Министерство и науки высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

УТВЕРЖДАЮ
Ректор КузГТУ
Яковлев А.Н.
29.08.2022г.

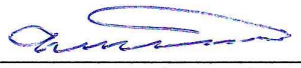
Рабочая программа дисциплины (модуля)
Корпоративная безопасность
(наименование дисциплины(модуля))

Дополнительная профессиональная программа
программа профессиональной переподготовки
Менеджмент В
(наименование дополнительной профессиональной программы)

Форма(ы) обучения очно-заочная

Кемерово 2022

Рабочую программу дисциплины (модуля) составил:



Зникин В.К.

(должность, структурное подразделение) *(подпись)* *(ФИО)*

Рабочая программа дисциплины(модуля) обсуждена на заседании *методической комиссии дополнительного профессионального образования*

Протокол № 1 от 29.08.2022

Руководитель структурного подразделения  Т.Г. Королёва

(подпись)

1. Объем дисциплины (модуля) с указанием количества академических часов, выделенных на контактную работу обучающихся с педагогическим работником (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины (модуля) составляет 24 академических часов.

Виды учебных занятий	Количество часов		
	ОФ	ЗФ	ОЗФ
Контактная работа по видам учебных занятий, в т.ч.			**14**
электронное обучение, дистанционные образовательные технологии			*0*
Самостоятельная работа, в т.ч.			**10**
электронное обучение, дистанционные образовательные технологии			*0*
Форма промежуточной аттестации	**зачет**		

2. Содержание дисциплины (модуля), структурированное по разделам (темам)

Тематика	Контакт. раб.	Самост. раб.	из гр. 2 и гр. 3 активные методы обучения
1	**2**	**3**	**4**
Общие положения теории безопасности	2	2	1 Проблемная лекция
Сущность и система экономической безопасности компании	4	2	2 Деловая игра 2 Лекция-визуализация
Деловая разведка и контрразведка	4	2	2 Мозговой штурм 2 Лекция-беседа
Основы личной безопасности	2	2	1 Проблемная лекция 1 Деловая игра
Риски в бизнесе	2	2	1 Проблемная лекция 1 Тренинг
Итого	14	10	12

3. Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования профессиональных компетенций в результате освоения дополнительной профессиональной программы

ПК-1	Способность управлять организациями, подразделениями, группами (командами) сотрудников, проектами и сетями
ПК-5	Владение методами экономического и стратегического анализа поведения экономических агентов и рынков в глобальной среде
СК-1	Способность к выстраиванию каналов коммуникаций в различных условиях
ЦК-1	Способность к использованию умных сред, средств сетевой коммуникации, виртуальной и дополненной реальности, автоматизированных систем управления и машинного обучения, технологий робототехники и искусственного интеллекта
ЦК-4	Способность организовывать систему информационной безопасности при использовании сетевых решений, при поиске и проверке информации, обеспечивать сохранность персональных данных и данных организации (компании).

Индикаторы достижения компетенции

№	Состав промежут. аттестации	Код компетенции	Индикаторы достижения компетенции			
			Знает	**Умеет**	**Имеет опыт и (или) навык и (или) владеет**	**Уровень**
1.	Собеседование	ПК-1	основные понятия и теоретические положения о необходимых составляющих безопасности бизнеса			Высокий Средний
2.	Собеседование	ПК-5	новейшие публикациями по актуальным проблемам корпоративной безопасности			Высокий Средний
3.	Собеседование Решение кейса	СК-1	специфические особенности организации корпоративной безопасности	самостоятельно ставить задачи по безопасности бизнеса работников компании, находя адекватные методы их решения		Высокий Средний
4.	Собеседование Решение кейса	ЦК-1	особенности преодоления существующих угроз бизнеса на основе современных подходов к формированию системы безопасности компании;		реализовывать специальные знания (умение защитить, скрыть и хранить секреты компании; умение вступать в контакт с внешним миром и скрывать свои контакты) с использованием умных сред, средств сетевой коммуникации, виртуальной и дополненной реальности, автоматизированных систем управления и машинного обучения, технологий робототехники и искусственного интеллекта	Высокий Средний
5.	Решение кейса	ЦК-4			применять полученные теоретические знания на практике в процессе управления системами информационной безопасности компании при использовании сетевых решений, при поиске и проверке информации, обеспечивать сохранность персональных данных и данных организации (компании).	Высокий Средний

Высокий уровень *– компетенция сформирована, рекомендованные оценки: отлично, хорошо.*
Средний уровень *– компетенция сформирована, рекомендованные оценки: удовлетворительно.*
Низкий уровень *– компетенция не сформирована, оценивается неудовлетворительно.*

4. Оценочные средства, используемые для проведения процедуры промежуточной аттестации обучающихся.

В ходе промежуточной аттестации обучающиеся устанавливается уровень сформированности компетенций по дисциплине. Промежуточная аттестация включает:

- процедуру собеседования;
- решение кейсов.

Промежуточная аттестация обучающиеся проводится с использованием системы Moodle ЭИОС КузГТУ. Полный комплект оценочных материалов (вопросов для собеседования), используемый при проведении процедуры промежуточной аттестации обучающихся, размещён в ЭИОС КузГТУ.

Доступ к оценочным материалам обучающимся предоставляет педагогический работник в авторизованном доступе перед началом процедуры промежуточной аттестации.

4.1. Примеры оценочных материалов с указанием шкалы оценивания.

4.1.1. Вопросы для собеседования

1. Что такое корпоративная безопасность и ее отличие от безопасности корпорации?
2. Что понимается под безопасностью вообще и безопасностью бизнеса?
3. Как соотносятся?
4. Как оценить уровень корпоративной безопасности? Приведите примеры положительных и негативных индикаторов конкретных состояний безопасности бизнеса.
5. Почему некоторые инструменты обеспечения корпоративной безопасности не работают? Что необходимо сделать для изменения ситуации в компании?
6. Что такое внутри объектовый режим безопасности компании и как он функционирует?
7. Какие существуют барьеры для совершенствования корпоративной безопасности?
8. Что значит – подготовиться к безопасным переговорам?
9. Какова особенность ведения переговоров по телефону?
10. Приведите некоторые примеры толкования жестов и поз при переговорах, излучающих вероятные угрозы.
11. Как не спровоцировать партнера на необдуманные и нежелательные действия?
12. Культурологические и коммуникативные особенности ведения безопасных переговоров с иностранными партнерами.
13. Какие есть типы вопросов? Как можно повлиять их постановкой на течение переговорного процесса?
14. Как защитить свои секреты?
15. Как вступать в контакт с внешним миром?
16. Как скрыть свои контакты?
17. Как защитить свои планы?
18. Как контролировать компьютер?
19. Как идентифицировать риски?
20. Каковы основные методы управления предпринимательскими рисками?
21. Назовите физическую природу возникновения технических каналов утечки информации;
22. Назовите методы и средства защиты информации;
23. Назовите структуру и задачи федеральных органов, ответственных за обеспечение и организацию работ в области технической защиты информации;

4.1.2. Пример кейса

Автотехцентр производит все виды технического обслуживания по автомобилям класса люкс.

Для обеспечения качественного оказания услуг руководство автотехцентра постоянно поддерживает достаточное количество запасных частей и принадлежностей на внутреннем складе на территории автотехцентра.
Стоимость этих запчастей высока, поэтому хищения со склада могут привести к значительным убыткам для компании.
Директором организации был обнаружен товар, хранящийся в несанкционированном месте склада и явно предназначенный к выносу.
Количество сотрудников автотехцентра, имеющих доступ на территорию склада – 15 человек.
Территория автотехцентра оборудована системой видеонаблюдения, но качество получаемого изображения и маленький срок хранения видеоархива не позволяет использовать данные системы видеонаблюдения для проведения расследования.
Объект оборудован системой контроля и управления доступом по отпечаткам пальцев.
Задача:
1. Описать основные этапы проведения расследования описанного случая подготовки хищения. Обосновать возможность использования в расследовании информации об отпечатках пальцев, имеющейся в СКУД.
2. Описать основные этапы разработки системы предотвращения хищений для данного случая.
Описание решения кейса:
1. Необходимо установить время поставки указанного товара на склад и временной интервал хранения на складе.
2. Необходимо установить круг лиц, потенциально имевших доступ к товару.
3. Произвести опросы подозреваемых и возможных свидетелей.
4. На основании опросов уточнить круг подозреваемых
5. Провести консультации с компанией-поставщиком СКУД и определить возможность использования информации об отпечатках пальцев для проведения расследования.
6. Предложить сотрудникам из круга подозреваемых пройти дактилоскопическую экспертизу
7. Предложить сотрудникам из круга подозреваемых пройти обследование на полиграфе
8. Проанализировать результаты проведенных мероприятий.

Критерии оценивания:

<table>
<tr><td>Критерии оценивания</td><td>Полный и правильный ответ на 2 вопроса; правильное решение кейса</td><td>Неполный, но правильный ответ на 2 вопроса, правильное решение кейса</td><td>Неполный правильный ответ на 2 вопроса с помощью наводящих вопросов педагогического работника или полный и правильный ответ на один вопрос и неполный, но правильный ответ на 2 вопрос, правильное решение кейса</td><td>Неявка на промежуточную аттестацию или ответ менее чем на 2 вопроса и (или) неправильное решение кейса</td></tr>
<tr><td rowspan="2">Оценка</td><td>отлично</td><td>хорошо</td><td>удовлетворительно</td><td>неудовлетворительно</td></tr>
<tr><td colspan="3">компетенции сформированы</td><td>компетенции не сформированы</td></tr>
</table>

5. Методические материалы, необходимые для освоения дисциплины (модуля)

5.1. Перечень основной литературы

1. Абчук В.А. Риски в бизнесе, менеджменте и маркетинге. – СПб.: Изд-во Михайлова В.А., 2006. – 480 с.

2. Балдин К.В. Управление рисками.- Москва: ЮНИТИ-ДАНА, 2005. – 511 с.

3. В.И. Ярочкин Система безопасности фирмы. – 3-е изд., перераб. и доп. – М.: Ось-89, 2003. – 352 с.

4. Вяткин В.Н., Гамза В.А., Екатеринославский Ю.Ю., Иванушко П.Н. Управление рисками фирмы: программы интегративного риск-менеджмента. – Москва: «Финансы и статистика», 2006. – 397 с.

5. Доронин А.В. Бизнс-разведка. – 20е изд., перераб. и доп. – М.: Издательство «Ось-89», 2003. – 384 с.

6. Коноплева И.А., Богданов И.А. Управление безопасностью и безопасность бизнеса: Учебное пособие для вузов/ Под ред. И.А. Коноплевой. – М.: ИНФРА-М, 2008. – 448 с.

7. Коршунова Л.Н. Оценка и анализ рисков. – Ростов н/Д, 2007. – 96 с.

8. Майский Р.А., Борисова Е.А. Основные принципы защиты информации при построении КСЗИ и их характеристика, 2016.

9. О. Грунин, С. Грунин Экономическая безопасность организации – СПб.: Питер, 2002. – 160 с.: ил. – (Серия «Учебные пособия»).

10. Самоукина Н.В. Незаменимый сотрудник и кадровая безопасность/ Самоукина Наталья Васильевна. – Москва: Вершина, 2008. – 176 с.

11. Сулейманов У. Правила охоты на «крыс», или Как бороться с внутрикорпоративными хищениями. Практическое пособие для предпринимателей. – М.: Ось – 89, 2007. – 144 с.

12. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

13. Управление рисками: инструменты руководителя: электронный учебник. Серия «БизнесШкола». Издательский дом «Равновесие», 2007.

14. Энциклопедия деловой разведки и контрразведки. – М.: Русь-Олимп, 2007. – 428 с.

15. Ярочкин В.И., Бузанова Я.В. Корпоративная разведка. – М.: «Ось-89», 2004. – 288 с.

5.2. Перечень дополнительной литературы

1. Андрианов В.И., Соколов А.В. Как сберечь свои секреты – 2-е изд. – М.: ООО «Фирма «Издательство АСТ»: СПб: ООО «Издательство «Полигон» 2000. – 272 с.

2. Деревицкий А. Коммерческая разведка. Курс агентуры для тех, кто продает и управляет продажами. – Спб., 2005. – 319 с.

3. Землянов В.М. Своя контрразведка. Минск: Харвест, 2002.

4. Зникин, В.К. Основы личной безопасности: модели, схемы и определения: учеб. пособие для вузов /В.К. Зникин, Р.Г. Драпезо, Е.С. Гольдшмидт, Н.А. Егорова; Кемерово. гос. ун-т. – Кемерово: ИПП «Кузбасс», 2008. – 120 с.

5. Зникин, В.К. Теоретические и прикладные основы оперативно-розыскного обеспечения раскрытия и расследования преступлений: учеб. пособие / В.К. Зникин; Кемеров. гос. ун – т. Кемерово: ИПП «Кузбасс», 2008. – 191 с.

6. Кузнецов А. Секрет фирмы. – М.: Ось –89, 2006. – 208 с. (Реальный успех).

7. Логинов О.И. Безопасность вашего бизнеса /Логинов О.И. – М.: НТ Пресс, 2006. – 208 с. – (Бизнес-букварь).

8. Лукаш Ю.А. Как обезопасить себя и свой бизнес от захвата, шантажа, мошенничества и иных враждебных проявлений / Ю.А. Лукаш. – Москва: ГроссМедиа, 2006. – 112 с. (Инструкция по выживанию).

9. Маккей Х. Как уцелеть среди акул: (Опередить конкурентов в умении продавать, руководить, стимулировать, заключать сделки): Пер. с англ. / Пер.: Ю.В. Семенов; Предисл.: И.В. Липсиц, Л.Б. Невзлин; Под общ. ред. И.В. Липсица. – М.: Экономика, 1992. – 172 с.

10. Организация и современные методы защиты информации (под общей редакцией Диева С.А., Шаваева А.Г.). – М., Концерн «Банковский Деловой Центр», 1998, 472 с.

11. Парад Борис Коммерческий шпионаж. 79 способов, которыми конкуренты могут получить секреты любого бизнеса. – М.: ТК Велби, 2005. – 160 с.

12. Ронин Р. Своя разведка. Минск: Харвест, 1999.

13. Черкасов В.Н. Бизнес и безопасность. Комплексный подход/ Худож. В. Родин. – М.: Армада –пресс, 2001. 384 с.: ил. – (Хотите Выжить?).

14. Ярочкин В.И., Бузанова Я.В. Аудит безопасности фирмы: теория и практика: Учебное пособие для студентов высших учебных заведений. – М.: Академический Прект; Королев: Парадигма, 2005. – 352 с.

5.3. Методические материалы для организации самостоятельной работы обучающихся по освоению дисциплины (модуля).

Самостоятельная работа обучающегося заключается в ознакомлении с содержанием рабочей программы по дисциплине, планируемыми результатами обучения по дисциплине, учебно-методическими материалами, указанными в настоящей рабочей программе.

Обучающийся обязан добросовестно осваивать образовательную программу, в том числе посещать предусмотренные учебным планом учебные занятия, осуществлять самостоятельную подготовку к занятиям, выполнять задания, данные педагогическими работниками в период обучения по дисциплине.

При подготовке к учебным занятиям обучающийся обязан освоить теоретический материал в соответствии с тематикой, установленной в настоящей рабочей программе дисциплины.

Вопросы, возникающие в период выполнения самостоятельной работы по дисциплине, обучающийся вправе обсудить с педагогическим работником, в том числе в форме синхронного и асинхронного взаимодействия в электронной информационной образовательной среде КузГТУ и (или) с использованием ресурсов корпоративной электронной почты КузГТУ.

5.4. Активные методы обучения

Лекции – визуализации: с помощью мультимедийного оборудования демонстрируются цифровой контент, содержащий схемы, таблицы, статистический и текстовой материал;

Проблемные лекции: перед началом изложения материала перед обучающимися ставится проблема, касающаяся возможного развития событий (преимуществ/ недостатков каждого метода маркетинговых исследований), пути разрешения проблемы раскрываются по мере изложения материала и обсуждаются в завершение лекции.

Лекции-беседы: часть лекции по указанным темам проходят в диалоговом режиме, инициируются вопросы педагогическим работником, мнение по ним высказывают все желающие, после чего озвучиваются эталонные ответы.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

6.1. Для изучения дисциплины, могут использоваться следующие электронно-библиотечные и справочные системы, электронные справочники

– eLIBRARY.RU

– «Университетская библиотека онлайн»
– «Лань»
– «Юрайт»
– НТБ КузГТУ
– «Znanium»
– «Информио»
– справочно-правовая система «Гарант»
– справочно-правовая система «Консультант плюс»

6.2. Для изучения дисциплины, могут использоваться следующие методы, средства обучения и образовательные технологии

- Кейс-технологии
- Технология деловой игры
- Информационные технологии в соответствующих отраслях для решения профессиональных задач
- Сквозные цифровые технологии, востребованные в соответствующих отраслях для решения профессиональных задач
- Технологии проблемного обучения
- Технологии проектного обучения
- Технологии искусственного интеллекта
- Практико – ориентированные технологии
- Электронное обучение, дистанционные образовательные технологии.

6.3. Для изучения дисциплины может использоваться следующее ПО:

- CASE-технологии
- Технологии анализа данных и язык R, Radiant и SOL
- Data science
- Браузеры Яндекс, Safari, Chrome, Mozilla и др.
- Яндекс Аудитория,
- Яндекс. Метрика
- Яндекс. Директ
- Яндекс. Диск
- Яндекс. Документы
- Яндекс. Почта
- Mentimeter
- Moodle
- «Фабрика кроссвордов»
- средства, технологии планирования и управления с помощью электронных таблиц;
- электронная почта и телекоммуникационные средства;
- математическое и компьютерное моделирование;
- экспертные и интеллектуальные системы;
- корпоративная электронная почта и телекоммуникационные средства;
- гипертекстовые технологии и WWW-технологии;
- Kali Linux - дистрибутив Linux для проведения тестов на безопасность.

6.4. Для изучения дисциплины, могут использоваться следующие цифровые платформы:

- Miro

6.5. Для изучения дисциплины, могут использоваться собственные цифровые платформы

ЭИОС КузГТУ (https://el.kuzstu.ru/login/index.php , https://library.kuzstu.ru/ ,

https://portal.kuzstu.ru/)
ресурсы электронной информационной образовательной системы.

6.6. Для изучения дисциплины, могут использоваться следующие Интернет ресурсы

- https://vc.ru/ - *Платформа для предпринимателей и высококвалифицированных специалистов малых, средних и крупных компаний*
- https://www.sostav.ru/ - *Новости рекламы и маркетинга*
- https://openedu.ru/ *Образовательная онлайн-платформа*
- http://www.machinelearning.ru/ *Профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных*

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

7.1. Минимальные технические требования к оборудованию и каналам связи участников образовательных отношений

- ***Персональный компьютер***

Платформа (Операционная система): Windows 7, MacOS 10.9 Maverics, Linux. Pentium 4.1 GHz (либо аналог), RAM 512 Mb, HDD 250 Mb, Клавиатура, Мышка, Широкополосный доступ, Разрешение экрана не менее 800x600.
Наличие интернет-браузера: Chrome 37.0, Firefox 38.0, Opera 10.53, Apple Safari.
Видеокамера, динамики (наушники), микрофон.

- ***Мобильное устройство:***

Любое мобильное устройство имеющее доступ в интернет, с установленным браузером.
Наличие видеокамеры, динамиков (наушников) и микрофона обязательно.

8. Иные сведения и (или) материалы

При осуществлении образовательного процесса применяются следующие образовательные технологии:

- традиционная с использованием современных технических средств;
- электронное обучение, дистанционные образовательные технологии;
- модульная;
- интерактивная.

Организация и проведение учебных занятий осуществляется с использованием электронных мультимедийных средств.

В процессе проведения учебных занятий в контактной работе используется диалоговая форма чтения лекций с постановкой и решением проблемных задач, обсуждением дискуссионных моментов.

Самостоятельная работа включает повторение теоретического материала и закрепление его при решении конкретных задач.