МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение безопасности мобильных систем

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»

Квалификация (степень) выпускника: Бакалавр

Кострома

Рабочая программа дисциплины «Обеспечение безопасности мобильных систем» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность, утвержден 01.12.2016 г.

Год начала подготовки 2017

Разработал: _____ Волков Антон Андреевич, доцент кафедры защиты информации, к.т.н.

Рецензент: _ Щекочихин Олег Владимирович, к.т.н., доцент, заведующий кафедры защиты информации

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _11_ от _30.05.2019_____ г.

Заведующий кафедрой защиты информации

_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _8_ от _6.04.2020_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _6_ от _22.01.2021_____ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

1. Цели и задачи освоения дисциплины

Цель дисциплины:

«Обеспечение безопасности мобильных систем» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; формирование у бакалавров знаний и навыков в предметной области. Предмет курса – защита данных в мобильных системах и приложениях.

Профессиональные цели курса — является формирование у будущих специалистов системы понятий, знаний, умений и навыков в области деятельности, связанной с подбором, эксплуатацией и обслуживанием мобильных систем и приложений.

Задачи дисциплины:

- ознакомление студентов с физическими основами передачи данных и базовыми принципами организации связи;
- обучение студентов основам организации и проектирования цифровых беспроводных широкополосных телекоммуникационных сетей;
- ознакомление студентов с основными уязвимостями мобильных систем и способами защиты данных в них;
- получение представлений о радиоэлектронной борьбе и радиоэлектронном подавлении;
- повышение технической грамотности студентов.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать:

- физические основы работы мобильных систем и возможные угрозы информационной безопасности;
- принципы построения мобильных систем с различной реализацией физического канала и методы обеспечения информационной безопасности;

уметь:

- формулировать политику информационной безопасности для мобильных систем;
- практически применять теоретические знания при решении задач защиты информации в мобильных системах;

владеть:

- методами защиты информации в мобильных системах;
- методами анализа и проектирования систем защиты информации в мобильных системах.

освоить компетенции:

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;

ПК-3 способностью администрировать подсистемы информационной безопасности объекта защиты

3. Место дисциплины в структуре ОП ВО

Дисциплина «Обеспечение безопасности мобильных систем» относится к циклу дисциплин по выбору.

Дисциплина изучается на четвёртом курсе, имеет предшествующие логические и содержательно-методические связи с дисциплинами математического и

естественнонаучного цикла: «Информатика», «Математические основы криптологии», «Сети и системы передачи информации».

4. Объем дисциплины (модуля)

4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	4
Общая трудоемкость в часах	144
Аудиторные занятия в часах, в том числе:	50
Лекции	16
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа в часах	94
Форма промежуточной аттестации	Зачет,

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	16
Практические занятия	-
Лабораторные занятия	34
Консультации	0,8
зачет	0.25
Экзамен	0
Курсовая работа	2
Всего	53,05

5. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

5.1 Тематический план учебной дисциплины

№	Название раздела, темы	Всего час	Аудиторные занятия			Самостоятельная работа
			Лекц.	Лаб.	Практ.	
1	Сетевая адресация и сетевые службы	14	2	4		10
2	Беспроводные технологии	14	2	4		10
3	Основы безопасности	14	2	4		10
4	Устранение проблем с сетями	14	2	4		10
5	Планирование структуры адресации	14	2	4		10
6	Защита от перехвата трафика в локальной сети	14	2	4		10
7	Аудит ИБ телекоммуникационных систем	14	4	10		34
	Итого:	**144**	**16**	**34**	**-**	**94**

5.2. Содержание:

Тема 1. Классификация и методы оценки угроз информационной безопасности мобильных системах и устройствах. Актуальность проблемы обеспечения безопасности. Место и роль мобильных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности мобильных систем. Субъекты информационных отношений, их безопасность. Угрозы безопасности мобильных систем. Уязвимость основных структурно-функциональных элементов мобильных систем.

Тема 2. Защита мобильных устройств. Принципы обеспечения безопасности мобильных систем. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в мобильных системах.

Тема 3. Внедрение систем *MDM* *(Mobile Device Management),* как составная часть стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств

Тема 4. Решение типовых проблем защиты мобильных устройств в корпоративной среде на примере использования *Trend Micro Mobile Security*

Тема 5. Современные тенденции и направления развития методов и средств защиты от мобильных угроз

Тема 6. Защита от перехвата трафика в мобильных системах

Методы защиты сетевого трафика. Незащищенность сетей передачи данных. Защита внутреннего трафика в локальной сети. Конфиденциальность данных при работе с веб-страницами. Протоколы SSL/TLS. VPN соединение.

Тема 7. Аудит ИБ мобильных систем

Общая информация и установка и настройка инструментов аудита ИБ сетей. Обзор инструментов. Тестирование сетей. Стресс-тесты сети. Сканирование сетей. Перехват данных в сетях.

6. Методические материалы для обучающихся по освоению дисциплины

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	Раздел (тема) дисциплины	Задание	Часы	Методические рекомендации по выполнению задания	Форма контроля
1	Классификация и методы оценки угроз информационной безопасности мобильных системах и устройствах.	Изучить материалы лекции и рекомендованной литературы.	6	Использовать материалы лекции и рекомендованной литературы [1,2,3,4]	Устный опрос, заслушивание и обсуждение докладов
2	Защита мобильных устройств	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	4	Использовать материалы лекции и рекомендованной литературы [1,2,3,4]	Устный опрос, защита лаб. работы
3	Внедрение систем *MDM*	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	4	Использовать материалы лекции и рекомендованной литературы [1,2,3,4]	Устный опрос, защита лаб. работы
4	Решение типовых	Изучить материалы	6	Использовать материалы лекции и	Устный опрос,

	проблем защиты мобильных устройств	лекции и рекомендованной литературы Создание отчета по лабораторной работе		рекомендованной литературы [1,2,3,4]	защита лаб. работы
5	Современные тенденции и направления развития методов и средств защиты от мобильных угроз	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	6	Использовать материалы лекции и рекомендованной литературы [1,2,3,4]	Устный опрос, защита лаб. работы
6	Защита от перехвата трафика в мобильных системах	Изучить материалы лекции и рекомендованной литературы	6	Использовать материалы лекции и рекомендованной литературы [1,2,3,4]	Устный опрос
7	Аудит ИБ мобильных систем	Изучить материалы лекции и рекомендованной литературы. Создание отчетов по лабораторным работам	6	Использовать материалы лекции и рекомендованной литературы [1,2,3,4]	Устный опрос, защита лаб. работ

6.3. Тематика и задания для лабораторных занятий

1	Разбор и генерация HTTP запроса
2	SQL injections. SQLMap
3	Межсайтовый скриптинг (XSS)
4	Защита от внедрения вредоносных файлов
5	Кликджекинг
6	Шифрование
7	Автоматизированное тестирование уязвимостей
8	Тестирование веб приложения

6.4. Тематика курсовых работ

1. Программное обеспечение для анализа рисков информационной безопасности.
2. Оценка вероятности угроз от мобильных устройств по отдельным категориям: потеря или кража мобильного устройства; перехват данных, которые передаются по сетям Wi-Fi или 3G; захват данных через соединения Bluetooth; мобильные вирусы (включая вирусы электронной почты).
3. Политики безопасного использования мобильных устройств в различных областях.
4. Обеспечение контроля за хаотичным подключением мобильных устройств к корпоративным ресурсам.
5. Распределение мобильных устройств и привязка к пользователям.
6. Обеспечение единообразия корпоративного программного обеспечения.
7. Распространение корпоративных настроек и политик безопасности на устройства.
8. Защита данных в случае кражи.
9. Контроль утечки данных мобильных устройств.
10. Защита мобильных устройств от вредоносных программ.
11. Защита мобильных устройств от фишинга.

12. Защита мобильных устройств от телефонного спама.
13. Возможности системы *MDM (Mobile Device Management)* для обеспечения контроля над мобильными устройствами, имеющими доступ к корпоративным сервисам организации, и возможности по снижению рисков, связанных с утечкой данных.Пути снижения рисков информационной безопасности при использовании систем MDM (Mobile Device Management).
14. Повышение управляемости и стабильности процессов управления мобильными устройствами пользователей.
15. Повышение экономической эффективности от внедрения *MDM* системы при реализации политик безопасности.
16. Контроль хаотичного подключения устройств к корпоративным ресурсам в *Trend Micro Mobile Security* и группировка их в домены управления для выполнения типовых настроек и упрощения администрирования.
17. Возможности *Trend Micro Mobile Security* централизованно устанавливать на устройствах настройки сетей *Wi-Fi*,*VPN*-подключений и электронной почты.
18. Возможность аудита установленных приложений, и отчетность по установленным приложениям.
19. Функции *Trend Micro Mobile Security* по удаленному блокированию/разблокированию устройств, удалению данных и отслеживанию его местоположения на картах Google.
20. Политики защиты устройств и ограничения функционала, привязанные к определенному местоположению в *Trend Micro Mobile Security*.
21. Защита от вредоносных программ и фишинга в *Trend Micro Mobile Security.*

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

Основная литература

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
2. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
3. Мельников, Д.А. Информационная безопасность открытых систем: учебник / Д.А. Мельников. - М.: Флинта, 2013. - 448 с.
4. Олифер В.Г., Олифер Н.А. Безопасность компьютерных сетей. –М.: «Горячая линия – Телеком», 2017. - 644 с.
5. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов –М.: «Горячая линия – Телеком», 2017. - 338 с.

Дополнительная литература

1. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.
2. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.

3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.
4. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2014. - 702 с.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Информационно-образовательные ресурсы:

1. Библиотека КГУ: URL: http://library.ksu.edu.ru/
2. Национальный открытый университет ИНТУИТ: URL: *http://www.intuit.ru*
3. Сайт компании Cisco Systems: URL: *http:/www.cisco.com*;
4. Сайт обмена знаниями по UNIX/Linux-системам, системам с открытым исходным кодом, сетям и другим родственным вещам: URL: *http://www.xgu.ru*;
5. Сайт ИТ-специалистов-блогеров:URL: *http://www.habr.com*

Электронные библиотечные системы:

1. ЭБС «Лань»
2. ЭБС «Университетская библиотека online»
3. ЭБС «Znanium»

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения всех видов занятий по дисциплине необходимо следующее материально-техническое обеспечение:

№ п/п	**Специализированные аудитории и классы**	Номер аудитории
1	Аудитория, оборудованная мультимедиа, для лекций	Е407. Е318, Е406
2	Компьютерные классы	Е406
Учебное оборудование		
	Персональные компьютеры, объединенные в локальную сеть, с выходом в Интернет	
№ п/п	**Программное обеспечение**	
1	MS Windows (Dream Spark Premium)	Е406
2	Офисный пакет	Е406
3	Симулятор вычислительной сети	Е406
4	ОС Linux	Е406