**Программа учебной дисциплины «Защита информационной среды бизнеса от киберпреступлений и иных угроз»**

Утверждена

Проректором С.Ю.Рощиным

от «26»\_июня\_2017 г.

|  |  |
| --- | --- |
| Автор  | А. В. Юрченко, профессор, А. Д. Рудченко, д.т.н., профессор |
| Число кредитов  | 5 |
| Контактная работа (час.)  | 62 |
| Самостоятельная работа (час.)  | 128 |
| Курс  | 3 |
| Формат изучения дисциплины | без использования онлайн курса |

1. **ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ**

Третья дисциплина майнора позволит студентам с позиций теории информации ознакомиться с основами современного информационного противоборства в бизнесе и сфере межгосударственных отношений.

Целью освоения дисциплины «Защита информационной среды бизнеса от киберпреступлений и иных угроз» является изучение студентами форм, методов и средств 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.

В результате освоения дисциплины 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.

Изучение дисциплины «Защита информационной среды бизнеса от киберпреступлений и иных угроз» 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,
	+ 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:

1. Дисциплины майнора «Безопасность предпринимательской деятельности»: «Обеспечение безопасности материальных ресурсов бизнеса и защита персонала».
2. **СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**
3. Общая теория информации и философия информационной безопасности бизнеса
4. Риски и угрозы промышленного шпионажа
5. Принципы отнесения предприятий к потенциальным объектам промышленного шпионажа
6. Формирование общих режимов противодействия
7. Выявление частных случаев промышленного шпионажа
8. Мониторинг защищенности предприятия от промышленного шпионажа
9. Взаимодействие бизнеса и государства в области противодействия промышленному шпионажу
10. Информация, ее носители и процессы, подлежащие социальной защите
11. Защита персональных данных
12. Защита конфиденциальной информации
13. Особенности защиты банковской тайны
14. Защита сведений, составляющих государственную тайну
15. Безопасность электронных ресурсов, систем и процессов
16. Типовые сценарии несанкционированного доступа к информации
17. Особенности противоправных корыстных посягательств на систему банк-клиент
18. Модели организации кибернетической безопасности предприятия
19. Построение систем информационной безопасности и аудит их эффективности
20. Архитектура стандартов защиты информации
21. Аутсорсинг в системе информационной безопасности
22. Взаимодействие с государственными органами в области
23. **ОЦЕНИВАНИЕ**

Текущий контроль знаний и навыков студентов осуществляется преподавателем в ходе проверки двух домашних заданий и эссе, а также путем оценивания его работы в аудитории (участие в 1 деловой игре).

Все домашние задания оцениваются на полноту выполнения (число использованных критериев для анализа), на глубину (насколько была проработана проблема, сколько внешних источников было привлечено и рассмотрено), на аргументированность.

Итоговый контроль знаний и навыков студентов осуществляется в ходе экзамена, который проводится в виде тестирования (предусмотрены формы итогового контроля реферат и защита проектной документации для определенных групп студентов).

Все оценки формируются по 10-балльной шкале. Способ округления оценок –арифметический, т.е. используются стандартные правила округления (до 0,5 баллов оценка округляется в меньшую сторону, после 0,5 включительно – в большую).

**Накопленная оценка по дисциплине формируется следующим образом:**

$$О\_{накопленная}=\frac{\left(О\_{ДЗ1}+О\_{ДЗ2}+О\_{ЭССЕ}+О\_{ДИ}\right)}{4}$$

Где $О\_{ДЗ}$ – оценка за каждое домашнее задание;

 $О\_{ДИ}$ – оценка за деловую игру;

**Итоговая оценка за дисциплину формируется по формуле:**

$$О\_{итоговая}=0,5\*О\_{накопленная}+0,5\*О\_{экзамен}$$

Оценка за экзамен и результирующая оценка по учебной дисциплине выставляются преподавателем в рабочую и экзаменационную ведомости.

 В диплом ставится результирующая оценка по учебной дисциплине.

1. **ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ**

# Оценочные средства для текущего контроля студента

***Домашнее задание:***

Условие домашнего задания:

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.

Оценочные средства для промежуточного/итогового контроля студента

Обсуждение результатов проектов.

1. **РЕСУРСЫ**
	1. **Основная литература**
2. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Безопасность предпринимательской деятельности. 2015. М. Юрайт

 Выходит в печать. Студентам предоставляются материалы в электронном виде.

* 1. **Дополнительная литература**
* Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК-пресс. – 2014. – 702с.
* 149-ФЗ «Об информации, информационных технологиях и о защите информации».
* Белов В.М., Новиков С.Н., Солонская О.И. Теория информации. М.: Телеком, 2012;
* Компьютерное мошенничество. Под редакцией Дж. Т. Уэллса. М.: Маросейка, 2010;
* Хэл Абельсон и др. Атака битов: твоя жизнь, свобода и благополучие в цифровую эпоху. С-П, «Символ-Плюс», 2009;
* Глобальное исследование утечек конфиденциальной информации в 2017 году. Аналитический центр InfoWatch, www.infowatch.ru/analytics
	1. **Программное обеспечение**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование** | **Условия доступа** |
|   1. |  Microsoft Windows 7 Professional RUSMicrosoft Windows 10Microsoft Windows 8.1 Professional RUS | *Из внутренней сети университета (договор)* |
| 2. | Microsoft Office Professional Plus 2010 | *Из внутренней сети университета (договор)* |

* 1. **Профессиональные базы данных, информационные справочные системы,
	интернет-ресурсы (электронные образовательные ресурсы)**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование**   | **Условия доступа/скачивания**  |
| 1 |  Информационно-аналитические системы, СГА НКБ. | Из внутренней сети университета (договор) |
| 2 | Электронно-библиотечная система Юрайт | URL: https://biblio-online.ru/ |
| 3 | Консультант Плюс | Из внутренней сети университета (договор) |

* 1. **Материально-техническое обеспечение дисциплины**

Учебные аудитории для лекционных занятий по дисциплине обеспечивают использование и демонстрацию тематических иллюстраций, соответствующих программе дисциплины в составе:

ПЭВМ с доступом в Интернет (операционная система, офисные программы, антивирусные программы);

мультимедийный проектор с дистанционным управлением.