МИНОБРНАУКИ РОССИИ

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

УТВЕРЖДАЮ
Проректор по образовательной деятельности
В.Г. Шубаева
«24» мая 2023 г.

Расследование инцидентов информационной безопасности

Рабочая программа дисциплины

Направление подготовки/ *Специальность*	*10.03.01 Информационная безопасность*
Направленность (профиль) программы/ *Специализация*	*Безопасность компьютерных систем (в экономике и управлении)*
Уровень высшего образования	*Бакалавриат*
Форма обучения	*очная*
Год набора	*2023*

Составитель*(и)*:

к.физмат.н, Васильева Ирина Николаевна

Часов по учебному плану	108	**Виды контроля в семестрах:**
в том числе:		
контактная работа	64	Зачет: семестр 7
самостоятельная работа	44	
практическая подготовка	0	
часов на контроль	0	

Распределение часов дисциплины:

Семестр:	7
Вид занятий	Часы
Лекционные занятия	36
Практические занятия	
Лабораторные работы	28
Итого аудиторных часов	**64**
Самостоятельная работа	44
Часы на контроль	0
Итого академических часов	**108**
Общая трудоемкость в зачетных единицах	**3**

Санкт-Петербург
2023

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель:	Получение необходимых теоретических знаний и навыков по основным принципам и методам, применяемым при расследования инцидентов нарушений информационной безопасности в общей структуре процессов управления безопасностью, а также основных аспектов практической деятельности команды по расследованию инцидентов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина Б1.В Расследование инцидентов информационной безопасности относится к части, формируемой участниками образовательных отношений Блока 1.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции выпускника	**Код и наименование индикатора достижения компетенций**	**Планируемые результаты обучения по дисциплине**
ПК-5 - Способен выявлять угрозы безопасности информации и анализировать недостатки функционирования системы защиты информации на объектах информатизации	ПК-5.1 - Способен проводить анализ угроз безопасности и недостатков функционирования системы защиты информации, приведших к возникновению инцидентов информационной безопасности	Знать: международные стандарты управления инцидентами информационной безопасности, основы организации работы команды по реагированию на инциденты информационной безопасности, принципы определения компрометации компьютерных систем. Уметь: выявлять затронутые инцидентом компьютерные системы, проводить снятие данных для последующего криминалистического анализа. Владеть: технологиями работы с индикаторами компрометации компьютерных систем.
ПК-6 - Способен выявлять и идентифицировать инциденты в процессе эксплуатации автоматизированных систем	ПК-6.1 - Способен проводить ретроспективный анализ для выявления инцидентов информационной безопасности в компьютерных системах	Знать: основные принципы и процедуры управления компьютерными инцидентами, процедуры реагирования на инциденты в компьютерных системах, основы криминалистики компьютерных систем. Уметь: проводить криминалистический анализ носителей компьютерной информации и оперативной памяти, в том числе, образов дисков и дампов оперативной памяти, на наличие признаков компрометации. Владеть: базовыми техниками и средствами криминалистического анализа компьютерных систем.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ*

Номер и наименование тем и/или разделов/тем	Содержание дисциплины	Объем дисциплины (академические часы)			
		Контактная работа			СРО
		ЗЛТ	ПЗ	ЛР	
Тема 1. Правовая база расследования компьютерных правонарушений и инцидентов информационной безопасности.	Понятия компьютерного правонарушения, преступления в сфере компьютерной информации, преступления в сфере высоких технологий, компьютерного инцидента. Основные нормативно-правовые источники, регламентирующие деятельность по расследованию компьютерных инцидентов. Классификация компьютерных правонарушений. Криминалистическая характеристика компьютерных правонарушений. Способы совершения компьютерных правонарушений. Основные средства совершения атак на компьютерные системы. Жизненный цикл компьютерных атак. Техники, тактики и процедуры нарушителей.	8			8
Тема 2. Основные мероприятия расследования компьютерных правонарушений и инцидентов информационной безопасности.	Взаимодействие с правоохранительными органами. Порядок возбуждения уголовных дел по преступлениям в сфере компьютерной информации и высоких технологий. Опросы свидетелей. Участие специалистов и формы использования специальных познаний в сфере информационных технологий. Осмотр места происшествия. Копирование информации и изъятие носителей информации. Правовые основания выемки средств компьютерной техники, предметов, материалов и документов. Основные оперативно-розыскные мероприятия, нацеленные на установление причин нарушения информационной безопасности, выявление виновных лиц, обнаружение свидетельств компьютерного правонарушения или инцидента ИБ. Назначение компьютерной (технико-компьютерной) экспертизы, технико-криминалистической экспертизы документов и иных экспертиз.	8			8
Тема 3. Организация реагирования на инциденты информационной безопасности.	Международные стандарты управления инцидентами ИБ. Взаимосвязь событий ИБ и инцидентов ИБ. Идентификация событий и инцидентов ИБ. Средства обнаружения и блокирования компьютерных инцидентов (антивирусы, межсетевые экраны, IDS/IPS, DLP, SIEM-системы). Правовое обоснование использования данных мониторинга и DLP-систем. Процедура первичного реагирования на инциденты ИБ. Локализация инцидента. Изолирование и отключение пораженных систем. Идентификация, сбор, получение и хранение свидетельств, представленных в цифровой форме. Общие принципы и этапы процесса управления	8		6	8

	инцидентами ИБ. Роль процесса управления инцидентами ИБ в рамках общей системы управления ИБ. Роли и ответственность в процессе управления инцидентами ИБ. Создание и деятельность группы реагирования на инциденты (CSIRT). Деятельность центров оперативного управления информационной безопасностью (SOC) и центров по реагированию на инциденты (CERT).				
Тема 4. Методы и средства криминалистического исследования компьютерных систем.	Виды и принципы работы с индикаторами компрометации. Описание индикаторов компрометации с помощью YARA правил. Технологии выявления затронутых инцидентом систем. Основные источники свидетельств инцидента ИБ. Технические средства и приемы копирования информации с носителей, снятия образов оперативной памяти, захвата сетевого трафика. Задачи компьютерной криминалистики и виды исследований. Основные этапы криминалистического исследования компьютерных систем. Инструментальные средства исследования компьютерных систем. Технологии исследования носителей информации и восстановления данных. Технологии исследования оперативной памяти и ее дампов.	12		22	20
Контроль:					**0**
Всего по дисциплине:		**36**	**0**	**28**	**44**

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

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Рекомендуемая литература

Библиографическое описание издания (автор, заглавие, вид, место и год издания, кол. стр.)	**Электронные ресурсы**
Васильева И. Н. Расследование инцидентов информационной безопасности : учебное пособие - Санкт-Петербург : Изд-во СПбГЭУ, 2019 - 113 с.	http://opac.unecon.ru/elibrary ... B5%D0%BD%D1%82%D0%BE%D0%B2.pdf
Жукова М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности : Учебное пособие / Сибирский федеральный университет ; Сибирский федеральный университет - Красноярск : Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева", 2012 - 100 с.	http://znanium.com/catalog/document?id=230373

5.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в т.ч. отечественного производства

- 7-Zip
- Oracle VM VirtualBox
- Debian
- Kali Linux
- LibreOffice
- Ubuntu Linux Server
- Wireshark
- PT Industrial Security Incident Manager, конфигурация Education
- RStudio
- ОС Альт образование 10

5.3 Перечень информационных справочных систем (ИСС) и современных профессиональных баз данных (СПБД)

№	Наименование СПБД/ ИСС
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
6.	Справочная правовая система КонсультантПлюс (инсталлированный ресурс СПбГЭУ или www.consultant.ru)
7.	Справочная правовая система «ГАРАНТ» (инсталлированный ресурс СПбГЭУ или www.garant.ru)
8.	Информационно-справочная система «Кодекс» (инсталлированный ресурс СПбГЭУ или www.kodeks.ru)
9.	Электронная библиотечная система BOOK.ru - www.book.ru
10.	Электронная библиотечная система ЭБС ЮРАЙТ – www.urait.ru
11.	Электронно-библиотечная система ЗНАНИУМ (ZNANIUM) – www.znanium.com
12.	Электронная библиотека СПбГЭУ– opac.unecon.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ) групповых и

индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

Помещения оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование учебных аудиторий, перечень	**Адрес (местоположение) учебных аудиторий**
Ауд. 2014 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 56 посадочных мест (стол учебный 28шт.стульев 56шт.), рабочее место преподавателя, стол м/м, доска меловая 2 шт. (односекционная), кафедра 1шт.,стул 1шт.Компьютер Intel i3-2100 2.4 Ghz /4Gb/500Gb/Acer V193 19" - 1 шт., Мультимедийный проектор Optoma x 400 - 1 шт., Экран с электропривод,DRAPER 96 160x210 - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»
Ауд. 2049 Учебная аудитория (для проведения занятий лекционного типа и занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), оборудована мультимедийным комплексом.Специализированная мебель и оборудование: Учебная мебель на 36 посадочных мест, рабочее место преподавателя, доска меловая (односекционная) - 1 шт., стул - 1 шт. Переносной мультимедийный комплект: Ноутбук HP 250 G6 1WY58EA, Мультимедийный проектор LG PF1500G. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»
Ауд. 0007 Компьютерный класс (для проведения практических занятий, курсового проектирования (выполнения курсовых работ) с применением вычислительной техники). Оборудован мультимедийным комплексом. Специализированная мебель и оборудование: Учебная мебель на 33 посадочных места, рабочее место преподавателя, доска меловая - 1 шт., доска маркерная на колесиках - 1 шт., вешалка стойка - 3 шт., жалюзи - 3 шт., Компьютер Intel Core i3 6100/ MSI H110M PRO-D/ ОЗУ DDR4 8GB 2400MHz/SSD SATA III 240Gb/Aerocool Qs-180 400W/Клавиатура + мышь Microsoft400 for Business/монитор Asus VS228DE - 24 шт., Мультимедийный проектор Тип 1 Optoma x 400 - 1 шт., Ноутбук HP 250 G6 1WY58EA - 2 шт.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»

Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	
Ауд. 2021 Лаборатория "Лабораторный комплекс"Специализированная мебель и оборудование: Учебная мебель на 22 посадочных места (22 компьютерных стола, черных кресел 22шт.) Учебная мебель на 42 посадочных мест (парт 21 шт.,) рабочее место преподавателя (компьютерный стол 1шт.)доска, меловая 3-х секционная 1шт., доска маркерная на колесиках 1 ш., часы 1 шт., кафедра 1шт., стол 1шт., тумбочка 1шт., стул изо 4шт., вешалка стойка 2шт., жалюзи 3шт. Компьютер i5-8400/8GB/500GB_SSD/Viewsonic VA2410-mh - 23 шт., Установка демонстрационных учебных фильмов - 1 шт., Компьютер в комплектации системный блок Intel pentium x2 g3250 клавиатура+мышь L (жесткий диск500gb,монитор philips 21.5') - 1 шт. Наборы демонстрационного оборудования и учебно-наглядных пособий: мультимедийные приложения к лекционным курсам и практическим занятиям, интерактивные учебно-наглядные пособия.	191023, г. Санкт-Петербург, ул. Канал Грибоедова, 30/32, литер «А», «Б», «Р»

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩЕГОСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к изучению дисциплины, обучающемуся необходимо ознакомиться со следующими документами:

– учебно-методической документацией;

– локальными нормативными актами, регламентирующими основные вопросы организации и осуществления образовательной деятельности, в том числе регламентирующие порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся;

– графиком консультаций сотрудников профессорско-преподавательского состава.

Уровень и глубина освоения дисциплины определяются активной и систематической работой обучающихся на лекционных занятиях, занятиях семинарского типа, выполнением самостоятельной работы, в том числе в части выделения наиболее значимых и актуальных проблем для дальнейшего изучения. Особым условием качественного освоения дисциплины является эффективная организация труда, позволяющая распределить учебную нагрузку равномерно в соответствии с графиком учебного процесса.

При подготовке к учебным занятиям обучающимся предоставляется возможность посещения консультаций сотрудников профессорско-преподавательского состава СПбГЭУ согласно расписанию, установленному в графике консультаций.

Аудиторная и внеаудиторная работа обучающихся должна быть направлена на формирование:

- фундаментальных основ мировоззрения обучающихся и естественнонаучного познания;
- базисных знаний, соответствующих направлению подготовки и заявленной профессиональной области, формирующих целевую и профессиональную основу для подготовки кадров;
- профессиональных компетенций ориентированных на удовлетворение потребностей рынка труда;
- индивидуальной траектории посредством освоения уникального набора профессиональных компетенций дополняющих компетентностную модель обучающегося, за счет ориентации на конкретные профессиональные специализированные области знаний, определяемые представителями рынка труда;
- метанавыков обучающихся, таких как: командная работа и лидерство, анализ данных, цифровые навыки, разработка и реализация проектов, межкультурное взаимодействие.

8. 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.

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Контрольные вопросы и задания к промежуточной аттестации

Рабочей программой дисциплины не предусмотрено.

1.2 Темы письменных работ

Рабочей программой дисциплины не предусмотрено.

1.3 Контрольные точки

Номер контрольной точки	Тип контрольной точки	Способ проведения	Номера тем
1	Эссе	письменно	1-4
2	Имитационное упражнение	с помощью технических средств и информационных систем	3-4
3	Текущий контроль	с помощью технических средств и информационных систем	1-4

1.4 Другие объекты оценивания

Рабочей программой дисциплины не предусмотрено.

1.5 Самостоятельная работа обучающегося

Наименования самостоятельной работы	Номера тем
Работа с аналитическими базами данных, нормативными документами, справочной литературой	1-3
Решение профессиональных задач	3-4
Подготовка к лекционным и практическим занятиям	1-4

1.6 Шкала оценивания результата

Шкалы оценивания и процедуры оценивания результатов обучения **по дисциплине** регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования и Положением о балльно-рейтинговой системе.

Для оценки сформированности результатов обучения по дисциплине используется **балльно-рейтинговая система успеваемости обучающихся:**

Формой итогового контроля по дисциплине является зачет, итоговый результат формируется в соответствии со шкалой, приведенной ниже в таблице:

Баллы	Оценка
<55	Незачет
>=55	Зачет

Шкала оценивания результата

2 (балл до 54)	Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены. Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат.
3 (балл 55-69)	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер.
4 (балл 70-84)	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения.
5 (балл 85-100)	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход.