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.

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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 3
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 7
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 освоения дисциплины: дать студентам необходимые знания по основным принципам и методам, применяемым при расследовании инцидентов нарушений информационной безопасности в общей структуре процессов управления безопасностью, а также основных аспектов практической деятельности команды по расследованию инцидентов.

Задачи:

- приобретение знаний в области информационной безопасности в части принципов и этапов проведения расследования инцидентов ее нарушения;
- формирование умения определять состав защищаемой информации предприятия, разработки набора процедур, описывающих действие сотрудников организации в случае инцидента информационной безопасности;
- овладение навыками работы с источниками информации о нарушениях информационной безопасности, методами и средствами сбора и анализа улик, профессиональной терминологией.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина ФТД «Расследование инцидентов информационной безопасности» относится к факультативным дисциплинам и является необязательной для изучения при освоении образовательной 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)
ПК-10 - способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10	Знать: современное состояние, классификацию и тенденции развития нормативно-правовой базы информационной безопасности в области расследования инцидентов информационной безопасности З(ПК-10)

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 2 зачетных единиц, 72 часа.

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. Понятие компьютерного инцидента. Политика расследования инцидентов информационной безопасности	8			8
Тема 2. Организация реагирования на инциденты	8			8
Тема 3. Методы и средства обнаружения и блокирования компьютерных инцидентов	10			10
Тема 4. Оценка ущерба от произошедшего нарушения информационной безопасности и устранение негативных последствий инцидентов	10			10
Всего по дисциплине:	36			36

*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. Понятие компьютерного инцидента. Политика расследования инцидентов информационной безопасности

Предмет, цели, задачи и содержание дисциплины «Расследование инцидентов нарушений информационной безопасности». Роль и место дисциплины в подготовке бакалавров информационной безопасности.

Определение компьютерного инцидента. Проблема. Известная ошибка. Язык инцидентов и проблем.

Компьютерный инцидент как следствие невозможности создания абсолютной защиты Инциденты, причиной которых являются намеренно осуществляемые нападения на информационные ресурсы предприятия. Примеры инцидентов.

Цели и место политики расследования инцидентов в общей структуре процессов управления безопасностью и организацией в целом. Состав, структура, функциональные обязанности, зоны ответственности, роли, правила внутриорганизационного взаимодействия. Оценка критериев качества работы команды по расследованию инцидентов. Разработка форм отчётности и регламента оповещений об инциденте, разработка набора процедур, описывающих действие сотрудников организации в случае инцидента информационной безопасности.

Тема 2. Организация реагирования на инциденты

Фиксация времени. Оценка ситуации и определение пораженных информационных систем. Локализация инцидента. Изолирование и отключение пораженных систем. Сбор улик и иной доказательной базы. Восстановление работоспособности пораженных систем. Проведение расследования и анализ инцидента. Регистрация информации об инциденте. Меры по предотвращению рецидива.

Запись сетевого трафика. Сбор журналов с атакованных систем. Создание «снимков» памяти. Создание «снимков» дисков. Изъятие и «консервация» дисков. Сбор журналов сетевых, защитных и других смежных систем.

Восстановление хронологии событий. Определение причин и технических деталей реализации инцидента. Определение деструктивной составляющей инцидента. Определение виновников и причастных лиц. Установление местоположения.

Отчет должен содержать: восстановленную хронологию событий, описание проведенных исследований с подтверждающими материалами, информацию о виновниках и причастных лицах, анализ последствий и рекомендации по предотвращению (сокращению) ущерба, рекомендации по предотвращению и по выявлению подобных инцидентов, рекомендации по привлечению к ответственности.

Тема 3. Методы и средства обнаружения и блокирования компьютерных инцидентов

Системные журналы (логи, история команд). Сетевой трафик. Исполняемые процессы. Содержимое оперативной памяти. Открытые сетевые соединения.
Открытые порты. Открытые файлы. Файлы и файловая система. Архивы (электронной почты, теневых копий DLP-систем). Журналы систем защиты (антивирусы, IDS и т.д.)
Синхронизация времени. Централизованный сбор, анализ и хранение системных событий. Резервные копии. Архивы (электронной почты, теневых копий DLP-систем). Системы защиты (антивирусы, межсетевые экраны, IDS/IPS). Настройка правил журналирования. Подготовка технических средств. Определение и документирование порядка действий.

Программные средства: EnCase Forensic (guidance software), DFF (Digital Forensics Framework), SANS Investigative Forensic Toolkit ("SIFT").

Аппаратные средства: коллекторы сетевого трафика, дамперы, памяти, устройства защиты от записи.

Средства общего назначения: сниферы и анализаторы сетевого трафика, дебагеры, анализаторы логов.

Тема 4. Оценка ущерба от произошедшего нарушения информационной безопасности и устранение негативных последствий инцидентов

Информационные системы (и сегменты сети), затронутые инцидентом. Ущерб от инцидента. Возможные источники. Определение стратегии и целей управления инцидентом.

Смена скомпрометированных паролей отдельных пользователей, переустановка поврежденных операционных систем и поврежденного программного обеспечения и восстановление их конфигурации, восстановление поврежденной информации (баз данных).

6. ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА

Не предусмотрены.

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	Подготовка к контрольному опросу.
2	Подготовка к контрольному опросу.
3	Подготовка к выполнению индивидуального задания. Подготовка к контрольному опросу.
4	Подготовка к выполнению индивидуального задания. Подготовка к контрольному опросу.

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 самостоятельной работы по темам 3,4.

Выполнение индивидуальных заданий на ПК предполагает выполнение индивидуальных заданий по изучению пакетов прикладных программ, языков программирования, информационно-коммуникационных технологий (как правило, организационной формой таких занятий являются лабораторные работы).

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**
Жукова М.Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. — Электрон. дан. - Красноярск : Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2012 .— 100 с.	основная	–	ЭБС ZNANIUM
Особенности противодействия киберпреступности подразделениями уголовного розыска: учебно-методическое пособие / Б.П. Михайлов [и др.] ; под ред. Б.П. Михайлова, Е.Н. Хазова. — Электрон. дан. — М. : ЮНИТИ-ДАНА: Закон и право, 2017. — 151 с.	дополнительная	–	ЭБС ZNANIUM

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, 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).