактов, оторванность от реальности, погруженность в сферу мечтаний; невозможность адекватно оценить ситуацию и принять решение

Суть любого мошенничества составляют три основных элемента (треугольник мошенничества): давление внешних обстоятельств, возможность совершить мошенничество и самооправдание.

Методические материалы по теме 1

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 1: [1, с 5–28, 2, 3, 4].

Тема 2. Система управления кадровой безопасностью организации

Форма занятий – лекция.

Вопросы для изучения

Вопрос 1. Структура системы управления кадровой безопасностью организации

Вопрос 2. Субъекты и объекты системы управления кадровой безопасностью

Вопрос 3. Условия эффективного функционирования системы управления кадровой безопасностью

Вопрос 4. Корпоративное мошенничество

Методические указания по изучению темы 2

Вопрос 1. Структура системы управления кадровой безопасностью организации

Принципы формирования системы управления КБ: целостности; срочности; надежности; правомерности; экономичности; согласованности; открытости и приватности; профессионализма.

<i>Система управления кадровой безопасностью – совокупность взаимосвязанных элементов, подразделений и должностных лиц.</i>

Имеет типовую структуру и включает в себя *три основных элемента* (рисунок 2).

<i>Стратегия управления кадровой безопасностью (далее СУКБ) – совокупность долгосрочных целей и управленческих подходов, реализация которых обеспечивает защиту организации от любых потенциальных угроз, связанных с функционированием кадрового направления ее деятельности.</i>
--

На практике чаще всего применяются **три основных варианта СУКБ:**

1. Стратегия адекватного ответа на угрозы;
2. Стратегия пассивной защиты от угроз;
3. Стратегия упреждающего противодействия угрозам.

<i>Операционные подсистемы – это самостоятельные элементы системы управления, каждый из которых направлен на решение формализованного перечня однотипных задач по обеспечению КБС организации.</i>
--

Подсистем – две. Одна направлена на противодействие угрозам безопасности сотрудников, другая – на противодействие угрозам, исходящих от самих от сотрудников.



Рисунок 2 – Основные элементы системы управления кадровой безопасностью

Блок обеспечения включает в себя несколько направлений: информационное, нормативно-методическое, технологическое, кадровое, инструментальное, финансовое обеспечение органов, собственных подразделений и отдельных сотрудников.

Для оценки эффективности управления КБ используется критерии:

- общее количество выявленных угроз, с дифференциацией на угрозы, пресеченные в полном объеме, пресеченные лишь частично, негативно реализованные в полном объеме;
- прямой финансовый ущерб, нанесенный организации в результате частично и полностью реализованных угроз;
- потенциальный ущерб, который могли бы нанести организации полностью или частично пресеченные угрозы;
- результаты реализации плановых профилактических мероприятий;

– отсутствие обоснованных претензий к СБ со стороны правоохранительных

Процесс управления КБ должен строиться на основе системного подхода, учитывающего все аспекты обеспечения безопасности. Он представляет собой последовательность определенных действий (этапов):

- определение элементов СУ КБС;
- создание информационной базы;
- подсистема мониторинга угроз КБС;
- подсистема контроля.

Вопрос 2. Субъекты и объекты системы управления кадровой безопасностью

Все множество субъектов КБ можно разделить на две группы: внешние и внутренние, в каждой из которых выделяют по две подгруппы: противодействующие и способствующие обеспечению КБ.

Субъект кадровой безопасности – это активный участник процессов в деятельности обеспечения кадровой безопасности, воздействующий на объект кадровой безопасности независимо от характера этого воздействия: наносящего ущерб, разрушение или противодействующего этому.

Сотрудник организации является центральным, ключевым звеном всей совокупности субъектов.

Причины, по которым он может превратиться в источник угроз, следующие: политико-идеологические, психологические, социально-экономические, моральные, национальные, физиологические, стратегические, профессиональные, финансовые.

К *внешним субъектам, способствующим обеспечению КБ*, относятся: органы законодательной, исполнительной и судебной власти всех уровней; правоохранительные органы; функциональные и отраслевые министерства и ведомства; налоговые и таможенные службы и др.

К *внешним субъектам, противодействующим обеспечению КБ*, относятся конкуренты, теневые экономические структуры и элементы криминальных структур, бывшие сотрудники, неудовлетворенные оценкой своего труда.

К *внутренним субъектам, способствующим обеспечению КБ*, относятся сотрудники и структурные подразделения, непосредственно осуществляющие деятельность по защите КБ организации на основании предоставленных им полномочий принимать решения о целях, задачах, средствах и методах обеспечения КБ и осуществления их (служба безопасности (СБ), служба управления персоналом (СУП), финансовая служба и др.)

К внутренним субъектам, противодействующим обеспечению КБ организации, относятся нелояльные сотрудники, не удовлетворенные оценкой их труда.

Основным субъектом обеспечения КБ является СБ организации.

Служба безопасности – специализированное структурное подразделение организации, созданное для обеспечения ее защиты от возможных угроз.

Различают три стратегических подхода к организации работы СБ:

- 1) полный отказ от услуг сторонних специализированных структур и формирование полноценной по функциям собственной СБ;
- 2) минимизация штатных сотрудников СБ, с возложением основных ее функций на сторонние специализированные структуры;
- 3) возможность ограниченного использования услуг специализированных частных структур для выполнения локальных задач, обычно сомнительных с позиции их легитимности.

Перечень основных структурных подразделений СБ: информационно–аналитический отдел; отдел информационной безопасности; отдел физической защиты; отдел собственной безопасности; служба режима.

Функции СБ организации формируются в рамках ее взаимодействия с другими подразделениями, а именно:

а) взаимодействие с маркетинговой службой – совместное изучение и анализ конкурентов, подготовка аналитических обзоров и рекомендаций для руководства; выполнение специальных поручений по сбору дополнительной информации об отдельных клиентах и партнерах;

б) взаимодействие со службой персонала – проведение специальных проверок при найме новых сотрудников по заявке со стороны СУП; участие в первичном обучении вновь нанятых сотрудников; координация действий по контролю над лояльностью персонала и соблюдением правил обеспечения БС;

в) взаимодействие с финансовой службой – передача и обоснование заявок на финансовые ресурсы, необходимые для СБ, отчеты об использовании выделенных средств; совместное расследование фактов нарушений корпоративной финансовой дисциплины (в случае прямых хищений):

г) взаимодействие со службой информационных технологий – совместные действия по защите компьютерных сетей от несанкционированного проникновения и повреждения.

В области обеспечения безопасности функции СУП и КБ сходны, но имеются и различия.

Главное – направленность деятельности.

Если СБ осуществляет всестороннее обеспечение безопасности (силовую, информационную, техническую), то СУП занимается только кадровыми вопросами, её деятельность более специализирована (таблица 5).

Таблица 5 – Структура совместно выполняемых СУП и СБ функций

Функции СУП	Функции СБ
Отбор персонала	Проверка по базам данных
Оформление на работу	Уровень допуска к информации
Адаптация работника	Инструктаж по правилам безопасности и внутреннего распорядка
Социальная поддержка работника	Юридическая помощь работнику
Управление трудовой дисциплиной	Пропускной и внутриобъектовый режим
Управление конфликтами	Юридическая помощь работникам

Вопрос 3. Условия эффективного функционирования системы управления кадровой безопасностью

Для того, чтобы система управления КБ была эффективной, необходимо соблюдение следующих условий:

- системный подход к проблеме обеспечения КБ;
- приоритет мероприятий по предотвращению потенциальных угроз;
- обеспечение приоритетной защиты конфиденциальной информации;
- непосредственное участие в обеспечении КБ организации всех ее должностных лиц;
- обеспечение взаимодействия системы управления КБ с другими направлениями менеджмента;
- соразмерность затрат на обеспечение КБ организации реальному уровню угроз;
- формализованное закрепление не только функциональных обязанностей, но и полномочий (предела компетенции) СБ;
- использование всего спектра методов кадровой безопасности организации.

Методические материалы по теме 2

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.
Ссылки на рекомендуемые источники по теме 2: [1, с. 34–51, 3, 4].

Тема 3. Технология обеспечения кадровой безопасности

Форма занятий – лекция.

Вопросы для изучения

Вопрос 1. Обеспечение кадровой безопасности при найме и увольнении сотрудников

Вопрос 2. Развитие лояльности персонала для обеспечения кадровой безопасности

Вопрос 3. Контроль персонала как условие обеспечения кадровой безопасности

Вопрос 4. Корпоративное мошенничество

Методические указания по изучению темы 3

Вопрос 1. Обеспечение кадровой безопасности при найме и увольнении сотрудников

КБС предприятия зависит от трех факторов:

1. *Наем*, под которым понимается целый комплекс мер БС при приеме на работу и прогнозирования благонадежности;

2. *Лояльность* – комплекс мер по установлению позитивных отношений работников к работодателям;

3. *Контроль* – представляет собой комплекс мер, который непосредственно нацелен на ликвидацию возможностей причинения ущерба организации.

Таким образом, комплексная работа по обеспечению КБ организации может быть разделена на три основных этапа:

- деятельность на этапе проверки кандидата и приема его на работу;
- мероприятия на этапе осуществления работником своей основной профессиональной деятельности;
- обеспечение корпоративной безопасности на этапе увольнения работника.

При найме ключевыми элементами являются организация подбора и отбора кандидатов на вакантные должности.

Подбор персонала – комплекс мер, направленных на выявление целого ряда знаний о кандидате.

Комплексная проверка соискателя вакантной должности должна включать:

1) сбор официальной информации и формальные проверки (заполнение анкеты, предоставление копий документов и проверка их подлинности; получение отзывов с прежнего места работы, информации с баз данных, тестирование кандидата);

2) собеседования (первое проводит кадровик для уточнения данных; второе – кадровик, устраняя разногласия в информации; третье – руководитель для выяснения профессионализма; скрытые собеседования – вне компании);

3) сбор субъективной информации и неформальные проверки.

Контроль персонала при найме – самый ответственный этап, так как здесь возникают первые риски. Основная нагрузка по его осуществлению ложится на СУП предприятия, тогда как работники СБ привлекаются при необходимости.

Поиск персонала обычно происходит в двух направлениях:

- использование внутренних резервов компании;
- привлечение соискателя извне.

Существует ряд *подходов*, позволяющих решать проблемы БС при подборе и отборе сотрудников.

Первый подход – гарантии кадрового агентства в отношении подбираемых работников.

Второй подход – использование метода «сарафанное радио».

Третий подход – использование фирмой собственной службы безопасности для проверки кандидатов и предоставляемых ими сведений.

На **стадии отбора** решаются два основных вопроса:

- 1) отсев заведомо непригодных работников;
- 2) оценка личных и профессиональных качеств принятых на работу.

Также необходимо выявить принадлежность или склонность соискателя к одной из групп риска. К ним относят людей, имеющих следующие проблемы:

- склонность к коррупции;
- тяжелое социально-экономическое положение;
- различного рода зависимости.

Комплексная проверка соискателя вакантной должности должна включать в себя следующее:

- 1) сбор официальной информации и формальные проверки;
- 2) ряд собеседований;
- 3) сбор субъективной информации и неформальные проверки.

Контроль персонала в процессе трудовой деятельности представляет собой комплекс мер из установленных для персонала всех уровней регламентов, ограничений, режимов, оценочных операций и процедур безопасности.

Основными направлениями контроля персонала в процессе трудовой деятельности с позиции БС являются:

- контроль результатов деятельности (достижений);
- контроль использования рабочего времени;
- информационный контроль.

Обеспечение кадровой безопасности **на этапе увольнения работника.**

В ТК РФ четко прописана процедура выхода сотрудника из компании. Однако, если сама процедура была некорректной, компания может понести значительный моральный и материальный ущерб. *Моральный ущерб* может

быть нанесен через антирекламу организации, а *материальный* – в случае обращения уволенного сотрудника в суд.

Для того чтобы снизить подобные риски, можно использовать следующие меры:

- подписание при приеме на работу соглашения о невозможности работы на прямого конкурента при увольнении на протяжении определенного периода времени;
- подписание договора о неразглашении коммерческой информации с четким определением границ коммерческой тайны и суммами ответственности за ее разглашение;
- перед этапом высвобождения работника из компании осуществить его перевод на работу без доступа к информации, носящей коммерческую тайну;
- изучение причин увольнения и его отношения к компании.

В случае прекращения работы в организации и независимо от причин увольнения работник, до полного расчета должен вернуть все находящиеся в его распоряжении документы, информацию и другие материалы, закрепленные на любых носителях.

Профилактическая работа с увольняющимися сотрудниками. Основная задача руководителя СБ – получение оперативно значимой информации. Осуществляется с сотрудниками, увольняющимися по собственному желанию. Задача – получение информации из первых рук от людей, которым нет смысла что-то скрывать.

Вопрос 2. Развитие лояльности персонала для обеспечения кадровой безопасности

Одним из условий обеспечения КБС организации является сохранение лояльности персонала.

Лояльность сотрудника – это верность, преданность целям и ценностям компании, осуществление деятельности, которая поддерживает и помогает реализовывать эти цели.

Атрибуты лояльности:

- честность по отношению к объекту лояльности;
- разделение с объектом лояльности основных убеждений, ценностей;
- открытая демонстрация лояльности, доброжелательное отношение;
- переживание за успех объекта лояльности;
- готовность предупредить опасность для объекта лояльности;
- готовность при необходимости идти на определенные жертвы в пользу объекта лояльности;

- чувство гордости за причастность к объекту лояльности;
- стремление наилучшим образом исполнять обязанности, функции, миссию, возложенные на человека объектом лояльности.

Лояльность сотрудника – это верность, преданность целям и ценностям компании, осуществление деятельности, которая поддерживает и помогает реализовать эти цели. *Преданность может рассматриваться как высший уровень лояльности.*

Выделяют следующие уровни лояльности/нелояльности: лояльность на уровне убеждений; лояльность на уровне поступков и действий; лояльность на уровне внешних атрибутов; нулевая лояльность; скрытая (тайная) нелояльность; открытая (демонстративная) нелояльность.

Нелояльные сотрудники – это те сотрудники, которые равнодушны к ценностям компании и ее целям, не готовы прилагать усилия для их достижения.

Лояльность иногда отождествляют с благонадежностью персонала, однако, эти понятия не синонимичны.

Благонадежность сотрудника определяется как соблюдение (стремление соблюдать) человеком правовых и моральных норм, принятых в данной группе.

Для оценки благонадежности используются следующие методы: психологический, социометрический и контрразведывательный.

Лояльность и благонадежность могут сочетаться по-разному: благонадежен и лоялен; неблагонадежен, но лоялен; благонадежен, но не лоялен; неблагонадежен и нелоялен.

Можно выделить минимум три **составляющие лояльности**:

- доверие персонала к руководству компании;
- справедливость отношений, складывающихся у сотрудника с представителями администрации компании;
- удовлетворенность работой.

Развитие лояльности состоит в увеличении ее составляющих.

Вопрос 3. Контроль персонала как условие обеспечения кадровой безопасности

Контроль – комплекс мер, установленных для персонала и содержащихся в регламентах, объединяющих ограничения, режимы, технологические процессы, оценочные, контрольные и другие операции и процедуры безопасности.

Контроль персонала в процессе трудовой деятельности представляет собой комплекс мер из установленных для персонала всех уровней регламентов, ограничений, режимов, оценочных операций и процедур безопасности.

Он имеет целью ликвидацию возможности причинения ущерба со стороны работников. Как правило, такой контроль осуществляется СБ или другими подразделениями, в меньшей степени СУП.

Контроль в процессе трудовой деятельности осуществляется по четырем направлениям (нормативное, организационное, профессиональное, финансовое) и в рамках трех форм (предварительного, текущего и итогового контроля).

Обеспечение КБС предполагает и текущий контроль за «проблемным персоналом».

«Проблемный» – это персонал, который может выступать потенциальным источником причинения ущерба организации.

Группы работников, потенциально опасных для КБС:

- повышенно конфликтный персонал;
- подверженные воздействию;
- карьеристы;
- недовольные (амбициозные);
- любители красивой жизни;
- частые «отпускники».

Основными задачами организации контроля персонала организации выступают:

- оценка общей эффективности управления обеспечением безопасности организации;
- контроль над лояльностью конкретных сотрудников;
- выявление конкретных нарушений и их виновников.

Данная работа осуществляется службой безопасности одновременно по направлениям: профилактический контроль, контроль личной лояльности

Вопрос 4. Корпоративное мошенничество

Корпоративное мошенничество – это умышленное неправомерное действие или бездействие сотрудников частных или государственных компаний, направленное на получение личной выгоды против интересов компании.

В зоне риска мошенничества находятся сотрудники организации, которые: имеют существенные финансовые затруднения; увлекаются азартными играми; алко- и наркотически зависимы; имеют тяжелобольных

близких родственников; часто меняют место работы; психически неуравновешенны.

Практика выработала несколько **групп методов** противодействия корпоративному мошенничеству: методы предупреждения; методы выявления; методы расследования.

В каждой из трех групп можно выделить организационные и технические методы.

Методические материалы по теме 3

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 3: [1, с. 292–321, 3, 5, 6].

Тема 4. Противодействие угрозам безопасности персонала организации

Форма занятий - лекция.

Вопросы для изучения

Вопрос 1. Противодействие угрозе переманивания сотрудников организации

Вопрос 2. Противодействие угрозе склонения сотрудников к нелояльному поведению в отношении работодателя

Вопрос 3. Противодействие угрозе покушений на собственников и топ-менеджеров организации

Методические указания по изучению темы 4

Вопрос 1. Противодействие угрозе переманивания сотрудников организации

БС персонала организации- совокупность мер по обеспечению защиты сотрудников от потенциальных угроз в форме переманивания конкурентами, вербовки, шантажа, прямых угроз жизни и здоровью, покушений.

Субъекты угрозы:

– для любых организаций, кроме органов гос. управления – *конкуренты*;
– для государственных органов – *подведомственные или подконтрольные им коммерческие структуры*.

Объекты угрозы: менеджеры; ведущие специалисты; высококвалифицированные работники, представители рабочих профессий.

Формы реализации угрозы: предложение лучших условий найма, параллельном решении жизненно важной для человека проблемы; шантаж в форме угрозы передачи работодателю или правоохранительным органам компрометирующей сотрудника информации.

Основная причина успешной реализации данной угрозы – недовольство переманиваемого сотрудника. Противодействие – в его устранении.

Вопрос 2. Противодействие угрозе склонения сотрудников к нелояльному поведению в отношении работодателя

Нелояльный сотрудник – работник организации, способный в собственных имущественных или неимущественных интересах, либо в силу общей безответственности нарушить доверие работодателя и нанести ущерб.

Объекты угрозы – должностные лица, занимающие рабочие места, которые обеспечивают доступ: к конфиденциальной информации; к управлению денежными средствами и ТМЦ, а также к их хранению; к реализации функций управления, регулирования и надзора.

Субъекты угрозы могут быть внешними и внутренними.

- *Внешние:* государство (в лице правоохранительных, фискальных и контролирующих органов); конкуренты; криминальные структуры; индивидуально действующие злоумышленники.

- *Внутренние:* руководитель сотрудника–объекта угрозы; подчиненный сотрудника–объекта угрозы; работники подконтрольных сотруднику подразделений; коллеги по работе.

Формы реализации: превращение сотрудника в постоянно действующий источник утечки конфиденциальной информации; разовое разглашение сотрудником конфиденциальных сведений; соучастие сотрудника в реализации угроз в адрес работодателя со стороны третьих лиц; злоупотребление сотрудником своими служебными полномочиями в интересах третьего лица; акты прямого саботажа по заказу третьего лица.

Инструмент реализации данной угрозы вербовка – действия со стороны представителей конкурентов, криминальных группировок, правоохранительных органов государства, направленные на то, чтобы склонить конкретного работника к нарушению доверия со стороны работодателя. Вербовка может быть с использованием подкупа, шантажа, «игры» на недовольстве работодателем, прямых угроз.

Организация противодействия угрозе предполагает использование следующих прикладных процедур (технологий) и методов:

- 1) *Профилактика угрозы:* организация тщательного отбора кандидатов в целях отсева лиц, чьи личностные качества или автобиография делают их уязвимыми для вербовки; обучение сотрудников правилам служебного и внеслужебного поведения, исключающего возможность их последующего шантажа; специальное обучение сотрудников правилам поведения в случае попыток их вербовки; постоянный контроль над сотрудниками, занимающими рабочие места, опасные с позиции рассматриваемой угрозы; специальные

служебные проверки сотрудников, в отношении которых у руководителя или СБ по результатам контроля появились обоснованные подозрения.

2) *Пресечение угроз и наказание их виновников*: перевод сотрудника на другое рабочее место, неинтересное для потенциальных субъектов угрозы; мотивация сотрудника, своевременно проинформировавшего СБ о попытке его вербовки или угроз; освобождение сотрудника от ответственности за уже допущенные нарушения, ставшие поводом для шантажа, в случае своевременного информирования СБ об этой попытке; увольнение сотрудника, ставшего «агентом влияния»; использование завербованного сотрудника в качестве источника дезинформации, с последующим увольнением; использование уголовного преследования виновных сотрудников.

Вопрос 3. Противодействие угрозе покушений на собственников и топ-менеджеров организации

Причины устранения: участие в борьбе за раздел гос. собственности, осуществляемой с использованием нелегитимных методов; конфликты, связанные с рейдерским захватом чужого бизнеса; конфликты между конкурентами; невыполнение обязательств, принятых на себя в рамках сотрудничества с организованной преступностью или в отношении крупных клиентов и партнеров; нерешенные внутрикорпоративные проблемы.

Субъекты угрозы: внешние (конкуренты, криминальные структуры); внутренние (совладелец бизнеса, один из топ-менеджеров, близких по должностному статусу).

Объекты угрозы: собственники организации; топ-менеджеры организации или высокопоставленные государственные служащие.

Формы реализации: открытое покушение; имитация самоубийства; скрытое покушение с использованием нетрадиционных средств.

Организация противодействия угрозе предполагает использование следующих прикладных процедур (технологий) и методов:

1) *Профилактика угрозы*: отказ от работы в сфере бизнеса или участия в операциях, где угроза становится реальной; строгое соблюдение правил и норм, неформально сложившихся в соответствующей сфере бизнеса; эффективная деловая разведка и контрразведка; ликвидация самой причины покушения; специальное обучение собственников и топ-менеджеров правилам обеспечения собственной физической безопасности.

2) *Пресечение угрозы*: использование угроз адекватного воздействия на самого заказчика; усиление защиты объекта покушения до уровня, делающего угрозу практически нереализуемой; обращение к правоохранительным органам.

Однозначный приоритет методов профилактики при противодействии угрозе покушения на высших должностных лиц организации.

Методические материалы по теме 4

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 5: [1, с. 107–157, 2, 3, 4, 6].

Тема 5. Противодействие угрозам информационной безопасности организации со собственного персонала

Форма занятий – лекция.

Вопросы для изучения

Вопрос 1. Конфиденциальная информация как объект защиты

Вопрос 2. Реализация угроз информационной безопасности организации с участием персонала

Вопрос 3. Противодействие угрозам информационной безопасности организации со стороны ее персонала

Вопрос 4. Управление персоналом организации в целях обеспечения ее информационной безопасности

Методические указания по изучению темы 5

Вопрос 1. Конфиденциальная информация как объект защиты

Информационная БС организации (далее ИБС) – совокупность мер по обеспечению защиты конфиденциальной информации от ее перехвата, разглашения, а также искажения или уничтожения.

Конфиденциальная информация – информация, доступ к которой ограничивается в целях защиты коммерческой или клиентской тайны, а также другие сведения, разглашение которых по каким-либо причинам нежелательно для конкретной организации. Делится на две категории: составляющая коммерческую тайну; составляющая клиентскую тайну.

Коммерческая тайна – разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести ей имущественный или неимущественный ущерб.

Клиентская тайна – разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести имущественный или неимущественный ущерб ее клиентам или партнерам по хозяйственной деятельности.

Защита информации должна обеспечиваться соблюдением:

- конфиденциальности, т. е. защиты от несанкционированного доступа;
- целостности, т. е. защиты от несанкционированного изменения;
- доступности, т. е. защиты от несанкционированного удержания информации и ресурсов.

Вопрос 2. Реализация угроз информационной безопасности организации с участием персонала

Причины реализации угроз ИБС организации со стороны ее персонала – безответственность сотрудников или их злой умысел.

Субъекты угроз ИБС: конкуренты; криминальные структуры; хакеры; собственные нелояльные сотрудники; государство в лице фискальных или правоохранительных органов.

Формы реализации угроз ИБС организации: перехват конфиденциальной информации, хищение, повреждение или уничтожение, искажение.

Вопрос 3. Противодействие угрозам ИБС организации со стороны ее персонала осуществляется в несколько этапов:

1. Формирование ранжированного перечня конфиденциальных сведений организации и присвоение им соответствующего грифа секретности (конфиденциальности);
2. Оценка возможных каналов утечки (перехвата) конфиденциальной информации организации;
3. Определение перечня прикладных методов защиты информации;
4. Непосредственное формирование и внедрение подсистемы информационной безопасности организации.

Гриф конфиденциальности – специальная отметка на конфиденциальных документах (базах данных), определяющая степень защиты содержащихся в них сведений.

Чаще всего используется следующий типовой перечень конфиденциальных сведений организации:

- абсолютно конфиденциальные сведения;
- строго конфиденциальные сведения;
- конфиденциальные сведения;
- информация для служебного пользования.

Методы защиты информации делятся на следующие группы:

- методы программно-математического характера;
- методы технического характера;
- методы организационного характера.

Вопрос 4. Управление персоналом организации в целях обеспечения ее информационной безопасности подразумевает следующие направления.

- 1) обучение сотрудников организации правилам обеспечения информационной безопасности работодателя.
- 2) контроль над сотрудниками организации.

3) мотивация сотрудников организации в целях обеспечения ИБС

Общие методические требования к организации подготовки:

1) распространение подготовки на все категории персонала организации, с дифференциацией ее форм и методов по должностным категориям;

2) непрерывность подготовки, что обеспечивается регулярным проведением специальных профилактических бесед или разбором уже состоявшихся угроз в адрес организации;

3) привлечение к подготовке не только специалистов СБ и СУП, но и руководителей структурных подразделений;

4) использование в процессе обучения наряду с теоретическими материалами практических примеров из деятельности своей и сторонних организаций;

5) использование методов обучения, способных вызвать интерес обучаемых к самому процессу подготовки.

Формы контроля: профилактический контроль, контроль личной лояльности.

Мотивация сотрудников организации в целях обеспечения ее ИБС реализуется по двум направлениям:

1. Специальные поощрения за активную работу по укреплению ИБС;

2. Специальные санкции за допущенные нарушения в области соблюдения установленных правил обеспечения ИБС.

Методические материалы по теме 5

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 6: [1, с. 158–208, 2, 3, 6].

Тема 6. Противодействие угрозам имущественной безопасности организации с участием персонала

Форма занятий – лекция.

Вопросы для изучения

Вопрос 1. Имущество организации как объект защиты

Вопрос 2. Реализация угроз имущественной безопасности организации с участием персонала

Вопрос 3. Противодействие угрозам имущественной безопасности организации со стороны ее персонала

Вопрос 4. Управление персоналом организации в целях обеспечения ее имущественной безопасности

Методические указания по изучению темы 6

Вопрос 1. Имущество организации как объект защиты

Предприятие – это имущественный комплекс, используемый собственниками этого имущества для осуществления предпринимательской деятельности.

Имущественная БС организации (ИмБС) – совокупность мер по обеспечению защиты имущества от угрозы насильственного (ограбление) и ненасильственного (кражи) хищения, а также повреждения или уничтожения.

С позиции ИмБС высоколиквидные активы, а именно наличные денежные средства, а также часть имущества организации в материальной форме являются основным объектом хищения, а значит, защиты.

Вопрос 2. Реализация угроз имущественной безопасности организации с участием персонала

Субъектами угроз ИмБС организации могут выступать: конкуренты, криминальные структуры, индивидуальные злоумышленники, клиенты или партнеры организации, собственные сотрудники.

Формы реализации угроз имущественной безопасности:

- перехват прав собственности на имущество организации;
- хищение имущества;
- повреждение или уничтожение имущества;
- реализация невыгодных или прямо убыточных для нее хозяйственных операций.

Вопрос 3. Противодействие угрозам имущественной безопасности организации со стороны ее персонала

Включает несколько, последовательно выполняемых этапов:

1. Формирование ранжированного перечня имущества организации;
2. Оценка возможных угроз ИмБС организации со стороны ее сотрудников с учетом специфики ее деятельности;
3. Определение перечня прикладных методов защиты имущества;
4. Формирование и внедрение подсистемы ИмБС организации.

Вопрос 4. Управление персоналом организации в целях обеспечения ее имущественной безопасности

Работа с персоналом организации в целях профилактики и пресечения угроз ИмБС осуществляется по той же технологии и с использованием тех же базовых методов, что и при противодействии угрозам ИБС (см. тему 6).

Общее отличие: наличие рабочих мест, предполагающих прямую материальную ответственность занимающих их сотрудников за сохранность и правильное использование доверенных денежных средств и ТМЦ.

Особенности в организации обучения: специальное техническое обучение, уменьшающее вероятность неумышленного повреждения имущества;

специальное обучение сотрудников СБ технике отражения угроз ИмБС организации, осуществляемых насильственными методами.

Особенности в организации контроля: включение в число субъектов контроля финансовой службы, а также материально-ответственных лиц; использование методов финансового контроля, технологий инвентаризации, независимых экспертов для проверки заключаемых контрактов.

Особенности в организации мотивации: в области позитивной мотивации – использование форм дополнительной оплаты труда, снижающих вероятность финансовых злоупотреблений; в области специальных санкций – возмещение прямого ущерба, нанесенного материально ответственными лицами; привлечение сотрудников, виновных в хищениях имущества, не только к административной, но и к уголовной ответственности.

Методические материалы по теме 6

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 7: [1, с. 208–256, 2, 3, 5].

2 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ПОДГОТОВКИ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Тема 1. Кадровая безопасность организации: понятие и сущность

Форма занятий – практическое занятие

Цель: закрепление понятия кадровой безопасности и ее месте в системе экономической безопасности организации, приобретение умений и навыков оценки состояния КБС.

Методические указания для подготовки к практическим занятиям по теме 1

Практическое задание 1

Оценить процесс обеспечения экономической безопасности ООО «Континент», ее функциональных составляющих и посчитать совокупный критерий экономической безопасности предприятия.

Условия задачи

ООО «Континент» относится к области малого и среднего бизнеса. Фирма работает на рынке оптовой торговли Калининграда и области. Цель бизнеса на ближайший период – расширение рынка сбыта за счет монопольной реализации продукции. Офис и склад фирмы находятся в Калининграде. Продукция – вода минеральная питьевая газированная «Прусская» в бутылках

объемом 1,5 л. и 0,5 л. Покупатели – оптовые фирмы по реализации минеральных вод и магазины, реализующие данную продукцию в розницу.

Методические указания по выполнению практического задания

1) Пользуясь данными таблиц 6, 7, рассчитать следующие показатели и сделать вывод о состоянии экономической безопасности предприятия:

а) абсолютное отклонение объемов реализации по годам в сопоставимых ценах:

$$\Delta y_i = y_i - y_{i-1},$$

где y_i – объем реализации отчетного периода; y_{i-1} – объем реализации предшествующего периода;

б) темп роста объемов реализации по годам:

$$Tr = y_i / y_{i-1} * 100 \%;$$

в) темп прироста объемов реализации по годам:

$$Tpr = (y_i - y_{i-1}) / y_{i-1} * 100 \%.$$

2) На основании анализа данных таблиц 8, 9 сделайте выводы о состоянии кадровой безопасности и необходимости увеличения численности работников фирмы.

Таблица 6 – Реализация воды минеральной лечебно-столовой «Прусская» в бутылках емкостью 0,5 л, тыс. руб.

Год	Объем реализации	Абсолютное отклонение объемов реализации	Темп роста объемов реализации	Темп прироста объемов реализации
2021	2546,0			
2022	2889,5			
2023	3957,0			

Таблица 7 – Реализация воды минеральной лечебно-столовой «Прусская» в бутылках емкостью 1,5 л, тыс. руб.

Год	Объем реализации	Абсолютное отклонение объемов реализации	Темп роста объемов реализации	Темп прироста объемов реализации
2018	4306	-	-	-
2019	5023			
2020	6276			

Таблица 8 – Загрузка торгово-оперативного и вспомогательного персонала ООО «Континент»

Показатель	Водитель погрузчика	Водитель	Кладовщик	Кассир	Оператор
Количество человек	3	2	2	1	2
Коэффициент загрузки	0,8	0,7	0,9	0,9	0,8

Таблица 9 – Кадровый состав руководящих работников ООО «Континент»

Должность	Образование	Опыт работы
1. Генеральный директор	высшее	В течение 15 лет работал заместителем директора завода «Минеральные воды»
2. Главный бухгалтер	высшее	В течение 7 лет работал главным бухгалтером в оптовой фирме «Караван»
3. Заведующий складом	высшее	В течение 12 лет работал завскладом завода «Минеральные воды»

3) Провести оценку уровня экономической безопасности предприятия путем определения совокупного критерия экономической безопасности, рассчитываемого на основе мнений экспертов по частным функциональным критериям экономической безопасности по формуле:

$$СКЭБ = \sum K_i d_i$$

где K_i – значение частного функционального критерия экономической безопасности предприятия; d_i – коэффициент значимости функциональной составляющей экономической безопасности предприятия; n – количество составляющих. Результат оформить в форме таблицы 10.

Таблица 10 – Расчет совокупного критерия экономической безопасности ООО «Континент»

Функциональная составляющая (i)	Коэффициент весомости (d_i)	Экспертная оценка			Средняя оценка (K_i)	Взвешенная оценка ($K_i d_i$)
		Эксперт 1	Эксперт 2	Эксперт 3		
1. Финансовая	0,25					
2. Интеллектуально-кадровая	0,15					
3. Техничко-технологическая	0,20					
4. Политико-правовая	0,10					
5. Информационная	0,15					
6. Экологическая	0,05					
7. Силовая	0,10					
СКЭБ	1,0					

Оценка проводится тремя экспертами. При оценке используется 100-балльная шкала (0 – угроза экономической безопасности отсутствует, 25 – угроза, скорее всего, не реализуется, 50 – о наступлении события ничего сказать нельзя, 75 – угроза, скорее всего, проявится, 100 – угроза значительная, наверняка реализуется).

Практическое задание 2

Пользуясь учебной и справочной литературой, конспектами лекций, ответьте вопросы теста.

1. Под ЭБС предприятия понимается защищенность его производственного, технологического, кадрового и научно-технического потенциала от ... или ...экономических угроз.

- а) внешних и внутренних;
- б) активных и пассивных;
- в) прямых и косвенных;
- г) прямых (активных) и косвенных (пассивных).

2. Процесс предотвращения негативных воздействий на ЭБС предприятия за счет устранения рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом – ...

- а) управление безопасностью;
- б) кадровая безопасность;
- в) риск-менеджмент;
- г) фактор экономической безопасности.

3. По вероятности практической реализации выделяют угрозы:

- а) материального и нематериального характера;
- б) потенциальные, реализуемые, реализованные;
- в) информационной и имущественной безопасности.

4. На практике кадровая безопасность выражается ...

- а) устойчивым ростом основных показателей;
- б) устойчивым конкурентным преимуществом.
- в) степенью лояльности персонала;

5. Угроза кадровой безопасности – это ...

- а) намерение нанести какой-либо вред;
- б) возможность проявления негативного инцидента в будущем и размер последствий от него;

- в) предотвращение потенциальных угроз;
- г) анализ конкурентов.

6. Риск создания неблагоприятного имиджа организации на рынке входит в состав группы рисков кадровой безопасности при работе с персоналом ...

- а) на входе в организацию;
- б) внутри организации;
- в) на выходе из организации.

7. Риск финансовых претензий работника к организации входит в состав группы рисков кадровой безопасности при работе с персоналом ...

- а) на входе в организацию;
- б) внутри организации;

в) на выходе из организации.

8. *Субъект кадровой безопасности организации – это ...*

а) активный участник процессов в деятельности обеспечения кадровой безопасности, воздействующий на объект кадровой безопасности независимо от характера этого воздействия;

б) негативные внутренние риски компании и угрозы, связанные с деятельностью персонала;

в) сбор, анализ сведений из открытых источников для принятия решений о допуске к конфиденциальной информации, документам.

9. *Субъектами обеспечения кадровой безопасности организации не являются:*

а) менеджеры по персоналу;

б) менеджеры по безопасности;

в) охранники;

г) кандидаты на вакансии.

10. *Административно-независимая безопасность является элементом ...*

а) безопасности жизнедеятельности;

б) профессиональной безопасности;

в) социально-мотивационной безопасности;

г) антиконфликтной безопасности.

Практическое задание 3

Ответьте на вопросы для самоконтроля знаний:

1) Дайте определение кадровой безопасности, назовите ее цель и перечислите задачи.

2) Что называют кадровыми рисками и как их классифицируют?

3) Какие методы оценки кадровых рисков вам известны?

4) Перечислите и охарактеризуйте виды зависимостей.

5) Какие угрозы КБС создаются группами риска?

6) Как выявить сотрудника, принадлежащего к группе риска?

7) Назовите типы мошенничества и перечислите их признаки.

8) Перечислите и охарактеризуйте составляющие части КБС.

9) Какие требования предъявляют к менеджменту организации в ходе обеспечения КБС?

10) В чем сходство и различие кадровых рисков и кадровых угроз?

Методические материалы по практическому занятию 1

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 1: [1, с. 5–28, 2, 3, 4].

Тема 2. Система управления кадровой безопасностью в организации

Форма занятий – практическое занятие.

Цель занятия: закрепить общетеоретические знания о системе управления кадровой безопасностью современной организации как необходимом элементе комплексной системы безопасности, приобрести навыки и умения исследования ее состояния

Методические указания для подготовки к практическим занятиям по теме 2

Практическое задание 1

Сформулируйте положения по направлениям кадровой стратегии организаций-работодателей, способные оказать негативное влияние на их кадровую безопасность (КБС), заполнив для этого правую графу таблицы 11.

Таблица 11 – Негативное влияние кадровой стратегии на КБС

Направления кадровой стратегии	Недопустимые цели и приоритеты
Политика привлечения и сокращения персонала	
Политика реализации персонала	
Политика мотивации персонала	
Политика психологической поддержки персонала	

Практическое задание 2

Дать характеристику основных элементов стратегий управления кадровой безопасностью, проранжированных по степени их значимости. Задание выполнить путем заполнения таблицы 12.

Таблица 12 – Характеристика основных элементов СУКБС

Содержание стратегии	Стратегия упреждающего противодействия	Стратегия пассивной защиты от угроз	Стратегия адекватного ответа на угрозы
1. Принципы реализации			
2. Преимущества			
3. Недостатки			
4. Рекомендации по применению			

Практическое задание 3

Пользуясь учебной и справочной литературой, конспектами лекций, ответьте вопросы теста.

1. Обеспечение кадровой безопасности организации имеет целью...

- а) защиту персонала организации от возможных угроз;
- б) защиту организации от возможных угроз со стороны персонала;

в) как защиту персонала организации от возможных угроз, так и защиту организации от возможных угроз со стороны собственного персонала.

2. *Наиболее затратной из возможных стратегий обеспечения безопасности организации – работодателя выступает ...*

- а) стратегия упреждающего противодействия угрозам;
- б) стратегия адекватного ответа на угрозы;
- в) стратегия пассивной защиты от угроз.

3. *Наиболее распространенной из возможных стратегий обеспечения безопасности организации – работодателя выступает ...*

- а) стратегия упреждающего противодействия угрозам;
- б) стратегия адекватного ответа на угрозы;
- в) стратегия пассивной защиты от угроз.

4. *Основным недостатком стратегии упреждающего противодействия угрозам выступает ...*

- а) высокая ресурсоемкость;
- б) высокая вероятность конфликтов с законом;
- в) высокая вероятность конфликтов с конкурентами, клиентами, другими контактными аудиториями;
- г) высокая вероятность конфликтов с действующим законодательством, конкурентами и собственными сотрудниками.

5. *Структура системы управления кадровой безопасностью современной организации состоит из ... базовых элементов.*

- а) двух;
- б) трех;
- в) четырех;
- г) пяти

6. *К факторам, определяющим выбор варианта стратегии управления кадровой безопасностью не относится:*

- а) отрасль или сфера деятельности организации;
- б) степень агрессивности конкурентной стратегии организации;
- в) степень легитимности бизнеса организации;
- г) финансовые возможности конкурентов и контрагентов по обеспечению безопасности;
- д) квалификация персонала службы безопасности;
- е) наличие поддержки со стороны органов государственной власти.

7. *Один из вариантов стратегии обеспечения КБС организации, предполагающий приоритетную ориентацию на защиту со стороны государства в лице правоохранительных и судебных органов – ...*

- а) стратегия адекватного ответа на угрозы;
- б) стратегия пассивной защиты от угроз;
- в) стратегия упреждающего противодействия угрозам.

8. Совокупность долгосрочных целей и управленческих подходов, реализация которых обеспечивает защиту организации от любых потенциальных угроз, связанных с функционированием кадрового направления ее деятельности – ...

- а) стратегия управления кадровой безопасностью;
- б) операционные подсистемы;
- в) блок обеспечения.

9. Самостоятельные элементы системы управления, каждый из которых направлен на решение формализованного перечня однотипных задач по обеспечению кадровой безопасности организации -

- а) стратегия управления кадровой безопасностью;
- б) операционные подсистемы;
- в) блок обеспечения.

10. Система управления безопасностью современной организации по кадровому направлению ее деятельности должна включать в себя ...

- а) две операционные подсистемы;
- б) три операционные подсистемы;
- в) пять операционных подсистем.

Методические материалы по практическому занятию2

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 4: [1, с. 34–57, 2, 3, 4].

Тема 3. Технология обеспечения кадровой безопасности

Форма занятий – практическое занятие

Цель занятия: закрепление знаний об основах организации технологий обеспечения кадровой безопасности, получение умений и навыков осуществления мероприятий по обеспечению кадровой безопасности

Методические указания для подготовки к практическим занятиям по теме 3

Практическое задание 1

Напишите по одному из перечисленных ниже вопросов (по вариантам) небольшое эссе (объемом в 2–3 страницы):

1. Внутреннее нормативно-методическое обеспечение кадровой безопасности организации.

2. Роль руководителей структурных подразделений в обеспечении кадровой безопасности организации.

3. Проблемы кадрового обеспечения деятельности службы безопасности организации.

4. Проблемы финансового обеспечения кадровой безопасности организации.

5. Частные охранные предприятия и детективные агентства в современной России.

6. Взаимодействие службы безопасности и службы персонала.

7. Особенности организации службы безопасности в государственных учреждениях.

8. Особенности организации службы безопасности в малом предпринимательстве.

Практическое задание 2

Ответьте на вопросы для самоконтроля знаний:

1) Какие мероприятия в обеспечении кадровой безопасности организации при подборе и отборе персонала осуществляет СУП?

2) Перечислите и охарактеризуйте функции СБ при подборе и отборе персонала.

3) Какие основные законы входят в состав нормативно-правового обеспечения системы управления кадровой безопасностью?

4) Каковы условия безопасного для организации увольнения сотрудника?

5) Что такое лояльность сотрудника? Как она связана с благонадежностью?

6) Какой уровень лояльности персонала является необходимым для эффективности и безопасности функционирования организации?

7) Охарактеризуйте виды контроля персонала. Как и когда они реализуются?

Практическое задание 3

Пользуясь учебной и справочной литературой, конспектами лекций, ответьте вопросы теста.

1. *Кадровая безопасность зависит от трех основных факторов:*

а) наем, лояльность, контроль;

б) отбор, наем, лояльность;

в) наем, лояльность, увольнение.

2. *Комплекс мер безопасности при приеме на работу и прогнозирование благонадежности сотрудников – это ...*

а) наем;

б) лояльность;

в) контроль;

г) отбор.

3. *Конкурентная разведка – это метод ...*

- а) целенаправленного воздействия;
- б) тайного принуждения;
- в) информационно-психологического воздействия.

4. *Дискриминация – это метод ...*

- а) целенаправленного воздействия;
- б) тайного принуждения;
- в) информационно-психологического воздействия.

5. *Принятие, положительное отношение человека к чему-то конкретному – это ...*

- а) жизнеспособность организации;
- б) благонадежность сотрудника;
- в) лояльность сотрудника.

6. *Несоблюдение норм права, которое преследуется законом, и является результатом неблагонадежности сотрудника – это ...*

- а) делинквентное поведение;
- б) административно-управленческое деструктивное поведение;
- в) дисфункциональное поведение;
- г) эгоистическое, индивидуально-целевое деструктивное поведение;
- д) консервативное поведение;
- е) имитационное поведение;
- ж) девиантное поведение.

7. *Некомпетентность, несоответствие занимаемой должности – это ...*

- а) делинквентное поведение;
- б) административно-управленческое деструктивное поведение;
- в) дисфункциональное поведение;
- г) эгоистическое, индивидуально-целевое деструктивное поведение;
- д) консервативное поведение;
- е) имитационное поведение;
- ж) девиантное поведение.

8. *Скрытая (тайная) нелояльность имеет оценку:*

- а) -1; б) -2; в) 0; г) 1; д) 2; е) 3.

9. *Лояльность на уровне поступков и действий имеет оценку*

- а) -1; б) -2; в) 0; г) 1; д) 2; е) 3.

10. *С профессиональной компетентностью связана*

- а) скрытая (тайная) лояльность;
- б) демонстративная (открытая) лояльность;
- в) нулевая лояльность;
- г) лояльность на уровне поступков;
- д) лояльность на уровне действий;
- е) лояльность на уровне убеждений;

ж) лояльность на уровне внешних атрибутов.

Задание 3

Ознакомиться с порядком анализа результатов труда с помощью индивидуальной фотографии рабочего времени:

1. Заполнить наблюдательный лист для индивидуальной фотографии рабочего времени.

2. Составить сводку (группировку) одноименных затрат рабочего времени, оформив ее по форме таблицы 13.

3. Составить баланс затрат рабочего времени, оформив его по форме таблицы 13, с учетом того, что рабочий на 2 минуты опоздал с обеда.

4. Проанализировать затраты рабочего времени путем расчета соответствующих показателей.

Таблица 13 – Группировка одноименных затрат рабочего времени

№ п/п	Индекс категории затрат	Повторяемость затрат	Суммарная величина затрат, мин	В том числе перекрываемое время, мин.	Удельный вес затрат в общем времени наблюдения, %
	Тпз				
	Топ				
	Тобс				
	Тотд				
	Тпнт				
	Тпнд				
Итого					

Таблица 14 – Баланс затрат рабочего времени

№ п/п	Индекс категории затрат рабочего времени	Фактический баланс		Проектируемый баланс		Лишние затраты	
		мин.	%	мин.	%	мин.	%
1	Тпз						
2	Топ						
3	Тобс						
4	Тотд						
5	Тпнт						
6	Тпнд						
Итого							

Методические материалы по практическому заданию 3

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 5: [1, с. 257–291, 2, 3, 5, 6].

Тема 4. Противодействие угрозам безопасности персонала организации

Форма занятий—практическое занятие

Цель занятия: закрепить теоретические знания об основных угрозах безопасности сотрудников организации, их причинах и способах противодействия им

Методические указания для подготовки к практическим занятиям по теме 4

Практическое задание 1

Вставьте в пропуски номера приведенных внизу страницы слов и выражений, подходящих по смыслу:

Перечень вопросов:

- 1) Интенсивность конкуренции между работодателями зависит от двух факторов: () и ().
- 2) Объектами переманивания выступают: (), (), ().
- 3) К противоправным и недобросовестным действиям персонала предприятия относятся: (), (), ().
- 4) Имеются два подхода к переманиванию сотрудников конкурирующей организации: () и ().
- 5) Субъекты склонения сотрудников к нелояльному поведению могут быть () и ().
- 6) Вербовка сотрудников может быть осуществлена с помощью: (), (), ().
- 7) Выделяются три основные формы реализации устранения объекта угрозы: (), (), ().
- 8) Противодействие угрозам персоналу предполагает () и ().
- 9) Формами реализации угрозы переманивания сотрудников организации являются: (), (), ().
- 10) Внешними субъектами склонения сотрудников к нелояльному поведению считаются: (), (), (), ().
- 11) Выбор формы реализации угрозы устранения зависит от следующих факторов: (), (), ().
- 12) К внутренним субъектами склонения сотрудников к нелояльному поведению относятся: (), (), (), ().

Перечень ответов:

- 1) внутренние;
- 2) собственными силами;

- 3) открытое покушение;
- 4) шантаж;
- 5) профилактика угрозы;
- 6) менеджеры;
- 7) предложение лучших условий найма;
- 8) уровень квалификации работника;
- 9) государство;
- 10) имитация самоубийства;
- 11) мошенничество;
- 12) руководитель сотрудника – объекта угрозы;
- 13) внешние;
- 14) финансовые возможности заказчика;
- 15) прямые угрозы;
- 16) конкуренты;
- 17) ведущие специалисты;
- 18) подчиненный сотрудника–объекта угрозы;
- 19) эффективность организации защиты объекта;
- 20) незаконные сделки;
- 21) предложение о решении жизненно важной проблемы;
- 22) работники подконтрольных сотруднику подразделений;
- 23) с использованием услуг специализированных посредников;
- 24) профессионализм исполнителя заказа;
- 25) подкуп;
- 26) пресечение угрозы;
- 27) степень дефицитности специальности;
- 28) криминальные структуры;
- 29) скрытое покушение;
- 30) высококвалифицированные работники;
- 31) коллеги по работе;
- 32) «игра» на недовольстве работодателем;
- 33) индивидуально действующие злоумышленники;
- 34) недобросовестная конкуренция;
- 35) шантаж.

Практическое задание 2

Пользуясь учебной и справочной литературой, конспектами лекций, ответьте вопросы теста.

1. В настоящее время наблюдается наличие ... полярных подходов к организации противодействия кадровым угрозам безопасности организации.

- а) двух;
- б) трех;
- в) четырех;
- г) пяти

2. *Совокупность мер по обеспечению защиты сотрудников от потенциальных угроз в форме переманивания конкурентами, вербовки, шантажа, прямых угроз жизни и здоровью, покушений.*

- а) кадровая безопасность;
- в) безопасность организации;
- б) безопасность персонала;
- г) экономическая безопасность.

3. *Наиболее распространенной угрозой в адрес персонала организации выступает...*

- а) переманивание ведущих сотрудников организации конкурентами;
- б) вербовка сотрудников организации;
- в) покушения на руководителей организации.

4. *При переманивании персонала организация-работодатель преследует следующие цели:*

- а) усиление собственных конкурентных позиций за счет улучшения экономических или социальных условий найма;
- б) усиление собственных конкурентных позиций за счет улучшения психологического климата в организации;
- в) усиление собственных конкурентных позиций за счет улучшения качества своего человеческого капитала;
- г) усиление собственных конкурентных позиций за счет собственного профессионального и карьерного роста;
- д) ослабление позиций конкурентов за счет ухудшения качества их человеческого капитала.

5. *Субъектами переманивания сотрудников коммерческой организации выступают:*

- а) подведомственные структуры;
- б) подконтрольные структуры;
- в) коммерческие структуры;
- г) организации-конкуренты.

6. *Основная причина успешной реализации угрозы переманивания – ...*

- а) удовлетворенность переманиваемого сотрудника;
- б) страх переманиваемого сотрудника;
- в) недовольство переманиваемого сотрудника;
- г) жажда наживы переманиваемого сотрудника.

7. Наиболее эффективной группой методов противодействия угрозам кадровой безопасности организации являются ...

- а) профилактические методы;
- б) пресекающие методы;
- в) репрессивные методы.

8. В условиях рыночной экономики прямое переманивание сотрудников конкурирующей организации рассматривается как метод ...

- а) недобросовестной конкуренции;
- б) типовое проявление закона конкуренции на рынке труда,
- в) противоречащий действующему законодательству.

9. Переманивание ведущих менеджеров и специалистов конкурирующей организации в современных условиях чаще осуществляется путем ...

- а) прямых предложений о смене работодателя со стороны представителей конкурирующей организации;
- б) использование посреднических услуг специализированных рекрутинговых агентств,
- в) использования средств массовой информации.

10. Профилактика угроз переманивания сотрудников организации ее конкурентами обеспечивается в рамках.

- а) системы персонального менеджмента;
- б) реализации активной социальной политики;
- в) системы менеджмента безопасности;
- г) системы кадрового менеджмента.

Методические материалы по практическому занятию4

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 5: [1, с. 107–157, 2, 3, 4, 6].

Тема 5. Противодействие угрозам информационной безопасности организации со стороны собственного персонала

Форма занятий – практическое занятие

Цель занятия: закрепление теоретических знаний о проблемах обеспечения информационной безопасности в деятельности современной организации, об угрозах и методах противодействия им во взаимосвязи с кадровым аспектом работы.

Методические указания для подготовки к практическим занятиям по теме 5

Практическое задание 1

Провести систематизацию сведений, содержащихся в приведенном ниже перечне, по степени их конфиденциальности, занести в таблицу 15.

Перечень конфиденциальных сведений:

- 1) сведения из личных дел сотрудников;
- 2) информация о движении средств по счетам организации;
- 3) информация о клиентах организации, переданная на доверительной основе
- 4) информация о перспективных научно-технических разработках;
- 5) сведения о применяющихся организацией авторских технологиях внутрифирменного менеджмента;
- 6) сведения о готовящихся к заключению контрактах;
- 7) информация о результатах маркетингового мониторинга обслуживаемого организацией рынка;
- 8) информация о системах защитной сигнализации;
- 9) внутренняя служебная переписка организации;
- 10) информация о численности сотрудников конкретных подразделений;
- 11) информация о планируемых на следующий квартал финансовых показателях деятельности организации;
- 12) информация об изменениях в ассортиментной и нишевой политике организации;
- 13) информация об объемах товарных запасов на складе организации.

Таблица 15 – Перечень конфиденциальных сведений организации

Гриф конфиденциальности	Сведения
Абсолютно конфиденциально	
Строго конфиденциально	
Конфиденциально	
Для служебного пользования	

Практическое задание 2

Вставьте в пропуски номера приведенных внизу страницы слов и выражений, подходящих по смыслу:

Перечень вопросов:

- 1) Существуют две типовые первопричины реализации угроз ИБС организации со стороны ее персонала: () и ().
- 2) Защита информации должна обеспечиваться соблюдением: (), (), ().
- 3) Субъектами угроз ИБС организации являются: (), (), (), (), ().
- 4) Организация работы по противодействию угрозам ИБС включает этапы: (), (), (), ().
- 5) Методы защиты информации делятся на следующие группы: (), ().

6) В существующей коммерческой практике выделяют следующие формы угроз ИБС организации: (), (), (), ().

7) Конфиденциальная информация предприятия может быть представлена данными следующего вида: (), (), ().

8) Субъектами контроля над сотрудниками организации служат () и ().

9) Конфиденциальные сведения включают: (), (), ().

10) Для эффективной подготовки сотрудников используется дифференциация сотрудников по двум категориям: (), ().

11) Управление персоналом включает: (), (), ().

Перечень ответов:

- 1) злой умысел;
- 2) базы данных;
- 3) перехват;
- 4) технического характера;
- 5) конкуренты;
- 6) контроль соблюдения сотрудниками правил обеспечения ИБС;
- 7) конфиденциальность;
- 8) служба безопасности;
- 9) в электронном виде;
- 10) программно-математического характера;
- 11) хищение;
- 12) молодые специалисты;
- 13) нелояльные сотрудники;
- 14) обучение сотрудников правилам обеспечения ИБС;
- 15) формирование ранжированного перечня конфиденциальных сведений и присвоение им соответствующего грифа;
- 16) государство;
- 17) мотивация сотрудников организации в целях обеспечения ИБС;
- 18) на бумажных носителях;
- 19) криминальные структуры;
- 20) повреждение;
- 21) целостность;
- 22) сотрудники, имеющие опыт работы;
- 23) оценка возможных каналов утечки информации;
- 24) сведения о заработной плате сотрудников, а также о составе «резерва на выдвижение»;
- 25) руководители структурных подразделений;
- 26) организационного характера;
- 27) определение перечня прикладных методов защиты информации;

- 28) индивидуальные злоумышленники;
- 29) искажение;
- 30) безответственность;
- 31) внутренние регламенты;
- 32) в устном виде;
- 33) доступность;
- 34) непосредственное формирование и внедрение подсистемы ИБС.

Практическое задание 3

Пользуясь учебной и справочной литературой, конспектами лекций, ответьте вопросы теста.

1. *Наибольшую опасность с позиции современной организации представляет разглашение конфиденциальной информации ...*

- а) о деятельности самой организации;
- б) о деятельности клиентов и партнеров организации,
- в) вопрос не корректен, приоритета не выделяется.

2. *Разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести имущественный или неимущественный ущерб ее клиентам или партнерам по хозяйственной деятельности - ...*

- а) коммерческая тайна;
- б) клиентская тайна;
- в) служебная тайна;
- г) предпринимательская тайна.

3. *Работодатель ... самостоятельно определять, какая именно информация является для него настолько значимой, что для обеспечения ее сохранности необходимо предпринять ряд мер ее по охране.*

- а) вправе;
- в) не вправе.

4. *В современных условиях наиболее опасной для организации угрозой со стороны ее собственного персонала является ...*

- а) коррупция;
- б) растраты и хищения денежных средств работодателя;
- в) разглашение конфиденциальной информации.

5. *В результате перехвата конфиденциальной информации у субъекта угрозы ...*

- а) оказывается ее дубликат;
- б) не остается ее дубликата

6. Повреждение или уничтожение конфиденциальной информации имеет своей задачей ...

- а) получение дубликата информации организации;
- б) нанесение ущерба организации;
- в) лишение пострадавшей организации информации;
- г) принятие организацией ошибочного решения.

7. В современных условиях наиболее вероятна утечка конфиденциальной информации ...

- а) на электронных носителях;
- б) на бумажных носителях;
- в) в устной форме.

8. В отечественных условиях более вероятной причиной утечки конфиденциальной информации по вине сотрудников является ...

- а) осознанная нелояльность работодателю;
- б) безответственность виновного сотрудника,
- в) неэффективная защита информации самим работодателем.

9. Методы реализации угроз информационной безопасности классифицируются по следующим признакам:

- а) в зависимости от степени ответственности сотрудников;
- б) в зависимости от объекта угрозы;
- в) в зависимости от субъекта угрозы;
- г) в зависимости от вида данных, являющихся объектом угрозы.

10. Организация работы по противодействию угрозам информационной безопасности осуществляется в ... этапа:

- а) два;
- б) три;
- в) четыре;
- г) пять;
- д) шесть.

Методические материалы по практическому занятию 5

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 6: [1, с. 158–207, 2, 3, 6].

Тема 6. Противодействие угрозам имущественной безопасности организации

Форма занятий – практическое занятие

Цель занятия: закрепление теоретических знаний о проблемах обеспечения информационной безопасности в деятельности современной организации, об угрозах и методах противодействия им во взаимосвязи с кадровым аспектом работы.

Методические указания для подготовки к практическим занятиям по теме 6

Практическое задание 1

Сформулировать ранжированный по степени вероятности перечень основных угроз имущественной безопасности организации со стороны ее сотрудников, заполнив для этого приведенную ниже таблицу 16.

Таблица 16 – Перечень основных угроз имущественной безопасности организации

Отрасли	Типовые угрозы
Реальный сектор экономики	
Финансовый сектор экономики	
Торговля и сфера услуг	

Практическое задание 2

Определить санкции за нарушения конкретным сотрудником правил обеспечения имущественной безопасности работодателя, заполнив для этого правую графу таблицы 17.

Таблица 17 – Санкции за нарушение правил имущественной безопасности

Нарушение	Санкции
Небрежное отношение к имуществу работодателя, повлекшее за собою нанесение мелкого ущерба	
Сознательное повреждение имущества работодателя	
Мелкое хищение имущества работодателя	
Хищения денежных средств в особо крупных размерах	

Практическое задание 3

Пользуясь учебной и справочной литературой, конспектами лекций, ответьте вопросы теста.

1. *Имущественный комплекс, используемый собственниками этого имущества для осуществления предпринимательской деятельности - ...*

- а) организация;
- б) предприятие;
- в) институциональная единица;
- г) хозяйствующий субъект.

2. Внеоборотные активы предприятия ...

- б) имеют срок использования более 1 года;
- в) сразу переносят свою стоимость на продукцию;
- г) потребляются в течение 1 цикла;
- д) имеют срок использования менее 1 года;

3. Каждый элемент актива и пассива называется ...баланса.

- а) валютой;
- б) разделом;
- в) статьей.

4. Наиболее ценным элементом имущества организации, являющимся приоритетным объектом защиты от нелояльных сотрудников, выступают ...

- а) денежные средства в кассе;
- б) основное производственное оборудование;
- в) любые высоколиквидные активы;
- г) конфиденциальная информация.

5. В современных отечественных условиях наиболее вероятна такая угроза имущественной безопасности со стороны собственных сотрудников организации как ...

- а) хищение денежных средств;
- в) саботаж;
- б) мелкие хищения ТМЦ;
- г) перехват собственности.

6. Большинство реализованных угроз имущественной безопасности со стороны собственных сотрудников организации определяет ...

- а) их собственный злой умысел;
- б) их безответственность;
- в) влияние со стороны конкурентов;
- г) влияние со стороны криминала.

7. В отношении денежных средств организации могут быть реализованы следующие методы:

- а) хищения в ненасильственной форме;
- б) хищения в насильственной форме
- в) перехват прав собственности;
- г) хищение путем фальсификации финансовых документов;
- д) повреждение и уничтожение.

8. К методам реализации угроз в отношении имущества организации не относятся:

- а) хищения в насильственной форме
- б) перехват прав собственности;

- в) хищение путем фальсификации финансовых документов;
- г) повреждение и уничтожение;
- д) хищения с использованием информационных технологий.

9. *Мелкие хищения товарно-материальных ценностей, принадлежащих работодателю, обычно совершаются его сотрудниками, действующими ...*

- а) в индивидуальном порядке;
- б) в сговоре с коллегами по работе;
- в) в сговоре со сторонними для организации гражданами.

10. *Хищения высоколиквидных активов, принадлежащих работодателю, обычно совершается его сотрудниками, действующими ...*

- а) в индивидуальном порядке;
- б) в сговоре с коллегами по работе;
- в) в сговоре со сторонними для организации гражданами.

Методические материалы по практическому занятию 6

ФОС по дисциплине, конспект лекций в ЭИОС по соответствующей теме.

Ссылки на рекомендуемые источники по теме 7: [1, с. 207–256, 2, 3, 5].

3 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПОДГОТОВКЕ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация по дисциплине «Кадровая безопасность» проводится в форме экзамена.

К экзамену допускаются студенты, получившие положительную оценку по результатам выполнения практических работ.

Для сдачи экзамена студентам необходимо освоить учебный материал по дисциплине в соответствии со структурой, приведенной в первом разделе настоящего учебно-методического пособия.

Экзаменационные задания по дисциплине представлены в виде тестов, критерии оценки которых указаны во Введении.

Примерный перечень тестовых заданий промежуточного контроля представлен ниже.

Примерный перечень тестовых заданий

Тестовые задания открытого типа

1. *Активный участник процессов в деятельности обеспечения кадровой безопасности, воздействующий на объект кадровой безопасности независимо*

от характера этого воздействия (наносящего ущерб, разрушение, или противоречащего этому) – _____.

2. Процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет устранения рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом _____.

3. Специализированное структурное подразделение организации, созданное для обеспечения ее защиты от возможных угроз _____.

4. Главным методическим требованием к системе управления кадровой безопасностью выступает _____ подход.

5. Работник организации, способный либо в собственных имущественных или неимущественных интересах, либо в силу общей безответственности нарушить доверие работодателя и нанести ущерб его безопасности – _____ сотрудник.

6. Информация, доступ к которой ограничивается в целях защиты коммерческой или клиентской тайны, а также другие сведения, разглашение которых по каким-либо причинам нежелательно для конкретной организации – _____.

7. Разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести ей имущественный или неимущественный ущерб как хозяйствующему субъекту – это _____ тайна.

8. Разновидность конфиденциальной информации, находящейся в распоряжении организации, разглашение которой способно нанести имущественный или неимущественный ущерб ее клиентам или партнерам по хозяйственной деятельности – это _____ тайна.

9. Первопричинами реализации угроз информационной безопасности организации со стороны ее персонала является _____ сотрудников.

10. Специальная отметка на конфиденциальных документах (базах данных), определяющая степень защиты содержащихся в них сведений _____.

11. Установленное режимом безопасности организации для конкретного сотрудника, клиента, пользователя право доступа в защищенные от несанкционированного проникновения компьютерные сети и базы данных, входа в охраняемые помещения, работы с конфиденциальными документами – _____.

12. Действия (умышленные или неосторожные) сотрудников предприятия, влекущие нанесение ущерба – это ... _____.

13. Действия, явления или процессы, НЕ зависящие от воли и сознания сотрудников предприятия и влекущие нанесение ущерба – _____.

14. Совокупность мер по обеспечению защиты имущества от угрозы насильственного и ненасильственного хищения, а также повреждения или уничтожения _____.

15. На практике кадровая безопасность выражается в степени _____ персонала.

16. Вероятность наступления неблагоприятных событий реализации угроз, исходящих от людей, в результате принятия решений _____.

17. Совокупность долгосрочных целей и управленческих подходов, реализация которых обеспечивает защиту организации от любых потенциальных угроз, связанных с функционированием кадрового направления ее деятельности – это _____.

18. При противодействии угрозе покушения на высших должностных лиц организации следует однозначный приоритет методов _____.

19. Взаимное приспособление работника и организации, основывающееся на постепенной вработываемости сотрудника в новых профессиональных, социальных и организационно-экономических условий труда _____.

20. Основным объектом угроз имущественной безопасности организации являются _____.

21. Умышленное повреждение или уничтожение имущества организации – это _____.

22. Имущественный комплекс, используемый собственниками этого имущества для осуществления предпринимательской деятельности - _____.

Тестовые задания закрытого типа

23. Из представленного ниже перечня к функциональным составляющим экономической безопасности относятся:

- 1) финансовая;
- 2) интеллектуальная и кадровая;
- 3) ресурсная;
- 4) энергетическая.

24. Из представленного ниже перечня к функциональным составляющим экономической безопасности НЕ относятся:

- 1) технико-технологическая;
- 2) пожарная;
- 3) закупочно-сбытовая;
- 4) информационная.

25. Конфиденциальная информация делится на следующие две категории:

- 1) информация, составляющая коммерческую тайну;
- 2) информация, составляющая клиентскую тайну;
- 3) информация, составляющая технологическую тайну;
- 4) информация, составляющую контрагентскую тайну.

26. Перечень прикладных методов защиты информации включает методы:

- 1) программно-целевого характера;
- 2) технического характера;
- 3) организационного характера;
- 4) мотивационного характера.

27. Установите соответствие:

1	Один из вариантов стратегии обеспечения кадровой безопасности организации, предполагающий возможность использования наиболее активных и не всегда легитимных методов профилактики и противодействия возможным угрозам	а	Стратегия адекватного ответа на угрозы
2	Один из вариантов стратегии обеспечения кадровой безопасности организации, предполагающий приоритетную ориентацию на защиту со стороны государства в лице правоохранительных и судебных органов	б	Стратегия пассивной защиты от угроз
3	Один из вариантов стратегии обеспечения КБС организации, предполагающий возможность использования всего комплекса легитимных методов профилактики и отражения потенциальных угроз	в	Стратегия упреждающего противодействия угрозам
		г	Стратегия точечного воздействия на угрозы

28. Структура системы управления кадровой безопасностью включает три элемента:

- 1) контроль персонала;
- 2) стратегия управления кадровой безопасностью;
- 3) блок обеспечения кадровой безопасности;
- 4) операционные подсистемы.

29. Основной причиной успешной реализации угрозы переманивания является... :

- 1) недовольство переманиваемого сотрудника;
- 2) удовлетворенность переманиваемого сотрудника;
- 3) страх переманиваемого сотрудника;
- 4) жажда наживы переманиваемого сотрудника.

30. Определите правильную последовательность этапов противодействия угрозам информационной безопасности:

1) Формирование ранжированного перечня конфиденциальных сведений организации как объекта защиты и присвоение им соответствующего грифа секретности.

2) Оценка возможных каналов утечки (перехвата) конфиденциальной информации;

3) Определение перечня прикладных методов защиты информации;

4) Непосредственное формирование и внедрение подсистемы информационной безопасности.

Экзамен по дисциплине «Кадровая безопасность» может проводиться и в устной форме. В этом случае на экзамене студент, опираясь на изученный материал, должен дать ответ на контрольные вопросы по дисциплине, приведенные ниже.

Экзаменационная оценка («отлично», «хорошо», «удовлетворительно» или «неудовлетворительно») зависит от уровня освоения студентом тем дисциплины (наличия и сущности ошибок, допущенных при ответе):

«Отлично» – выставляется в случаях полного и четкого ответа на два теоретических вопроса и дополнительные вопросы по изученной дисциплине;

«Хорошо» – выставляется в случаях полного и четкого ответа на два теоретических вопроса и незначительных, не принципиальных погрешностях при ответах на дополнительные вопросы;

«Удовлетворительно» – при правильных ответах на теоретические вопросы. Допускаются не принципиальные погрешности или незначительная незавершенность ответов, диктуемая лимитом времени, а также незначительные замечания и неточности. Не менее 50 % основных положений вопросов должны быть раскрыты студентом полностью;

«Неудовлетворительно» – выставляется при ответах, не удовлетворяющих критериям, указанным в предыдущих пунктах.

Контрольные вопросы по дисциплине

1) Сущность понятия «кадровая безопасность» и ее место в системе ЭБС предприятия.

2) Субъекты, объекты и факторы кадровой безопасности

3) Структура кадровой безопасности организации

4) Кадровые риски: понятия и факторы формирования

5) Угрозы кадровой безопасности. Характеристика угроз по источнику формирования

6) Угрозы кадровой безопасности. Характеристика угроз по субъекту и вероятности реализации

- 7) Типы противоправного поведения сотрудников.
- 8) Виды зависимостей сотрудников и основные группы риска.
- 9) Девиантное поведение. Треугольник мошенничества. Типы мошенничества
- 10) Характеристика видов мошенничества в зависимости от характера совершаемых действий.
- 11) Контроль персонала на стадии найма
- 12) Контроль персонала в процессе трудовой деятельности
- 13) Структура системы управления кадровой БС: стратегия управления.
- 14) Принципы формирования СУ КБ. Операционные подсистемы.
- 15) Структура системы управления кадровой БС: блок обеспечения.
- 16) Субъекты управления КБ. Подходы к формированию СБ.
- 17) Служба безопасности организации и ее функции в рамках кадровой подсистемы системы ЭБС.
- 18) Методические принципы системы управления кадровой БС.
- 19) Деятельность на этапе проверки кандидата и приема его на работу в ходе найма
- 20) Мероприятия на этапе осуществления работником своей основной профессиональной деятельности
- 21) Обеспечение корпоративной безопасности на этапе увольнения работника
- 22) Лояльность сотрудника: связь с понятиями «преданность» и «благонадежность»
- 23) Уровни лояльности персонала
- 24) Повышение лояльности в организации
- 25) Контроль персонала – направления и формы
- 26) Специфика контроля за проблемным персоналом
- 27) Угроза переманивания сотрудников организации: факторы, субъекты, объекты, формы реализации, причины.
- 28) Угроза склонения сотрудников к нелояльному поведению в отношении работодателя: субъекты, объекты, формы реализации.
- 29) Угроза склонения сотрудников к нелояльному поведению в отношении работодателя: инструмент и организация противодействия.
- 30) Угроза покушений на собственников и топ-менеджеров организации: причины, субъекты, объекты, формы реализации.
- 31) Угроза покушений на собственников и топ-менеджеров организации: факторы, организация противодействия.
- 32) Конфиденциальная информация как объект защиты.

- 33) Угроза информационной безопасности организации с участием персонала: причины, субъекты, формы угроз.
- 34) Методы реализации угроз информационной безопасности.
- 35) Противодействие угрозам информационной БС: формирование ранжированного перечня конфиденциальных сведений и оценка возможных каналов утечки.
- 36) Противодействие угрозам информационной БС: определение перечня прикладных методов защиты; формирование и внедрение подсистемы информационной безопасности организации.
- 37) Обучение сотрудников организации правилам обеспечения информационной безопасности.
- 38) Контроль соблюдения сотрудниками правил обеспечения информационной безопасности организации.
- 39) Мотивация сотрудников организации в целях обеспечения информационной безопасности.
- 40) Имущество организации как объект защиты.
- 41) Реализация угроз имущественной БС организации с участием персонала.
- 42) Противодействие угрозам имущественной БС организации со стороны ее персонала.
- 43) Управление персоналом организации в целях обеспечения ее имущественной безопасности.

4 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

Освоение дисциплины студентами осуществляется в ходе посещения лекционных и практических занятий под руководством преподавателя. Однако, большая часть освоения дисциплины осуществляется студентами самостоятельно. Поэтому самостоятельная работа студента (СРС) является ключевой составляющей учебного процесса, которая определяет формирование навыков, умений и знаний, приемов познавательной деятельности и обеспечивает интерес к творческой работе.

Целью самостоятельной работы является освоение студентами фундаментальных знаний, опыта практической деятельности по профессии. Самостоятельная работа должна способствовать развитию ответственности и

организованности, а также творческого подхода к решению нестандартных задач. Самостоятельная работа студентов предполагает многообразные виды индивидуальной и коллективной деятельности студентов, осуществляемые под руководством, но без непосредственного участия преподавателя в специально отведенное для этого аудиторное и внеаудиторное время.

Самостоятельная работа студентов по данной дисциплине включает:

- 1) конспектирование лекций, изучение предыдущего материала и подготовка к очередной лекции (форма контроля – отчёт о практических занятиях по соответствующей теме);
- 2) то же для практического занятия (форма контроля – отчёт о практических занятиях по соответствующей теме);
- 3) подготовку к сдаче экзамена (форма контроля – экзамен).

Помимо этого, самостоятельная работа студента включает работу с учебниками, иной учебной и учебно-методической литературой, а также с законодательными и нормативными актами РФ по соответствующим темам курса, реферирование литературы, аннотирование книг, статей, выполнение заданий поисково-исследовательского характера.

СПИСОК ЛИТЕРАТУРЫ

Основная учебная литература

1. Алавердов, А. Р. Управление кадровой безопасностью организации: учебник / А. Р. Алавердов. – 2-е изд., доп. и перераб. – Москва: Университет Синергия, 2020. – 460 с.
2. Андруник, А. П. Кадровая безопасность: инновационные технологии управления персоналом: учеб. пособие / А. П. Андруник, М. Н. Руденко, А. Е. Суглобов. – 4-е изд. – Москва: Дашков и К°, 2024. – 508 с.
3. Управление кадровой безопасностью организации: учебник для бакалавриата и магистратуры / Ю. В. Долженкова, Е. В. Камнева, А. Л. Сафонов [и др.]; под ред. Ю. В. Долженковой; Финансовый университет при Правительстве Российской Федерации. – Москва: Прометей, 2022. – 286 с.

Дополнительная учебная литература

4. Лукаш, Ю. А. Эффективная кадровая политика как составляющая обеспечения безопасности и развития бизнеса: учеб. пособие / Ю. А. Лукаш. – 3-е изд., стер. – Москва: ФЛИНТА, 2024. – 202 с.
5. Лукаш, Ю. А. Контроль персонала как составляющая безопасности и развития бизнеса: учеб. пособие / Ю. А. Лукаш. – 3-е изд., стер. – Москва: ФЛИНТА, 2024. – 24 с.
6. Лукаш, Ю. А. Профилактика конфликтов и иных негативных проявлений со стороны персонала как составляющая обеспечения безопасности и развития бизнеса: учеб. пособие / Ю. А. Лукаш. – 3-е изд., стер. – Москва: ФЛИНТА, 2024. – 70 с.

Локальный электронный методический материал

Алла Евгеньевна Тарутина

КАДРОВАЯ БЕЗОПАСНОСТЬ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 4,5. Печ. л. 3,8.

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1