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.

ЗАЩИТА СЕТЕВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

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.т.н., доцент Чернокнижный Г.М.

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 5
6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА 6
7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ 7
7.1. Методические указания для обучающегося по освоению дисциплины 7
7.2. Организация самостоятельной работы 7
8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 8
9. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ 8
9.1 Учебно-методическое и информационное обеспечение дисциплины 8
9.2. Материально-техническое обеспечение учебного процесса 9
10. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ 9
11. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ 10

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цель (цели) освоения дисциплины: дать студентам необходимые знания, умения и навыки защиты сетевых информационных технологий (ИТ) с применением современных программно-аппаратных средств, необходимые для использования их в работе в компаниях, нуждающихся в защите конфиденциальной информации

Задачи:

- расширить теоретические знания студентов в прикладных областях знаний для использования при защите информации в компьютерных сетях;
- сформировать представления о компьютерных атаках и методах их обнаружения;
- выработать практические навыки выявления и анализа угроз;
- дать студентам необходимые теоретические сведения и практические навыки работы с современными системами обнаружения вторжений, системами защиты информации в различных средах, в том числе, виртуальной и облачной.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В.ДВ. «Защита сетевых информационных технологий» относится к выборным дисциплинам части дисциплин Блока 1 и является обязательной для освоения обучающимся после их выбора.

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)
ПК-1. способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	***Второй уровень (углубленный) (ПК-1) –2***	***Декомпозиция II*** ***Знать*** принципы работы программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (СЗИ). *З2 (II)(ПК-1)* ***Уметь:*** выполнять работы по обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических СЗИ. *У2(II) (ПК-1)* ***Владеть:*** способностью выполнять работы по установке и настройке программных, программно-аппаратных (в том числе криптографических) и технических СЗИ. *В2 (II)(ПК-1)*
ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты	***Второй уровень(углубленный) (ПК-3) –2***	***Декомпозиция I*** ***Знать:*** принципы защиты подсистем информационной безопасности (ИБ) объекта защиты с помощью программно-аппаратных средств. *З2 (I)(ПК-3)* ***Уметь:*** администрировать подсистемы ИБ объекта защиты с использованием программно-аппаратных средств. *У2(I) (ПК-3)* ***Владеть:*** способностью планировать и проводить ремонтно-восстановительные работы и модернизацию

Код и наименование компетенции выпускника	Этапы формирования компетенций	Планируемые результаты обучения/индикаторы достижения компетенций (показатели освоения компетенции)
		подсистем ИБ объекта защиты *В2 (I)(ПК-3)*
ПСК-1.2 способность администрировать средства защиты информации в компьютерных системах и сетях	***Второй уровень (углубленный) (ПСК-1.2) –2***	***Знать:*** достоинства и недостатки сертифицированных операционных систем с точки зрения информационной безопасности *З2(ПСК-1.2)* ***Уметь***: настраивать работу сетевых операционных систем в безопасном режиме *У2 (ПСК-1.2)* ***Владеть:*** способностью администрировать средства защиты информации в компьютерных системах и сетях *В2 (ПСК-1.2)*

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов, из которых 36 часов самостоятельной работы обучающегося отводится на подготовку и защиту экзамена

Форма промежуточной аттестации: экзамен 7 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
1.1. Компьютерные атаки и их обнаружение	1			6
1.2. Анализаторы сетевых пакетов	1	4		6
1.3. Средства сканирования сети	2	6		6
2.1. Межсетевые экраны	2	4		8
2.2. Виртуальные частные сети	2	4		8
2.3. Системы обнаружения вторжений	2	4		6
2.4. Средства защиты информации от несанкционированного доступа	2	6		8
2.5. SIEM-системы	1	4		6
2.6. Системы защиты от утечек	2	10		6
2.7. Безопасность в беспроводной среде	2			8
2.8. Безопасность электронной почты	1			6
2.9. Защита виртуальной среды	1			6
2.10. Безопасность облачных вычислений	1			6
3.1. Резервирование электропитания	1			4
3.2. Резервное копирование данных	1	6		6
3.3. Отказоустойчивость дисков	1			6
3.4. Методы кластеризации	1			6
Всего по дисциплине:	**24**	**48**		**108**

*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

Раздел 1. Средства анализа сети

1.1. Компьютерные атаки и их обнаружение
Основные понятия. Классификация атак. Основные типы атак. Сценарий атаки.

1.2. Анализаторы сетевых пакетов
Wireshark. TcpDump. Network Monitor.

1.3. Средства сканирования сети
Примеры сетевого сканирования. Обзор сетевых сканеров.

Раздел 2. Средства защиты сети

2.1. Межсетевые экраны
Технология межсетевого экранирования. Фильтрация пакетов. Шлюзы прикладного уровня. Средства межсетевого экранирования

2.2. Виртуальные частные сети.
VPN канального уровня. VPN сетевого уровня, VPN транспортного уровня. Примеры построения VPN.

2.3. Системы обнаружения вторжений.
Общие сведения. Направления развития СОВ. Классификация систем обнаружения вторжений. Система обнаружения вторжений Snort. Примеры сертифицированных СОВ. Методы обхода СОВ.

2.4.Средства защиты информации от несанкционированного доступа
Secret Net Studio. Dallas Lock. Блокхост-Сеть 2.0.

2.5.SIEM-системы
Архитектура SIEM-систем. Назначение и функции SIEM-систем. Архитектура SIEM-систем. Обзор популярных SIEM-систем. Система OSSIM. Обзор существующих SIEM-систем.

2.6. Системы защиты от утечек
Назначение и функции DLP-систем. Архитектура DLP-систем. Обзор популярных DLP-систем. Система Falcongaze. Система Infowach.

2.7.Безопасность в беспроводной среде
Безопасность стандарта IEEE 802.11. Безопасность технологии Bluetooth. Безопасность в сетях IEEE 802.16. Обнаружение вторжений в беспроводную сеть.

2.8.Безопасность электронной почты
Протоколы электронной почты - SMTP, POP3, IMAP4. Спам. Средства защиты электронной почты.

2.9.Защита виртуальной среды
Проблема обеспечения безопасности виртуальной среды Нормативные документы по защите виртуальной среды. Средства защиты информации платформ виртуализации.

2.10. Безопасность облачных вычислений
Предпосылки появления и развития облачных вычислений. Виды облачных услуг. Угрозы безопасности в облаке. Организационные меры и средства защиты информации в облачной среде. Особенности проведения мероприятий по защите ИС на основе облачных технологий в России.

Раздел 3. Защита сетевого оборудования от краха

3.1. Резервирование электропитания
Источники бесперебойного питания. Автономные генераторы.

3.2. Резервное копирование данных

Что следует копировать. Когда выполнять резервное копирование. Как следует выполнять резервное копирование

3.3. Отказоустойчивость дисков

RAID уровня 1. RAID уровня 3. RAID уровня 5.

3.4. Методы кластеризации

Кластеры с балансировкой нагрузки. Вычислительные кластеры. Grid-вычисления.

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Таблица 6.1 – Практические занятия/Семинарские занятия/Лабораторные работы

№ темы	Тема занятия	Вид занятия/Наименование оценочного средства
1	*2*	*3*
1.2.	Работа с Wireshark. TcpDump. Network Monitor. Nmap.	ПЗ, Решение практических задач, отчет
1.3.	Работа с XSpider, MaxPatrol, ВС-сканер	ПЗ, Решение практических задач, отчет, Индивидуальное задание № 1
2.1.	Настройка межсетевого экрана Comodo	ПЗ, Решение практических задач, отчет
2.2.	VPN VIPNET: создание туннеля и полутуннеля	ПЗ, Решение практических задач, отчет
2.3.	Настройка и применение СОВ Snort	ПЗ, Решение практических задач, отчет
2.4.	Работа с Secret Net Studio. Dallas Lock. Блокхост-Сеть 2.0	ПЗ, Решение практических задач, отчет, Индивидуальное задание № 2
2.5.	Исучение работы SIEM-системы OSSIM	ПЗ, Решение практических задач, отчет
2.6.	Изучение DLP-системы Falcogaze	ПЗ, Решение практических задач, отчет
	Изучение DLP-системы Infowach	
3.2	Создание резервных копий в Windows Server 2016	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*
1.2.	Подготовка к выполнению и защите отчета по выполнению практического задания. Подготовка к экзамену.
1.3.	Подготовка к выполнению контрольной точки 1. Подготовка к экзамену.
2.1.	Подготовка к выполнению и защите отчета по выполнению практического задания. Подготовка к экзамену.
2.2.	Подготовка к выполнению и защите отчета по выполнению практического задания. Подготовка к экзамену..
2.3.	Подготовка к выполнению и защите отчета по выполнению практического задания. Подготовка к экзамену
2.4.	Подготовка к выполнению контрольной точки 2. Подготовка к экзамену
2.5.	Подготовка к выполнению и защите отчета по выполнению практического задания. Подготовка к экзамену.
2.6.	Подготовка к выполнению и защите отчета по выполнению практического задания. Подготовка к экзамену.
2.7.	Подготовка к экзамену.
2.8.	Подготовка к экзамену.
2.9.	Подготовка к экзамену.
2.10.	Подготовка к экзамену.
3.1.	Подготовка к экзамену.
3.2.	Подготовка к экзамену.
3.3.	Подготовка к экзамену
3.4.	Подготовка к экзамену.

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

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения.

Активные и интерактивные методы обучения:

К интерактивным методам обучения относится выполнение индивидуальных заданий на ПК в ходе лабораторных работ в виртуальной среде и самостоятельной работы по темам 1-6.

Выполнение индивидуальных заданий на ПК предполагает выполнение задач по изучению процессов инсталляции и настройки различных ОС, работы пользователя и администратора для обеспечения информационной безопасности операционной среды.

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**
Чернокнижный Г.М. Защита сетевых информационных технологий: учебное пособие . – Санкт-Петербург: Изд-во СПбГЭУ, 2018. – 132 с. — Сведения доступны также по Интернету: opac.unecon.ru .	Основная	35	ЭБ OPAC.UNECON.RU
Чернокнижный Г.М. Вычислительные сети. Контроль безопасности в компьютерных сетях: учебное пособие.— Санкт-Петербург: Изд-во СПбГЭУ, 2016 .— 97 с. – Сведения доступны также по Интернету: opac.unecon.ru.	Основная	35	ЭБ OPAC.UNECON.RU
Чернокнижный Г.М. Операционные системы: учебное пособие / Г.М.Чернокнижный, И.Н.Васильева – Санкт-Петербург: Изд-во СПбГЭУ, 2018. – 176 с.— Сведения доступны также по Интернету: opac.unecon.ru .	Дополнительная	25	ЭБ OPAC.UNECON.RU
Шаньгин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие . — Электрон. дан. — М. : ИД «ФОРУМ» : ИНФРА-М, 2020. — 592 с.	Дополнительная	–	https://znanium.com/catalog/document?id=358722

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 КиберЛенинка – 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).