

**Федеральное государственное автономное образовательное учреждение  
высшего профессионального образования  
"Национальный исследовательский университет  
"Высшая школа экономики"**

Институт проблем безопасности

Кафедра проблем безопасности

**Майнор «Безопасность предпринимательской деятельности»**

Рабочая программа дисциплины «Защита информационной среды бизнеса от  
киберпреступлений и иных угроз»

для уровня подготовки - бакалавриат

Разработчик(и) программы  
Юрченко А.В. [ayurchenko@hse.ru](mailto:ayurchenko@hse.ru)  
Рудченко А.Д. [arudchenko@hse.ru](mailto:arudchenko@hse.ru)

Утверждена «\_\_» \_\_\_\_\_ 2016 г.  
Директор института проблем безопасности  
Юрченко А.В. \_\_\_\_\_ [подпись]

Москва, 2016

*Настоящая программа не может быть использована другими подразделениями университета  
и другими вузами без разрешения подразделения-разработчика программы.*



## 1 Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает минимальные требования к знаниям и умениям студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и студентов, изучающих дисциплину «Защита информационной среды бизнеса от киберпреступлений и иных угроз» в рамках майнора «Безопасность предпринимательской деятельности».

## 2 Цели освоения дисциплины

Третья дисциплина майнора позволит студентам с позиций теории информации ознакомиться с основами современного информационного противоборства в бизнесе и сфере межгосударственных отношений. Студенты изучат формы, методы и средства промышленного шпионажа, а также ведения информационной борьбы. Особое внимание будет уделено кибернетическим угрозам и современным защитным мерам, позволяющим обеспечивать безопасность информации и информационных процессов. Обучающиеся научатся распознавать признаки возникновения возможных угроз в названных областях, ознакомятся с деятельностью структурных подразделений и самостоятельных предприятий, осуществляющих деятельность по защите всех видов информационных ресурсов бизнеса.

## 3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате изучения главы студент должен **знать** основы теории информации и основные угрозы в области информационной безопасности предприятия; о преднамеренной деятельности государств и транснациональных корпораций по хищению охраняемой информации в процессе промышленного шпионажа; об умышленном и непреднамеренном разрушении системы передачи информации в целях управления, что может привести к нарушению нормальной жизнедеятельности предприятия; **уметь** использовать признаки несанкционированного доступа к информации в местах ее хранения, в процессе ее передачи от одного пользователя к другому путем перехвата каналов связи и компрометации шифров; **владеть** методами выявления рисков и угроз в области информационной безопасности предприятия.

В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код по ФГОС/ НИУ	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
	ОК-1	[Глаголы-подсказки, даны по мере повышения уровня освоения: дает определение, воспроизводит, распознает, использует, демонстрирует, владеет, применяет, представляет связи, обосновывает, интерпретирует оценивает]	

## 4 Место дисциплины в структуре образовательной программы

Настоящая дисциплина «Защита информационной среды бизнеса от киберпреступлений и иных угроз» входит в состав майнора «Безопасность предпринимательской деятельности»,



который включен в состав вариативной части профессиональных дисциплин образовательной программы.

Изучение данной дисциплины базируется на следующих дисциплинах:

**«Глобальные вызовы современности и организация комплексной системы безопасности бизнеса», «Деловая (конкурентная) разведка. Защита бизнеса от угроз в области экономики и финансов».**

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями и компетенциями:

**знать** теорию и практику обеспечения безопасности бизнеса, основные положения общей и частных теорий конфликтов, общей и частных теорий безопасности, основных систем предпринимательских и хозяйственных рисков, неэкономических рисков и угроз безопасности предпринимательской деятельности, соотношение интересов личности, бизнеса и государства, историю и современное состояние отрасли безопасности предпринимательской деятельности, способы выявления и минимизации рисков недобросовестных контрагентов, кредитных, операционных, криминальных рисков и угроз применения противоправных методов конкуренции; **уметь** применить эти знания на практике, понять особенности и органическую взаимосвязь экономической, финансовой, информационной, физической, инженерно-технической и кадровой функций безопасности предприятия, уметь объединить эти функции в единую комплексную систему обеспечения безопасности предприятия в целях предупреждения и минимизации возможных угроз, применить эти знания на практике, работать с информационно-поисковыми системами; **владеть** основными современными методами противодействия внутренним и внешним угрозам, правильно оценивать особенности среды предприятия, его уникальные особенности и масштабы деятельности, отраслевую и региональную специфику, методикой изучения контрагентов.

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

Дисциплины майнора «Безопасность предпринимательской деятельности»: «Обеспечение безопасности материальных ресурсов бизнеса и защита персонала».

## 5 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы *			Самостоятельная работа
			Лекции	Практические занятия, мастер-классы, деловая игра	Семинары	
1	Угрозы в области информационной безопасности	8	4			4
2	Защита персональных данных. Защита конфиденциальной информации/ Защита государственной и служебной тайны	22	4	4	2	12
3	Электронные информационные ресурсы, системы и процессы	24	4	4		16
4	Типовые угрозы кибернетической безопасности предприятия	36	6	2	4	24
5	Архитектура стандартов кибернетической безопасности	32	4		4	24
6	Превентивная защита информации на АРМ, в сетях и БД, в системе ЭФ	34	6	4		24
7	Защита информации в сети Интернет. Расследование киберинцидентов.	34	4	6		24



ИТОГ	190	32	20	10	128
------	-----	----	----	----	-----

\*- дисциплина предназначена для дистанционной формы обучения. Все активности студентов представляются в системе LMS

## 6 Формы контроля знаний студентов

Тип контроля	Форма контроля	1 год		Параметры **
		1	2	
Текущий (неделя)	Контрольная работа			
	Эссе		1	
	Реферат			
	Коллоквиум			
	Домашнее задание	1	1	Выполнение задания требует от 30 минут до 2 часов времени
Итоговый	Экзамен		1	Тест (возможен реферат для дистанционных студентов и защита проектной документации для студентов, выполняющих проекты)

### 6.1 Критерии оценки знаний, навыков

**Домашние задания** - все работы оцениваются на полноту выполнения (число использованных критериев для анализа), на глубину (на сколько была проработана проблема, сколько внешних источников было привлечено и рассмотрено), на аргументированность.

Экзамен проводится в виде защиты проекта.

## 7 Содержание дисциплины

- 1) Общая теория информации и философия информационной безопасности бизнеса
- 2) Риски и угрозы промышленного шпионажа
- 3) Принципы отнесения предприятий к потенциальным объектам промышленного шпионажа
- 4) Формирование общих режимов противодействия
- 5) Выявление частных случаев промышленного шпионажа
- 6) Мониторинг защищенности предприятия от промышленного шпионажа
- 7) Взаимодействие бизнеса и государства в области противодействия промышленному шпионажу
- 8) Информация, ее носители и процессы, подлежащие социальной защите
- 9) Защита персональных данных
- 10) Защита конфиденциальной информации
- 11) Особенности защиты банковской тайны
- 12) Защита сведений, составляющих государственную тайну
- 13) Безопасность электронных ресурсов, систем и процессов
- 14) Типовые сценарии несанкционированного доступа к информации
- 15) Особенности противоправных корыстных посягательств на систему банк-клиент
- 16) Модели организации кибернетической безопасности предприятия
- 17) Построение систем информационной безопасности и аудит их эффективности



- 18) Архитектура стандартов защиты информации
- 19) Аутсорсинг в системе информационной безопасности
- 20) Взаимодействие с государственными органами в области

## **8 Образовательные технологии**

Образовательные технологии, используемые при реализации различных видов учебной работы: активные и интерактивные формы проведения занятий - деловые и ролевые игры, разбор практических задач и кейсов, компьютерные симуляции. В рамках курса предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов

### **8.1 Методические рекомендации преподавателю**

Даются по желанию автора. Методические рекомендации (материалы) преподавателю могут оформляться в виде приложения к программе дисциплины и должны указывать на средства и методы обучения, применение которых для освоения тех или иных тем наиболее эффективно.

### **8.2 Методические указания студентам**

Даются по желанию автора. Методические указания студентам могут оформляться в виде приложения к программе дисциплины и должны раскрывать рекомендуемый режим и характер учебной работы, особенно в части выполнения самостоятельной работы.

## **9 Оценочные средства для текущего контроля и аттестации студента**

### **9.1 Тематика заданий текущего контроля**

Домашнее задание:

Условие домашнего задания:

Условия задачи: Ваш научный руководитель по электронной почте получил приглашение (прилагается) от Центра научных публикаций принять участие во II Международной мульти дисциплинарной конференции на тему «Наука в эпоху дисбалансов», которая должна состояться 25 января 2016 года. Прием материалов и заявок заканчивается также 25 января 2016 года. Ваш научный руководитель сообщил, что организатор конференции ему неизвестен и поручил Вам изучить вопрос, а по итогам представить заключение о возможности и целесообразности участия в названной международной конференции. Задание: Проведите изучение поступившего приглашения, сайта организатора и других необходимых источников информации, а также руководствуясь своими знаниями об организации международных научных конференций, выполните поручение научного руководителя. •Выводы необходимо отразить в электронном документе.

**Примерный перечень тем рефератов:**

1. Промышленный шпионаж и принципы защиты конфиденциальной информации при подготовке и проведении служебных совещаний.
2. Меры защиты собственных интересов лица при совершении сделок по покупке товаров в сети Интернет.
3. Особенности нормативно-правовой защиты кибернетической информации в нашей стране.



4. Меры государственного контроля в области обеспечения безопасности кибернетической информации.
5. Участие уполномоченных государственных органов в защите кибернетической информации в реальном секторе экономики от неправомерных посягательств.
6. Самозащита гражданских прав предприятия в случае совершения кибернетического инцидента.
7. Информационные инциденты в сфере кибернетической безопасности, требующих взаимодействия с уполномоченными органами государства.

Каждый слушатель вправе выбрать предложенную тему или выбрать свою в рамках вопросов, рассматриваемых в дисциплине № 3 майнора

## **9.2 Вопросы для оценки качества освоения дисциплины**

Примерный перечень вопросов к зачету (экзамену) по всему курсу или к каждому промежуточному и итоговому контролю для самопроверки студентов.

## **9.3 Примеры заданий промежуточного /итогового контроля**

Обсуждение результатов проектов.

## **10 Порядок формирования оценок по дисциплине**

Накопленная оценка формируется из равновзвешенных оценок за текущий контроль (домашние задания и эссе) и деловую игру. Оценка за экзамен выставляется по итогам прохождения тестирования (предусмотрены формы итогового контроля реферат и защита проектной документации для определенных групп студентов). Итоговая оценка выставляется как средняя арифметическая двух оценок и округляется по арифметическим правилам.

### **Учебно-методическое и информационное обеспечение дисциплины**

#### **10.1 Базовый учебник**

Шульц В.Л., Рудченко А.Д., Юрченко А.В. Безопасность предпринимательской деятельности. 2015. М. Юрайт

Выходит в печать. Студентам предоставляются материалы в электронном виде.

#### **10.2 Основная литература**

[ Укажите обязательную литературу, которая является обязательной для освоения студентами. Должна быть доступна студентам по нормативу обеспеченности не менее 50 %. Несоблюдение данного норматива может распространяться не более чем на 10 % источников из списка основной литературы.

Укажите, если доступна электронная версия каких-либо учебных пособий].

#### **10.3 Дополнительная литература**

Библиография (экономическая безопасность):

1. Астахов П.А. Противодействие рейдерским захватам. 2008. М. Эксмо;-
2. Брэгг С. Слияния и поглощения. 2011. М. Маросейка;
3. Брюн Ж.-П., Грей Л. и др. Руководство по возврату активов для специалистов-практиков. 2015. М. Альпина;
4. Валласк Е.В. Мошенничество с использованием ценных бумаг. 2007. СПб. Юридический центр;
5. Гринберг Т., Сэмюэль Л. и др. Возврат похищенных активов. 2014. М. Мировой банк/Альпина;
6. Доронин А.И. Бизнес-разведка. 2010. М. Ось-89;



7. Котлер Ф., Келлер К.Л. Маркетинг менеджмент. 2015. М.-СПб. Питер;
8. Криминалистика. Под редакцией А.Г. Филиппова. 2014. М. Юрайт;
9. Криминология. Под редакцией В.Н. Кудрявцева, В.Е. Эминова. 2013. М. Норма/Инфра-М;
10. Кротков А.П. Все великие аферы мошенничества и финансовые пирамиды. 2008. М. Астрель;
11. Крупнейшие мировые аферы. Составитель В. Башкирова. 2010. М. Эксмо;
12. Ларичев В.Д., Иконников Д.Н. и др. Преступления в сфере банковского кредитования и методика их предупреждения. 2012. М. Дело и Сервис;
13. Лемке Г.Э. Конкурентная война. Нелинейные методы и стратагемы. 2012. М. Ось-89;
14. Лемке Г.Э. Секреты коммерческой разведки. 2012. М. Ось-89;
15. Маркополос Г. Финансовая пирамида Бернарда Мэдоффа. 2012. М.-СПб.-Киев. Диалектика;
16. Нежданов И.Ю. Технологии разведки для бизнеса. 2013. М. Ось-89;
17. Новые русские аферы. Составители В. Башкирова, А. Соловьев. 2010. М. Эксмо;
18. Подделка первичных документов и сговор с поставщиками. Под редакцией Дж. Т. Уэллса. 2010. М. Маросейка;
19. Портер М. Конкурентная стратегия. Методика анализа отраслей и конкурентов. 2015. М. Альпина;
20. Рид С.Ф., Рид Лажу А. Искусство слияний и поглощений. 2014. М. Альпина;
21. Рубин Ю.Б. Теория и практика предпринимательской конкуренции. 2010. М. Маркет ДС;
22. Рудык Н.Б. Методы защиты от враждебного поглощения. 2008. М. Дело;
23. Саблин М.Т. Взыскание долгов от профилактики до принуждения. 2011. М. Волтерс Клувер;
24. Сычев П. Хищники. Теория и практика рейдерских захватов. 2011. М. Альпина;
25. Тарташев В.А. Как заработать на чужих долгах. 2010. Ростов-на-Дону. Феникс;
26. Федоров А.Ю. Рейдерство и корпоративный шантаж. 2010. М. Волтерс Клувер;
27. Ярочкин В.И., Бузанова Я.В. Корпоративная разведка. 2011. М. Ось-89.

Библиография (финансовая безопасность):

1. Богаченко В.М., Кириллова Н.А. Основы бухгалтерского учета, налогообложения и аудита. 2012. Ростов-на-Дону. Феникс;
2. Валютное право. Под редакцией Ю.А. Крохиной. 2013. М. Юрайт;
3. Гринберг Т., Грей Л. Политически значимые лица. 2015. М. Мировой банк/Альпина;
4. Жубрин Р.В. Борьба с легализацией преступных доходов. 2011. М. Волтерс Клувер;
5. Кобозева Н.В. Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в аудиторской деятельности. 2012. М. Инфра-М;
6. Кучеров И.И. Валютно-правовое регулирование в Российской Федерации. 2013. М. Инфра-М;
7. Литвин Д.В., Богданова Е.П. Аудит. 2008. М. Маркет ДС;
8. Международные стандарты аудита и контроля качества. В трех томах. 2012. Киров. Областная типография;
9. Потемкин С.А. Формирование системы финансового мониторинга в кредитных организациях. 2010. М. Кнорус;
10. Прошунин М.М. Финансовый мониторинг. 2009. М. Статус;
11. Ревенков П.В., Дудка А.Б. и др. Финансовый мониторинг: управление рисками отмывания денег в банках. 2012. М. Кнорус;
12. Стандарты по аудиторской деятельности. Составитель Е.В. Невешкина. 2012. М. Омега-Л;



13. Чашин А.Н. Выявление необычных сделок как метод противодействия отмыванию преступных доходов и финансированию терроризма. 2010. М. Дело и Сервис.

Кадровая безопасность:

1. Алавердов А.Р. Управление кадровой безопасностью организации. 2010. М. Маркет ДС;
2. Бекасов Ш. Банковская тайна. 2011. М. Кнорус;
3. Дафт Р. Теория организации. 2012. М. Юнити;
4. Журин С.И. Практика и теория использования детекторов лжи. 2011. М. Горячая линия-Телеком;
5. Крез. Я – аферист. Признания банкира. 2010. М. Астрель;
6. Лисон Н. Как я обанкротил «Бэрингз». Признания трейдера-мошенника. 2011. М. Кейс;
7. Мелтон К., Пилиджан К. Офисный шпионаж. 2013. М. АНФ;
8. Многоликая коррупция. Под редакцией Э. Кампоса. 2014. Альпина. Альпина/Мировой банк;
9. Муштук О.З. Искушение бизнесом. 2011. М. МФПА;
10. Назаров О.В. Как воруют в ресторане. 100 способов обмануть владельца. 2010. М. Ресторанные ведомости;
11. Павлович С. Как я украл миллион. Исповедь раскаявшегося кардера. 2014. М.-СПб. Питер;
12. Полиграф в России (1993-2008). Составитель Ю.И. Холодный. 2008. М. МГТУ им. Н.Э. Баумана;
13. Современные стандарты и технологии противодействия коррупции. Материалы Третьего Евразийского антикоррупционного форума. 2015. М. ИЗСП;
14. Соломанидина Т.О., Соломанидин В.Г. Кадровая безопасность компании. 2011. М. Альфа-Пресс;
15. Уголовно-правовые меры по противодействию коррупции за рубежом. Под редакцией И.С. Власова. 2014. М. ИЗСП;
16. Фукс А. Защита бизнеса от мошенничества. 2011. М. Business School for Owners;
17. Цыро С.В. Как победить воровство в ресторане. 2011. М. Ресторанные ведомости.

#### **10.4 Справочники, словари, энциклопедии**

[ Укажите рекомендуемые справочники, словари, энциклопедии. Источники оформляются в соответствии со стандартами как указано выше.

Укажите, если используются, электронные версии изданий справочников, словари или электронные справочники]

#### **10.5 Программные средства**

Информационно-аналитические системы.

#### **10.6 Дистанционная поддержка дисциплины**

Дисциплина может преподаваться дистанционно, все материалы и перечень активностей представлены в LMS.





## **11 Материально-техническое обеспечение дисциплины**

Проектор, ноутбук