Программа учебной дисциплины «Конфиденциальность, непрерывность и безопасность бизнеса»

Утверждена
Академическим советом ООП
Протокол № 2 от «19» апреля 2017г.

Автор	Левашов М.В., к.ф-м.наук., старший научный сотрудник
Число кредитов	6
Контактная работа (час.)	72
Самостоятельная работа (час.)	156
Курс	2
Формат изучения дисциплины	Без использования on-line курса

I. ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ

Целями освоения дисциплины «Конфиденциальность, непрерывность и безопасность бизнеса» являются:

Освоение учащимися знаний в области:

- современных методов к обеспечению информационной и кибербезопасности (далее – ИБ) бизнеса с учетом последних достижений в области анализа больших данных с применением элементов искусственного интеллекта,
- риск ориентированного подхода к этому вопросу,
- законодательной и нормативно-методической базы ИБ,
- стандартизации элементов и требований ИБ,
- аудита ИБ.

Формирование у учащихся навыков, практического опыта и компетенций:

- комплексного построения и обеспечения процессов защиты информации и ИТ,
- проведения анализа информационных рисков,
- использования современных методик и инструментария для решения задач обеспечения ИБ.
- применения стандартов ИБ,
- проведения аудита ИБ.

Настоящая дисциплина относится к циклу технико-гуманитарных дисциплин и блоку дисциплин, обеспечивающих подготовку магистров.

Изучение данной дисциплины базируется на следующих дисциплинах:

Методика и инструментарий моделирования бизнес и информационных процессов
Математическое моделирование
Системный анализ и проектирование
Теория систем
Проектирование информационных (компьютерных) систем
Правовая информатика и арбитраж
ИТ в криминалистике
Кадровые вопросы в ИТ и профайлинг
и других.

Для освоения учебной дисциплины, студенты должны владеть основами следующих знаний и компетенций:
базовыми понятиями и указанных выше областей знаний;
понятиями базовых разделов математики;
применять понятийно-категориальный аппарат;
использовать правовые нормы в профессиональной и общественной деятельности;
защищать права на интеллектуальную собственность;
владеть навыками философского мышления для выработки системного, целостного взгляда на окружающий мир и имеющиеся в нем проблемы;
навыками публичной речи, аргументации, ведения дискуссии.

II. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Тема 1. Философия обеспечения информационной и кибербезопасности бизнеса.

Парадигма ИБ бизнеса. Взаимодействие бизнеса и органов ИБ. Уязвимости, угрозы и инциденты ИБ. Катастрофоустойчивость ИКТ. Отраслевые вопросы обеспечения ИБ. Понятие кибербезопасности и современные подходы ее обеспечения. Цифровая экономика и цифровая безопасности. Философия новых подходов к цифровой безопасности.

Тема 2. Нормативно-правовое обеспечение ИБ в РФ и за рубежом.

Государственная система мер по обеспечению информационной безопасности. Госорганы - регуляторы, вовлечённые в эти процессы. Правовые акты, стандарты, рекомендации.

Лицензирование и сертификация в отрасли. Сходство и различие подходов к регулированию ИБ в РФ и за рубежом. GDPR и другие Акты. Трансграничная передача данных и места хранения. Ввоз/вывоз криптографических систем.

Тема 3. Организация обеспечения ИБ бизнеса.

Основные функции обеспечения ИБ бизнеса. Процессы ИБ и варианты их организационного обеспечения. Кибербезопасность и ее специфика. Менеджмент ИБ.

Тема 4. Риск ориентированный подход.

Анализ рисков ИБ и управление ими. Стандарты. Технологии анализа информационных рисков. Аудит рисков.

Тема 5. Основные процессы обеспечения ИБ.

IDM, DLP, NGFW, WAF, SIEM и прочие средства защиты информации и ИТ. Новые технологии, включающие машинное обучение и ИИ. Обработка больших данных. Процессы и управление ими. Правовые аспекты, арбитраж и социальная инженерия. Все элементы и механизмы обеспечения ИБ.

Тема 6. Российские и международные стандарты обеспечения ИБ.

- Виды стандартов. Национальные стандарты в области ИБ (финансовая отрасль). Отрас-левые стандарты (стандарты организаций): комплекс СТО БР ИББС. Стандарты, обязательные к исполнению. Взаимодействие стандартов с законодательными актами в области ИБ.

Тема 7. Аудит ИБ.

Определение аудита, основные требования. Схема и особенности проведения аудита ИБ. Внешний и внутренний аудит. Частота проведения аудитов. Технический аудит (пен тест). Стандарты аудита. Отраслевая специфика.

Тема 8. Особенности обеспечения ИБ в различных отраслях (финансовый, телекоммуникационный, нефтегазовый секторы).

Организация и управление процессами обеспечения ИБ и кибербезопасности в финансвом секторе. Особенности выполнения требований ИБ в банках, брокерских компаниях, у страховщиков и НПФ.. Специфика операторов связи.

Тема 9. Участие в расследованиях нарушений.

Организация внутренних расследований нарушений требований ИБ. Внутренняя нормативнометодическая база. Сбор и сохранение улик по фактам компьютерных нарушений. Работа с правоохранительными органами. Стандарты.

III. ОЦЕНИВАНИЕ.

Итоговая оценка по учебной дисциплине складывается из следующих элементов:
• опрос по материалам лекций;
• работа на практических занятиях (доклады, обсуждения, к/р);
• реферат, эссе, презентация;
• экзамен.

Структура экзаменационной оценки по учебной дисциплине:
Вклад в накопленную оценку (%):
-Опрос по материалам лекций (теория) 30
-Работа на практических занятиях (доклады, обсуждения, к/р) 30
-Реферат (к/р) 40
Накопленная оценка по 10-ти бальной системе округляется в большую сторону.

Итоговая оценка вычисляется как половина суммы накопленной оценки и оценки экзамена, округленной в большую сторону.

IV. ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ

Все возможные оценочные средства перечислены в предыдущем пункте.

V. РЕСУРСЫ

a. Основная литература

1. Крысин, А. В. Информационная безопасность: практ. рук. / А. В. Крысин. – М.: Спаррк; Киев: Век+, 2003.
2. Романовский В. И. Теория вероятностей, статистика и анализ

b. Дополнительная литература

1. Одинцов, А. А. Защита предпринимательства: Экономическая и информационная безопасность: Учеб. пособие для вузов / А. А. Одинцов. – М.: Междунар. отношения, 2003.
2. Огнев, Е. Информационная безопасность и защита критически важных структур. Государственная служба, 2010, N.2., с.. 117-118.
3. Ярочкин, В. И. Информационная безопасность: учебник для вузов. М.: Академический Проект: Трикста, 2005.
4. Нестеров, С. А. Информационная безопасность: учебник и практикум для акад. бакалавриата. М.: Юрайт, 2016. – (Сер. "Университеты России") .
5. Lange K. Applied probability. Серия: Springer texts in statistics. Springer, 2010 г.

6. Gordon H. Discrete probability. Серия: Undergraduate texts in mathematics. Springer, 1997 г.

7. Баруча-Рид А. Т. Элементы теории марковских процессов и их приложения. Наука. Гл. ред. физ.-мат. лит., 1969.

8. Лидбеттер М. Экстремумы случайных последовательностей и процессов. Мир, 1989 г.

c. 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)*

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

№ п/п	Наименование	Условия доступа

	Профессиональные базы данных, информационно-справочные системы	
1.	Консультант Плюс	*Из внутренней сети университета (договор)*
2.	Электронно-библиотечная система Юрайт	URL: https://biblio-online.ru/
	Интернет-ресурсы (электронные образовательные ресурсы)	
1.	Открытое образование	URL: https://openedu.ru/

е. 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.