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

Утверждена
Проректором С.Ю.Рощиным
от «13»_марта_2019 г.

Автор	А. В. Юрченко, профессор, А. Д. Рудченко, д.т.н., профессор
Число кредитов	5
Контактная работа (час.)	56
Самостоятельная работа (час.)	134
Курс	3
Формат изучения дисциплины	без использования онлайн курса

I. 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».

II. СОДЕРЖАНИЕ УЧЕБНОЙ 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

III. 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:

$$О_{\text{накопленная}} = 0{,}4 * \frac{(О_{ДЗ1} + О_{ДЗ2} + О_{ЭССЕ})}{3} + 0{,}2 * О_{ДИ} + 0{,}2 * КВЛ_{СР} + 0{,}2 * О_{СЕМ}$$

Где $О_{ДЗ}$ – оценка за каждое домашнее задание;

$О_{ДИ}$ – оценка за деловую игру;

$КВЛ_{СР}$- среднее за контрольные вопросы на лекциях;

$О_{СЕМ}$ – оценка за самостоятельную работу при подготовке к семинарам.

Итоговая оценка за дисциплину формируется по формуле:

$$О_{\text{итоговая}} = 0{,}7 * О_{\text{накопленная}} + 0{,}3 * О_{\text{экзамен}}$$

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

В диплом ставится результирующая оценка по учебной дисциплине.

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Оценочные средства для текущего контроля студента

Домашнее задание:

Условие домашнего задания:

В качестве объекта для модернизации системы информационной безопасности рассматривается «ПРОМРЕГИОНБАНК» - региональный банк среднего размера, специализирующийся на предоставлении розничных услуг для юридических и физических лиц.

Краткое описание банка.

- Бизнес-моделью банка является привлечение средств от физических и юридических лиц региона, их размещение с минимальными рисками в кредиты населению и бизнесу, прежде всего среднему и малому, того же региона.
- Уставный капитал банка на 01 января 2018 года составлял 1 млрд. 750 млн. рублей
- Банк располагает сетью из 15 клиентских центров и центральным офисом в региональном центре, а также сетью из 85 банкоматов, расположенных в различных частях города.
- В каждом клиентском офисе имеется оборудование и персонал для работы с наличными денежными средствами и осуществления электронных платежей.
- Клиентские офисы оборудованы специальными переговорными для проведения встреч с представителями организаций и физическими лицами по различным вопросам их кредитования и иным услугам банковского обслуживания.
- Банк широко использует для работы с юридическими и физическими лицами систему дистанционного банковского обслуживания (ДБО), включая интернет – банкинг, сеть банкоматов, а также платежные терминалы в торговых точках и сервисных центрах.
- Для осуществления инкассации денежных средств банк использует услуги объединения «РОСИНКАСС».
- В настоящее время система обеспечения информационной безопасности банка состоит из ряда элементов, обеспечивающих защиту персональных данных, защиту базовых функций ДБО, общие средства защиты от DDOS атак, а также включает базовый комплекс программных средств для защиты компьютеров банка от вирусов и неправомерных действий пользователей.
- Численность персонала банка составляет более 800 человек.

В ближайшее время в интересах расширения деятельности банка планируется создание комплексной системы информационной безопасности в соответствии с требованиями «Стандарта Банка России» СТО БР ИББС-1.0-2014, а также в соответствии с требованиями международного стандарта по информационной безопасности ISO/IEC 27001. В этой связи необходимо разработать предложения в «Проект Политики информационной безопасности «ПРОМРЕГИОНБАНКА», в части следующих основных разделов документа:

1. Основные принципы обеспечения информационной безопасности банка.
2. Цели и задачи системы информационной безопасности.

3. Объекты защиты.

4. Требования по информационной безопасности.

5. Владение информацией и основные владельцы.

6. Модели угроз и нарушителей.

Предложения должны быть разработаны в соответствии с указанными выше руководящими документами. При этом они должны быть представлены в виде отчета, объемом не более 3-5 страниц машинописного текста, выполненного в формате «Word», шрифтом «Times New Roman», размером - 12, с 1,5 - м интервалом.

Примерный перечень тем эссе:

1. Когда промышленный шпионаж бессилен, или как обсудить конфиденциальные вопросы на служебном совещании.
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. Инциденты в сфере кибер безопасности и государство: звать или не звать?
8. Загадочный биткоин: благо или всемирная угроза?
9. Индустрия киберпреступности. Что дальше?
10. Что же защищает информационная безопасность в компании, или какие тайны страшнее.
11. Цифровая экономика в эпоху кибервойн – фантастика или реальность?
12. Информационное противоборство в бизнесе: кто же реально управляет предприятием?
13. География киберпреступности: преступление и наказание.
14. Страсти по кибер шифровальщикам: вымогательство или разминка перед апокалипсисом?
15. Импортозамещение и информационная безопасность бизнеса.
16. Так ли всесильны DLP системы?
17. Темная сторона искусственного интеллекта в информационной безопасности.
18. А вы видели безопасное облако?
19. Интернет вещей, или что выбрать: удобства или безопасность?
20. Как сделать умный дом ещё и безопасным.
21. Кибербезопасность объектов критически важной инфраструктуры: что делать и кто виноват?
22. Анонимность в Интернете: наука и искусство.
23. Когда надо звать аудиторов информационной безопасности.

Оценочные средства для промежуточного/итогового контроля студента

Примерные задания теста:

Определение понятия «информация» как «обозначение содержания, полученного нами из внешнего мира, в процессе приспособления к нему нас и наших чувств» принадлежит:

- Клоду Шеннону
- Уильям Эшби
- Норберту Винеру
- Грегори Бейтсон

Можно ли отнести к коммерческой тайне сведения о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений?

- Да
- Нет

Проблемой применения модели PDCA (цикл Шухарта-Деминга) для управления информационной безопасностью является:

- Попытка все самое сложное вместить на первый шаг цикла
- Постоянное улучшение цикла
- Нелинейность информационной безопасности

Примерный перечень тем рефератов(для студентов, изучающих майнор дистанционно):

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.

Обсуждение результатов проектов – для студентов, участвующих в проектной деятельности по майнору (критерий участия – средний балл 8 и выше за две предыдущие дисциплины манора).

V. РЕСУРСЫ

5.1 Основная литература

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

5.2 Дополнительная литература

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.
2. Внуков, А. А. Защита информации : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс).
3. Демидов О. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества. 2016. М. Альпина.
4. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М. : Издательство Юрайт, 2019. — 325 с. — (Серия : Профессиональное образование).
5. Осокин, А. Н. Теория информации : учеб. пособие для прикладного бакалавриата / А. Н. Осокин, А. Н. Мальчуков. — М. : Издательство Юрайт, 2016. — 205 с. — (Серия : Университеты России).

5.3 Программное обеспечение

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

5.4 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	Деловая библиотека «Альпина Диджитал»	URL: https://alpinadigital.ru/
4	Электронно-библиотечная система ЗНАНИУМ (Znanium.com)	URL: https://Znanium.com
5	Консультант Плюс	Из внутренней сети университета (договор)

5.5 Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине обеспечивают исполь-

зование 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.