

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Вишневский Дмитрий Александрович
Должность: Ректор
Дата подписания: 30.04.2025 11:55:50
Уникальный программный ключ:
03474917c4d012283e5ad996a48a5e70bf8da057

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и
автоматизации производственных процессов
Кафедра интеллектуальных систем и информационной безопасности



УТВЕРЖДАЮ
И.о. проректора
по учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Расследование инцидентов информационной безопасности
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Расследование инцидентов информационной безопасности» является формирование у будущих специалистов теоретических знаний и практических навыков для решения научно-исследовательских и прикладных задач.

Задачи изучения дисциплины. Формирование у студентов теоретических знаний в области расследования инцидентов информационной безопасности, а также навыков практического применения полученных знаний. Изучение разделов: формирование политики управления инцидентами; оценка событий инцидента информационной безопасности; сдерживание, устранение инцидента и восстановление после него; определение инцидента внедрения вредоносного кода; матрицы для определения значимости инцидентов; правовые основы реагирования на инциденты.

Дисциплина направлена на формирование общепрофессиональных (ОПК-5.1, ОПК-5.3) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в элективные дисциплины БЛОКА 1 «Дисциплины (модули)» подготовки студентов по специальности 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: : «Информатика», «Социология и психология управления», «Основы информационной безопасности», «Физические основы построения технических средств защиты информации», «Безопасность систем баз данных», «Безопасность операционных систем», «Методы и средства криптографической защиты информации», «Защита информации от утечки по техническим каналам».

Является основой для изучения следующих дисциплин: «Управление информационной безопасностью». Приобретенные знания, могут быть использованы при подготовке и защите выпускной квалификационной работы, при прохождении практики, а также в профессиональной деятельности.

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с применением знаний в области информационной безопасности.

Курс является фундаментом для ориентации студентов в сфере разработки систем информационной безопасности.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), практические (36 ак.ч.) занятия, самостоятельная работа студента (72 ак.ч.).

Дисциплина изучается на 5 курсе в 9 семестре. Форма промежуточной аттестации – зачет.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Расследование инцидентов информационной безопасности» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ОПК-5.1	ОПК-5.1.2 Реализует политику информационной безопасности открытых информационных систем
Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ОПК-5.3	ОПК-5.3.1 Осуществляет контроль обеспечения информационной безопасности в открытых информационных системах ОПК-5.3.2 Проводит верификацию данных в открытых информационных системах

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к зачету.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		9
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	36	36
Лабораторные работы (ЛР)	-	-
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	72	72
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	-	-
Подготовка к практическим занятиям / семинарам	36	36
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	-	-
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	9	9
Работа в библиотеке	9	9
Подготовка к зачету	9	9
Промежуточная аттестация – зачет (З)	3	3
Общая трудоемкость дисциплины		
ак.ч.	144	144
з.е.	4	4

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 3 темы:

- тема 1 (Введение в курс);
- тема 2 (Расследование инцидентов ИБ);
- тема 3 (Стратегии управления).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Введение в курс	Введение. Цели и задачи курса. Понятие инцидента информационной безопасности и правовые основы реагирования на него.	4	Формирование политики управления инцидентами ИБ. Классификация инцидентов ИБ по значимости	2 2	-	-
2	Расследование инцидентов ИБ	Цель создания и роль группы реагирования на инциденты. Подготовка к обработке инцидентов и их классификация. Проверка функционирования системы управления инцидентами. Первичная оценка событий инцидента и последовательность действий при ее проведении. Вторичная оценка событий инцидента и последовательность действий при ее проведении. Сдерживание и устранение инцидента.	20	Оценка событий ИБ. Сдерживание, устранение инцидента ИБ и восстановление после него. Формирование и хранение свидетельств инцидентов ИБ. Инцидент внедрения вредоносного кода. Инцидент несоответствующего использования. Стратегии управления непрерывностью функционирования АС	4 4 4 4 4	-	-

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Стратегии управления	Восстановление работоспособности систем после устранения. Стратегии управления непрерывностью функционирования систем. Матрицы определения значимости инцидентов. Предвестники и указатели инцидентов.	12	Матрицы для определения значимости инцидентов неавторизованного доступа. Предвестники и указатели инцидентов неавторизованного доступа. Матрицы для определения значимости инцидентов сбора информации. Меры по сдерживанию, устранению инцидентов сбора информации и восстановлению после них. Матрицы для определения значимости инцидентов внедрения вредоносного кода. Меры по сдерживанию, устранению инцидентов внедрения вредоносного кода и восстановлению после них. Матрицы для определения значимости инцидентов несоответствующего использования. Меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них.	2 2 2 2 2 2	-	-
Всего аудиторных часов		36		36		-	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-5.1, ОПК-5.3	Зачет	Комплект контролирующих материалов для зачета

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– выполнение заданий практического занятия – всего 100 баллов.

Зачет проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Зачет по дисциплине «Расследование инцидентов информационной безопасности» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время зачетной недели студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п.п. 6.5), либо в результате тестирования.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 4.

Таблица 4 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Расчетно-графическая работа (РГР) – индивидуальное задание

Расчетно-графическая работа не предусмотрена.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Введение в курс)

- 1) В чем заключаются основные задачи курса?
- 2) Что такое инцидент информационной безопасности?
- 3) Какие существуют правовые основы реагирования на инцидент информационной безопасности?
- 4) Что означает термин «Реагирование на инцидент информационной безопасности»?
- 5) С какими инцидентами информационной безопасности приходится сталкиваться чаще всего?

Тема 2 (Расследование инцидентов ИБ)

- 1) С какой целью создается группа реагирования на инциденты?
- 2) Какую классификацию имеют инциденты ИБ?
- 3) Как осуществляется проверка функционирования системы управления инцидентами?
- 4) Какова последовательность действий при проведении первичной оценке событий инцидента?
- 5) Какова последовательность действий при проведении вторичной оценке событий инцидента?

Тема 3 (Стратегии управления)

- 1) Каковы меры по сдерживанию, устранению инцидентов несоответствующего использования и восстановлению после них?
- 2) Что представляют из себя матрицы для определения значимости инцидентов неавторизованного доступа?

3) Что представляют из себя матрицы для определения значимости инцидентов сбора информации?

4) Что представляют из себя матрицы для определения значимости инцидентов внедрения вредоносного кода?

5) Что представляют из себя матрицы для определения значимости инцидентов несоответствующего использования?

6.5 Вопросы для подготовки к зачету

1) Какие существуют типы инцидентов информационной безопасности, связанные с отказом в обслуживании?

2) С какой целью инциденты информационной безопасности «сбор информации» проводят разведку?

3) Какие примеры атак, направленные на сбор информации, Вам известны?

4) Какими факторами могут быть вызваны инциденты информационной безопасности?

5) Какие примеры несанкционированного доступа с помощью технических средств Вам известны?

6) Какие факторы воздействия на информацию и последствия Вы знаете?

7) Какие основные предпосылки для возникновения компьютерных инцидентов Вам известны?

8) Какие признаки компьютерного инцидента Вам известны?

9) Какие юридические предпосылки и меры для минимизации нанесенного ущерба Вы можете назвать?

10) Какие программно-технические меры для минимизации нанесенного ущерба Вы можете назвать?

11) Какие действия в случае возникновения компьютерного инцидента должны быть проведены?

12) Как проводится расследование компьютерных инцидентов в РФ?

13) Каков порядок взаимодействия с правоохранительными органами и сторонними организациями?

14) Какие технические мероприятия проводятся при возникновении компьютерного инцидента?

15) С какой целью проводится изъятие и исследование компьютерной техники и носителей информации при возникновении компьютерного инцидента?

16) Как проводится оформление экспертизы?

17) Какие факторы влияют на успешную возможность расследования инцидента?

18) Каков порядок снятия образов с жестких дисков?

19) Какие методы анализа образов жестких дисков Вам известны?

20) Как проводится выявление удаленных данных и зашифрованных областей?

- 21) Какие методы восстановления удаленных данных и зашифрованных областей Вам известны?
- 22) Какие инструменты применяются при анализе журналов ОС и безопасности?
- 23) Какие методы анализа журналов ОС и безопасности применяются?
- 24) Что такое анализ памяти?
- 25) Какие инструменты применяются при анализе памяти?
- 26) Как проводится анализ файлов виртуальной памяти ОС?
- 27) Какие инструменты используются при анализе файлов виртуальной памяти ОС?
- 28) Как проводится анализ файлов-образов виртуальных систем, файлов состояний виртуальных систем?
- 29) Какие инструменты применяются при анализе файлов-образов виртуальных систем, файлов состояний виртуальных систем?
- 30) Каков порядок исследования сетевых признаков компьютерных инцидентов?
- 31) Как проводится анализ конфигураций сетевых устройств?
- 32) Какие инструменты применяются при анализе конфигураций сетевых устройств?
- 33) Как проводится анализ журналов сетевых устройств?
- 34) Какие инструменты применяются при анализе журналов сетевых устройств?
- 35) Как проводится анализ дампов сетевого трафика?
- 36) Какие инструменты применяются при анализе дампов сетевого трафика?
- 37) Каким может быть повод для возбуждения уголовных дел по преступлениям в сфере высоких технологий?
- 38) Каков алгоритм расследования компьютерных преступлений?
- 39) Каков порядок привлечения к расследованию специалистов?
- 40) Как проводится осмотр места происшествия?
- 41) Какие электронные документы подлежат осмотру при возникновении инцидентов ИБ?
- 42) Какие оперативно-розыскные мероприятия проводятся при возникновении инцидентов ИБ?
- 43) Как проводится перехват и исследование сетевого трафика в случае возникновения инцидентов ИБ?
- 44) Что такое кейлогер?
- 45) Как проводится определение принадлежности IP адресов в случае возникновения инцидентов ИБ?
- 46) Как проводится определение принадлежности доменных имен адресов в случае возникновения инцидентов ИБ?
- 47) Как проводится определение принадлежности адреса электронной почты в случае возникновения инцидентов ИБ?
- 48) Что такое индикатор компрометации?

49) С какой целью проводится анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным (если оно было успешным)?

50) С какой целью проводится анализ последствий (в том числе и долгосрочных) нападения для всей деятельности предприятия?

51) С какой целью проводится анализ и оценка работы персонала и взаимоотношений с предприятиями партнерами (в том числе и с поставщиками информационных систем и средств защиты информации)?

52) Какова Процедура сбора свидетельств инцидента ИБ?

6.6 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Энсон С. Реагирование на компьютерные инциденты. Прикладной курс / С. Энсон. пер. с англ. Д.А. Беликова. – Москва: ДМК Пресс, 2021. – 436 с. – Доступ ЭБС «Консультант студента».. – [Электронный ресурс]: – Режим доступа: <https://www.studentlibrary.ru/ru/book/ISBN9785970604847.html> (Дата обращения 26.08.2024).

Дополнительная литература

2. Пелешенко В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие: [16+] / В.С. Пелешенко, С.В. Говорова, М.А. Лапина. – Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с.: ил. – URL: <https://biblioclub.ru/index.php?page=book&id=467139> [Электронный ресурс]: Режим доступа: по подписке. (дата обращения: 26.08.2024).

Учебно-методические материалы и пособия

1. Погорелов Р.Н. Расследование инцидентов информационной безопасности: методические указания к лабораторным работам [Электронный ресурс] – URL: <https://moodle.dstu.education/course> Режим доступа: для авториз. пользователей. — Текст: электронный. (Дата обращения 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education.— Текст : электронный.
2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: <http://ntb.bstu.ru/jirbis2/> .— Текст : электронный.
3. Консультант студента : электронно-библиотечная система.— Москва. — URL: <http://www.studentlibrary.ru/cgi-bin/mb4x> .— Текст : электронный.
4. Университетская библиотека онлайн: электронно-библиотечная система. – URL: http://biblioclub.ru/index.php?page=main_ub_red .— Текст : электронный.
5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: <http://www.iprbookshop.ru/> . —Текст : электронный.
6. Сайт кафедры СКС <http://scs.dstu.education>.

Материально-техническое обеспечение представлено в таблице 9.

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: <i>Мультимедийная аудитория. (60 посадочных мест), оборудованная специализированной (учебной) мебелью (скамья учебная – 20 шт., стол – 1 шт., доска аудиторная – 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран.</i> <i>Аудитории для проведения лекций:</i> <i>Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:</i>	ауд. <u>207</u> корп. <u>4</u> ауд. <u>217</u> корп. <u>3</u> ауд. <u>211</u> корп. <u>4</u>

Лист согласования РПД

Разработал:

ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)


(подпись)

Р.Н. Погорелов
(Ф.И.О.)

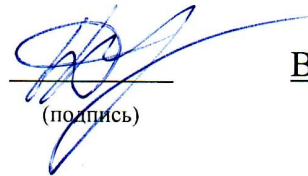
И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Протокол № 1 заседания кафедрыот 27.08.2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)


(подпись)

В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03
Информационная безопасность
автоматизированных систем


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Начальник учебно-методического центра


(подпись)

О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	