Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Безопасность мобильных устройств и приложений

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-3 Способен администрировать средства защиты информации в компьютерных системах и сетях

ПК-3.3 Администрирует средства защиты информации прикладного и системного программного обеспечения

и включает:

для текущего контроля успеваемости:

Форма реализации: Устная форма

1. Защита информации в мобильных системах (Коллоквиум)
2. Информационная безопасность мобильных систем (Коллоквиум)
3. Обеспечения безопасности конфиденциальной информации в мобильных устройствах (Коллоквиум)
4. Проблемы обеспечения безопасности мобильных устройств и приложений (Коллоквиум)

БРС дисциплины

8 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Проблемы обеспечения безопасности мобильных устройств и приложений					
Тема 1. Мобильные платформы. Защита информации		+			
Тема 2. Мобильные ОС Windows Mobile/ Windows Phone и ОС Android. Обзор актуальных угроз и средств защиты информации		+			
Тема 3. Классификация угроз безопасности информации и методы оценки безопасности мобильных систем и устройств			+		
Обеспечение безопасности информации мобильных устройств и приложений					
Тема 4. Защита мобильных устройств. Принципы обеспечения безопасности мобильных систем.			+		
Тема 5. Решение типовых проблем защиты мобильных устройств и приложений				+	+
Тема 6. Защита от перехвата трафика в мобильных системах				+	+

Тема 7. Мобильные веб-браузеры. Уязвимости. Средства защиты			+	+
Вес КМ:	20	20	30	30

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-3	ПК-3.3$_{ПК-3}$ Администрирует средства защиты информации прикладного и системного программного обеспечения	Знать: основы функционирования мобильных систем, возможные угрозы информационной безопасности и уязвимости специального и прикладного программного обеспечения при их эксплуатации злоумышленниками Уметь: формулировать политику информационной безопасности для мобильных систем администрировать системное и программное обеспечение мобильных систем	Информационная безопасность мобильных систем (Коллоквиум) Проблемы обеспечения безопасности мобильных устройств и приложений (Коллоквиум) Обеспечения безопасности конфиденциальной информации в мобильных устройствах (Коллоквиум) Защита информации в мобильных системах (Коллоквиум)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Информационная безопасность мобильных систем

Формы реализации: Устная форма
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Самостоятельная разработка ответов на вопросы коллоквиума

Краткое содержание задания:
Подготовить ответы на вопросы коллоквиума и разработать презентацию доклада
Вопросы коллоквиума:
1. Место и роль мобильных устройств и приложений в управлении бизнес-процессами
2. Архитектура мобильных устройств
3. Причины обострения проблемы обеспечения информационной безопасности мобильных систем
4. Инструменты безопасности. Средства синхронизации. Уязвимости. Виды и примеры вредоносного ПО.
5. Антивирусные средства. Возможности шифрования данных. Политики безопасности

Контрольные вопросы/задания:

Знать: основы функционирования мобильных систем, возможные угрозы информационной безопасности и уязвимости специального и прикладного программного обеспечения при их эксплуатации злоумышленниками	1. Место и роль мобильных устройств в управлении бизнес-процессами 2. Место и роль приложений мобильных устройств в управлении бизнес-процессами 3. Архитектура мобильных устройств 4. Проблемы обеспечения информационной безопасности мобильных систем

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-2. Проблемы обеспечения безопасности мобильных устройств и приложений

Формы реализации: Устная форма
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Самостоятельная разработка ответов на вопросы коллоквиума

Краткое содержание задания:

Подготовить ответы на вопросы коллоквиума и разработать презентацию доклада
Вопросы коллоквиума:
1.Субъекты информационных отношений и их безопасность
2. Угрозы безопасности мобильных устройств и приложений
3. Модели угроз безопасности информации
4. Уязвимости основных структурно-функциональных элементов мобильных устройств и приложений

Контрольные вопросы/задания:

Уметь: формулировать политику информационной безопасности для мобильных систем	1.Порядок выявления актуальных угроз безопасности информации в мобильных устройствах и приложениях 2.Порядок мониторинга угроз безопасности информации в мобильных устройствах и приложениях

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-3. Обеспечения безопасности конфиденциальной информации в мобильных устройствах

Формы реализации: Устная форма
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Самостоятельная разработка ответов на вопросы коллоквиума

Краткое содержание задания:
Подготовить ответы на вопросы коллоквиума и разработать презентацию доклада
Вопросы коллоквиума:
1.Виды мер противодействия угрозам безопасности
2. Принципы построения системы обеспечения безопасности информации в мобильных системах
3. Достоинства и недостатки различных видов мер защиты
4. Стратегия обеспечения безопасности конфиденциальной информации в мобильных устройствах на основе внедрения систем MDM (Mobile Device Management)
5. Защита мобильных устройств в корпоративной среде с использованием Trend Micro Mobile Security

Контрольные вопросы/задания:

Уметь: администрировать системное и программное обеспечение мобильных систем	1.Администрирование обеспечение безопасности конфиденциальной информации в мобильных устройствах на основе внедрения систем MDM (Mobile Device Management) 2.Администрирование обеспечение безопасности конфиденциальной информации в мобильных

	устройствах на основе внедрения систем Trend Micro Mobile Security

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

КМ-4. Защита информации в мобильных системах

Формы реализации: Устная форма
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Самостоятельная разработка ответов на вопросы коллоквиума

Краткое содержание задания:
Подготовить ответы на вопросы коллоквиума и разработать презентацию доклада
Вопросы коллоквиума:
1. Методы защиты сетевого трафика
2. Защита внутреннего трафика в локальной сети
3. Протоколы SSL/TLS
4. VPN соединение
5. Мобильные веб-браузеры. Сравнительный обзор. Уязвимости. Средства защиты.
6. Разновидность атак на веб-приложения. Выявление паттернов

Контрольные вопросы/задания:

Уметь: администрировать системное и программное обеспечение мобильных систем	1. Порядок применения протоколов SSL/TLS 2.Порядок выявления паттернов

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Оценка "зачтено" выставляется если задание выполнено правильно или с незначительными недочетами

Оценка: не зачтено
Описание характеристики выполнения знания: Оценка "не зачтено" выставляется если задание не выполнено в отведенный срок или результат не соответствует заданию

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8 семестр

Форма промежуточной аттестации: Зачет

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ПК-3.З$_{ПК-3}$ Администрирует средства защиты информации прикладного и системного программного обеспечения

Вопросы, задания

1.Место и роль мобильных устройств и приложений в управлении бизнес-процессами
2.Архитектура мобильных устройств

3.Причины обострения проблемы обеспечения информационной безопасности мобильных систем
4.Мобильные ОС Windows Mobile/ Windows Phone и ОС Android
5.Инструменты безопасности мобильных устройств
6.Антивирусные средства мобильных устройств
7.Закрытые и открытые архитектуры, средства взаимодействия
8. Возможности шифрования данных в мобильных устройствах и приложениях
9.Угрозы безопасности мобильных устройств и приложений.

10.Модели угроз безопасности информации
11.Уязвимость основных структурно-функциональных элементов мобильных устройств и приложений
12. Виды мер противодействия угрозам безопасности
13.Принципы построения системы обеспечения безопасности информации в мобильных системах
14.Достоинства и недостатки различных видов мер защиты
15.Стратегия обеспечения безопасности конфиденциальной информации в мобильных устройствах на основе внедрения систем MDM (Mobile Device Management)
16.Защита мобильных устройств в корпоративной среде с использованием Trend Micro Mobile Security
17.Методы защиты сетевого трафика
18.Защита внутреннего трафика в локальной сети
19.Уязвимости мобильных веб-браузеров
20.Средства защиты мобильных веб-браузеров
21.Разновидность атак на веб-приложения. Выявление паттернов

Материалы для проверки остаточных знаний

1.Мобильная ОС Windows Mobile

Ответы:

-

Верный ответ: Windows Mobile – семейство ОС для мобильных устройств фирмы Microsoft. Оно относится к семейству Windows CE (Consumer and Embedded) – Windows для встроенных систем. Ядро ОС Windows Mobile основано на ОС Windows CE. Текущая версия Windows Mobile (2010) – Windows Phone Classic 6.5. В США Windows Mobile - третья по популярности ОС для мобильных устройств (после Blackberry OS и iPhone OS). Windows Mobile поддерживает следующие виды мобильных устройств: PocketPC, смартфоны, коммуникаторы (например, Qtek).

Первая версия Windows Mobile была выпущена в 1996 г. Windows Mobile: возможности и ПО. ОС Windows Mobile предоставляет разнообразный набор возможностей и программного обеспечения: Office Mobile – аналог Microsoft Office для мобильных устройств; полная совместимость по форматам; Windows Media Player – мультимедийный проигрыватель, аналог проигрывателя для настольной версии Windows; Internet Explorer Mobile – Web-браузер, аналог Internet Explorer для настольной версии Windows; Программное обеспечение для поддержки Bluetooth и Wi-Fi – современных видов коммуникации; Программное обеспечение Microsoft ActiveSync для синхронизации данных с настольными компьютерами. Windows Mobile поддерживает пользовательский интерфейс с мобильным устройством с помощью касания экрана стайлусом и пальцами, в том числе (в современных версиях) – multi-touch.

2.Угрозы безопасности мобильных устройств и приложений.

Ответы:

-

Верный ответ: Существует пять основных сценариев атаки. Среди них: Физический доступ. Если телефон был украден или потерян, владелец отдал его в сервис или подключил к поддельному зарядному устройству по USB — все это открывает возможность для атаки. Вредоносное приложение на устройстве. Иногда такие приложения могут попасть на устройство даже из официальных источников, Google Play и App Store (для Android, для iOS). Атакующий в канале связи. Подключившись к недоверенному Wi-Fi, прокси-серверу или VPN, мы становимся уязвимыми для атак в канале связи. Удаленные атаки. Атакующий может действовать при этом удаленно, пользуясь серверами мобильных приложений или иными службами для доставки эксплойта. Атаки на серверную часть. Отдельно от всего можно рассмотреть атаки на серверную часть мобильных приложений, поскольку в этом случае доступ к устройству злоумышленнику не требуется.

3.Вредоносные программы для ОС Android

Ответы:

-

Верный ответ: Вредоносные программы для ОС Android: 1. Трояны Android.Gongfu, Android.Wukong, Android.DreamExploid, Android.Geinimi, Android.Spy. Такие вредоносные программы выполняют сбор конфиденциальной информации, получение и выполнение команд от злоумышленников, установка программ. 2. Рекламные модули, используемые в приложениях для заработка, однако рекламные модули могут быть не внутри приложения, а в статусной строке, тем самым злоумышленники этим пользуются и пишут что-то типа «Требуется обновление системы» [2]. С вредоносными программами немного разобрались, но также существует множество уязвимостей платформы Android, такие как: 1. Одна из самых главных уязвимостей Android является получение root прав. Есть множество программ и скриптов для получения root прав, но как правило люди осознано делаю root доступ для получения большего контроля над устройством. Но если к вам на устройство попадает вредоносная программа которая получит root доступ, то она беспрепятственно и без вашего ведома может устанавливать программы (как это делают различные модификации Android.Gongfu и Android.DreamExploid). 2. Еще угрозы может представлять неофициальные или сторонние прошивки. Поводов для беспокойства здесь несколько. Во-первых, в такие прошивки изначально могут быть встроены вредоносные программы. Во- вторых, когда цифровой подписью образа системы подписывается какое-либо приложение, оно получает те же права, что и сама система, в которой оно работает. В рамках Android Open Source Project (AOSP) подписи для образов являются приватными, поэтому такой сценарий возможен, например, в случае кражи соответствующей подписи. Подобный способ заражения

применялся, в частности, вредоносной программой Android. SmsHider, которая могла незаметно для пользователей, использующих определенные сторонние прошивки, установить содержащийся в ней троянский арк. 3. Ошибка обнаружена в MMS модуле. Злоумышленник создает MMS, к которому крепится мультимедийный файл с вредоносным кодом, в результате чего хакер получает доступ к микрофону, камере, внешнему накопителю данных, а в зависимости от модели смартфона даже Root-доступ. Но самым неприятным является то, что вредоносный код может быть внедрен и активирован даже без активных действий со стороны пользователя. Можно сказать, что пользователи операционной системы Android подвержены большей опасности получения на свои устройства вредоносного программного обеспечения, способного передавать злоумышленникам персональные данные и деньги пользователей, чем владельцы гаджетов Apple. Однако пользователи ОС iOS также подвержены угрозам. Закрытая операционная система является более защищённой так как любой контент загружаемый на нее проверяется разработчиком, однако существует ряд уязвимостей данной системы: 1. Один из первых случаев публично продемонстрированных уязвимостей на iOS имел место на конференции Black Hat в 2009 году. Специалисты по вопросам компьютерной безопасности Чарли Миллер и Коллин Муллинер обратили внимание разработчиков мобильных платформ на то, что они не уделяют внимания защите SMS-компонентов. В ходе своего выступления хакеры показали, что определенные команды по SMS позволяют загружать мобильный процессор на все 100% или получать полный контроль над устройством. 2. В апреле 2013 некоторые пользователи устройств под управлением Apple iOS 6 начали жаловаться на некое подобие DDoS-атак, которые производились через другой стандартный компонент платформы — фирменный клиент сообщений iMessage. При помощи микроприложений AppleScript неизвестные злоумышленники отправляли одним и тем же пользователям лавины сообщений. Нагрузка на устройства возрастала до того, что никакие другие апплеты на них просто не запускались. 3. В операционной системе iOS обнаружена серьезная уязвимость, позволяющая хакерам подменять в смартфонах популярные приложения на вредоносные аналоги. О методе атаки, получившем название ’’Маска" (Masque), рассказал технический руководитель компании FireEye Саймон Маллис. По его словам, о наличии в своем гаджете опасного ПО владелец может не догадываться долгое время. На сегодняшний день известно о поддельных Twitter, Facebook, WhatsApp, Viber и Skype, при "установке новой версии" они заменяют настоящие

II. Описание шкалы оценивания

Оценка: зачтено
Описание характеристики выполнения знания: Работа выполнена верно или с несущественными недостатками

Оценка: не зачтено
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу