МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный экономический университет»

УТВЕРЖДАЮ
Проректор по учебной и методической работе
_____/Шубаева В.Г./
«28» августа 2020 г.

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Рабочая программа дисциплины

Направление подготовки	10.03.01 Информационная безопасность
Направленность (профиль) программы	Безопасность компьютерных систем (в экономике и управлении)
Уровень высшего образования	бакалавриат
Форма обучения	очная

Составитель:
_____/к.ф.-м.н., доцент Васильева И.Н.

Санкт-Петербург
2020

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ 3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ 3
4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ 4
5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ 4
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА 5
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 5
7.1. Методические указания для обучающегося по освоению дисциплины 5
7.2. Организация самостоятельной работы 6
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 6
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 7
9.1 Учебно-методическое и информационное обеспечение дисциплины 7
9.2. Материально-техническое обеспечение учебного процесса 8
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 8
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 8

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель (цели) освоения дисциплины: изучение основ и подходов современного менеджмента организации, сложившихся международных практик и методик управления в сфере информационной безопасности.

Задачи:

- получение теоретических знаний в области современного корпоративного менеджмента в сфере информационной безопасности (ИБ);
- ознакомление с международными и национальными стандартами, затрагивающими вопросы управления ИБ;
- овладение практическими приемами разработки политики безопасности,
- получение представления о методах оценки и управления рисками ИБ;
- овладение практическими навыками, необходимыми для разработки, внедрения и сертификации системы менеджмента информационной безопасности организации;
- закрепление теоретических знаний в среде прикладных программ специального назначения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.Б. Основы управления информационной безопасностью относится к базовой части дисциплин Блока 1 и является обязательной для освоения обучающимся вне зависимости от направленности (профиля) программы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы представлены в таблице 3.1.

Таблица 3.1 – Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование компетенции выпускника	Этапы формирования компетенций	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
ОПК-7 – способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Третий уровень (продвинутый) (ОПК-7)-З	Декомпозиция II Знать: классификацию активов предприятия, угроз и уязвимостей информационной безопасности З3 (II)(ОПК-7) Уметь: определять виды и формы информации, подверженной угрозам, возможные угрозы и риски информационной безопасности; выявлять требования и ограничения информационной безопасности с учетом специфики организации. У3(II) (ОПК-7) Владеть: методами оценки информационной безопасности организации; навыками разработки политик (правил, процедур) информационной безопасности предприятия. В3 (II)(ОПК-7)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

Форма промежуточной аттестации: зачет – 6 семестр.

Распределение фонда времени по темам по очной форме обучения представлено в таблице 4.1

Таблица 4.1 – Распределение фонда времени по темам дисциплины (очная форма обучения)

Номер и наименование тем	Объем дисциплины (ак. часы)			
	Контактная работа			СРО
	ЗЛТ	ПЗ	ЛР	
1	*2*	*3*	*4*	*5*
Тема 1. Основы корпоративного управления и политики ИБ	4	2		10
Тема 2. Развитие стандартов ИБ	4	2		10
Тема 3. Процессный подход к обеспечению ИБ	2			8
Тема 4. Система менеджмента ИБ	4	4		10
Тема 5. Управление рисками ИБ	4	6		14
Тема 6. Оценка ИБ компании	4	6		14
Всего по дисциплине:	22	20		66

*ЗЛТ – занятия лекционного типа, ПЗ – все виды занятий семинарского типа, кроме лабораторных работ, ЛР – лабораторные работы, СРО – самостоятельная работа обучающегося

5. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

Тема 1. Основы корпоративного управления и политики ИБ

Основные направления обеспечения информационной безопасности организации. Риск-ориентированный подход. Понятие корпоративной политики безопасности. Основные требования и подходы к разработке политики безопасности. Многоуровневый подход.

Управления информационной безопасностью на основе соответствий требованиям (compliance management). Анализ упущений (gap-анализ). Модель непрерывного совершенствования (замкнутый цикл менеджмента PDCA).

Тема 2. Развитие стандартов ИБ

Уровни организации деятельности по обеспечению информационной безопасности компании и общая структура стандартов информационной безопасности. Оценочные стандарты информационной безопасности («Оранжевая книга», ITSEC, ISO/IEC 15408 «Общие критерии»). Статус стандартов ISO/IEC в РФ.

«Лучшие практики» информационной безопасности (стандарты BSI, BS 7799 / ISO/IEC 17799, 27002).

Стандарты менеджмента информационной безопасности. Состав и структура серии международных стандартов ISO/IEC 2700x. Российские гармонизированные стандарты.

Национальные стандарты и стандарты саморегулируемых организаций в сфере управления информационной безопасностью и информационными технологиями (BS-100, NIST 800, ITIL, ISM 3, Cobit). Сервис-ориентированный и процессно-ориентированный подходы к управлению ИБ и ИТ. Концепция корпоративного управления информационной безопасностью (IS Governance).

Эволюция модели информационной безопасности.

Тема 3. Процессный подход к обеспечению ИБ

Суть процессного подхода. Классификация и атрибуты процессов. Процессы управления и обеспечения информационной безопасности. Эталонная модель процесса для управления ИБ (ГОСТ Р 57640-2017, ISO/IEC TS 33052:2016). Проблемы внедрения процессного подхода.

Тема 4. Система менеджмента ИБ

Построение системы менеджмента информационной безопасности (СМИБ) на основе ISO/IEC 27001. Организационная структура системы менеджмента информационной безопасности. Система частных менеджментов. Сертификация соответствия СМИБ ISO/IEC 27001.

Тема 5. Управление рисками ИБ

Управление рисками информационной безопасности на основе ISO 27005. Процедуры оценки и обработки рисков. Методология оценки рисков ИБ.

Тема 6. Оценка ИБ компании

Виды и способы оценки информационной безопасности. Процесс оценки (аудита) ИБ. Метрики информационной безопасности (ISO/IEC 27004, NIST 800-55).

Оценка процессов информационной безопасности на основе моделей зрелости (ГОСТ Р ИСО/МЭК 33020-2017, ISO 21827, ISO 15504).

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Оценочное средство
1	*2*	*3*
1	Разработка политики безопасности компании	ПЗ, Групповой тренинг
2	Задача 1. Оценка соответствия ГОСТ Р ИСО/МЭК 27002	ПЗ, Решение практических задач, отчет. Индивидуальное контрольное задание №1
4	Задача 2. Идентификация и оценка активов объекта защиты	ПЗ, Решение практических задач, отчет
	Задача 3. Идентификация и оценка угроз ИБ объекта защиты	
5	Задача 4. Идентификация и анализ рисков информационной безопасности объекта защиты	ПЗ, Решение практических задач, отчет. Индивидуальное контрольное задание №2
6	Задача 5. Изучение методики СТО БР ИББС оценки ИБ Задача 6. Анализ уровня защищенности и риска ИБ организации с помощью MSAT	ПЗ, Решение практических задач, отчет

* ПЗ – практические занятия, СЗ – семинарские занятия, ЛР – лабораторные работы

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

7.1. Методические указания для обучающегося по освоению дисциплины

Для формирования четкого представления об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине в самом начале учебного курса обучающийся должен ознакомиться с учебно-методической документацией:

– рабочей программой дисциплины: с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, перечнем знаний и умений, которыми в процессе освоения дисциплины должен владеть обучающийся,

– порядком проведения текущего контроля успеваемости и промежуточной аттестации;

– графиком консультаций преподавателей кафедры.

Систематическое выполнение учебной работы на занятиях лекционных и семинарских типов, а также выполнение самостоятельной работы позволит успешно освоить дисциплину.

В процессе освоения дисциплины обучающимся следует:

– слушать, конспектировать излагаемый преподавателем материал;
– ставить, обсуждать актуальные проблемы курса, быть активным на занятиях;
– задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений;
– выполнять задания практических занятий полностью и установленные сроки.

При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале не удалось, то обратится к лектору (по графику его консультаций) или к преподавателю на занятиях семинарского типа.

Обучающимся, пропустившим занятия (независимо от причин), не имеющим письменного решения задач или не подготовившимся к данному занятию, рекомендуется не позже чем в 2 - недельный срок явиться на консультацию к преподавателю и отчитаться по теме.

7.2. Организация самостоятельной работы

Под самостоятельной работой обучающихся понимается планируемая работа обучающихся, направленная на формирование указанных компетенций, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, без его непосредственного участия.

Методическое обеспечение самостоятельной работы при наличии обучающихся лиц с ограниченными возможностями представляется в формах, адаптированных к ограничениям их здоровья.

Виды самостоятельной работы по дисциплине представлены в таблице 7.2.1.

Таблица 7.2.1 – Организация самостоятельной работы обучающегося

№ темы	Вид самостоятельной работы
1	*2*
1	Изучение нормативных документов и литературных источников, подготовка к ПЗ, подготовка по контрольным вопросам.
2	Изучение нормативных документов и литературных источников, подготовка к ПЗ, подготовка по контрольным вопросам.
3	Изучение нормативных документов и литературных источников, подготовка по контрольным вопросам.
4	Изучение нормативных документов и литературных источников, подготовка к ПЗ, подготовка по контрольным вопросам.
5	Изучение нормативных документов и литературных источников, подготовка к ПЗ, подготовка по контрольным вопросам.
6	Изучение нормативных документов и литературных источников, подготовка к ПЗ, подготовка по контрольным вопросам.
1-2	Подготовка к контрольной точке №1.
5	Подготовка к контрольной точке №2.

Каждый вид СРО, указанный в таблице 7.2.1 обеспечен методическими материалами.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «*Основы управление информационной*

безопасностью» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

К интерактивным методам обучения относятся:

- групповой тренинг по теме 1;

- выполнение индивидуальных заданий на ПК в ходе практических занятий и самостоятельной работы по темам 2,4,5,6.

Групповой тренинг предполагает имитацию особой учебно-экспериментальной обстановки, позволяющей студентам освоить нестандартные подходы к решению проблем, используя новые техники и тактики, излагаемые преподавателем и демонстрируемые в ходе занятия.

Выполнение индивидуальных заданий на ПК предполагает решение практических задач по идентификации и анализу активов предприятия, угроз и рисков ИБ с помощью пакетов прикладных программ, изучению специального программного обеспечения, используемого для решения профессиональных задач в сфере оценки и управления ИБ компании.

9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1 Учебно-методическое и информационное обеспечение дисциплины

Таблица 9.1.1 – Учебно-методическое обеспечение дисциплины

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	**Основная/ дополнительная литература**	**Книгообеспеченность**	
		Кол-во экз. в библ. СПбГЭУ	**Электронные ресурсы**
Шилов А.К. Управление информационной безопасностью: учебное пособие. — Электрон. дан. – Ростов-на-Дону: Издательство Южного федерального университета (ЮФУ), 2018. – 120 с.	основная	–	ЭБС ZNANIUM
Васильева И.Н. Управление информационной безопасностью : учебное пособие / И.Н.Васильева. – Санкт-Петербург: Изд-во СПбГЭУ, 2014. – 82 с. — Сведения доступны также по Интернету.	основная	58	ЭБ OPAC.UNECON.RU
Веселов Г.Е. Менеджмент риска информационной безопасности: учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. — Электрон. дан. - Таганрог:Южный федеральный университет, 2016. - 107 с.	дополнительная	–	ЭБС ZNANIUM
Васильева И.Н. Управление рисками информационной безопасности : учебное пособие - Электрон. текстовые дан. - Санкт-Петербург: Изд-во СПбГЭУ, 2016. – 177 с.	дополнительная		ЭБ OPAC.UNECON.RU

Таблица 9.1.2 – Перечень современных профессиональных баз данных (СПБД)

№	Наименование СПБД
1	Электронная библиотека Grebennikon.ru – www.grebennikon.ru
2	Научная электронная библиотека eLIBRARRY – www.elibrary.ru
3	Научная электронная библиотека КиберЛеника – www.cyberleninka.ru
4	База данных ПОЛПРЕД Справочники – www.polpred.com
5	База данных OECD Books, Papers & Statistics на платформе OECD iLibrary – www.oecd-ilibrary.org

Таблица 9.1.3 – Перечень информационных справочных систем (ИСС)

№	Наименование ИСС
1	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
2	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
3	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
4	Электронная библиотечная система BOOK.ru - www.book.ru
5	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
6	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
7	Электронная библиотека СПбГЭУ– opac.unecon.ru

9.2. Материально-техническое обеспечение учебного процесса

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Таблица 9.2.1 – Перечень программного обеспечения (ПО)

№ п/п	Наименование ПО
1	Microsoft Windows Professional (КОНТРАКТ № 244/20 «26» июня 2020 г
2	Microsoft Office Professional (КОНТРАКТ № 244/20 «26» июня 2020 г)
3	7-Zip (freeware)

10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья Университет обеспечивает:

– для инвалидов и лиц с ограниченными возможностями здоровья по зрению: размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме справочной информации о расписании учебных занятий; присутствие ассистента, оказывающего обучающемуся необходимую помощь; выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

– для инвалидов и лиц с ограниченными возможностями здоровья по слуху: надлежащими звуковыми средствами воспроизведение информации;

– для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата: возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения кафедры, а также пребывание в указанных помещениях.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом и является приложением к рабочей программе дисциплины (модуля).