Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

ФД.3 «Разработка безопасных мобильных приложений для OS Android»

специальности подготовки
10.05.03 "Информационная безопасность автоматизированных систем"

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 2
часов в неделю – 2
всего часов – 72,
в том числе:
лекции – 18
лабораторные занятия – 18
самостоятельная работа – 36
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: изучение вопросов обеспечения информационной безопасности, возникающих при использовании мобильных устройств, а также основ разработки защищенных мобильных приложений для OS Android.

Задачи изучения дисциплины:

- формирование у обучаемых целостного представления о комплексном подходе к обеспечению безопасности при использовании в информационной системе мобильных устройств;
- приобретение обучаемыми необходимого объема знаний и практических навыков в области разработки, распространения и эксплуатации защищенных мобильных приложений для OS Android.

2. Место дисциплины в структуре ООП ВПО

Для успешного усвоения дисциплины «Разработка безопасных мобильных приложений для OS Android» необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – знать формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей;

«Языки программирования» – знать язык программирования высокого уровня (объектно-ориентированное программирование), уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

«Основы информационной безопасности» – знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, владеть профессиональной терминологией в области информационной безопасности;

«Сети и системы передачи информации» – знать основные характеристики сигналов электросвязи, спектры и виды модуляции, принципы построения и функционирования систем и сетей передачи информации, способы кодирования информации, основные телекоммуникационные протоколы.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующей компетенции:

- способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности (ПК-3).

Студент должен знать:

- процедуру формирования цифровой подписи кода приложения, необходимой для доступа и использования различных функций безопасности мобильных устройств Android;
- правила, процедуры, практические приемы для управления информационной безопасностью.

Студент должен уметь:

- разрабатывать модели угроз и нарушителей информационной безопасности в процессе разработки, распространения и эксплуатации защищенных мобильных приложений;
- рационально выбирать методы и средства для реализации процессов разработки, распространения и эксплуатации защищенных мобильных приложений;
- составлять комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

Студент должен владеть:

- навыками в области разработки, распространения и эксплуатации защищенных мобильных приложений для OS Android;
- методами организации и управления деятельностью служб защиты информации на предприятии.

4. Распределение трудоемкости (час.) дисциплины по темам и видам занятий

№ Модуля	№ Недели	№ Темы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лекции	Коллоквиумы	Лабораторные	Практические	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
8 семестр									

1	1	1	Введение	10	2	-	-	-	8
1	2	2	Обеспечение безопасности мобильных устройств	16/2	4/2	-	2	-	10
2	6	3	Интерфейсы программирования защищенных мобильных приложений	22/2	6/2	-	8	-	8
2	10	4	Средства Android для формирования и проверки цифровой подписи Java-приложений	24/4	4/2	2/2	8	-	10
Всего				**72/8**	**16/6**	**2/2**	**18**	**-**	**36**

5. Содержание лекционного курса

№ темы	Всего часов	№ лекции	Тема лекции. Вопросы, отрабатываемые на лекции	Учебно-методическое обеспечение
1	**2**	**3**	**4**	**5**
1	2	1	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения.	1, 2, 3, 5, 6, 7, 8
2	2	2	Специфика угроз и уязвимостей для мобильных устройств. Угрозы, связанные с установкой сторонних приложений. Способы снижения рисков. Особенности планирования сетевой инфраструктуры для повышения безопасности сети.	1, 2, 3, 5, 6, 7, 8
2	2	3	Настройка параметров безопасности в мобильных устройствах Android. Архитектура пакета JavaME, функциональные возможности его компонент. Разновидности ключей для защиты данных. Шифрование данных при передаче между JavaME и устройством. Настройка глобальной политики безопасности с помощью JavaME. Настройка политики безопасности для сторонних приложений. Особенности процедур надежного удаления данных (Scrubbing). Способы защиты данных с помощью шифрования при блокировке смартфона.	1, 2, 3, 5, 6, 7, 8
3	2	4	Возможности библиотеки Security and Trust Services API (SATSA) для разработки защищенных мобильных приложений: - Создание защищенного канала для взаимодействия со смарт-картами; - Формирование электронной цифровой подписи (ЭЦП) для авторизации пользователей и транзакций; - Обеспечение безопасного хранения	1, 2, 3, 5, 6, 7, 8

			криптографических ключей, - Использование функций библиотеки General Purpose Cryptographic Library для хеширования сообщений, проверки ЭЦП, шифрования и дешифрования данных. Усиленная аутентификация с использованием Android Smart Card Reader и защита Bluetooth-соединений.	
3	2	5	Проверка разрешений и политика контроля доступа к API SATSA. Концепция доверенных приложений в спецификации MIDP v.2.0. Особенности выполнения непроверенных приложений. Разрешения для защищенных API и функций отдельных классов. Понятие защищенного домена (Protection Domain).	1, 2, 3, 5, 6, 7, 8
3	2	6	Применение инфраструктуры открытых ключей (PKI) для подписи и верификации мобильных приложений. Создание и выдача сертификата открытого ключа (формат X.509v3) удостоверяющим центром. Генерация ЭЦП на базе алгоритмов SHA-1 и RSA. Проверка подлинности и действительности полученного сертификата, построение пути сертификации до корневого удостоверяющего центра. Окончание срока действия и аннулирование сертификатов. Особенности процедуры проверки подлинности ЭЦП jar-файла мобильного приложения.	1, 2, 3, 5, 6, 7, 8
4	2	7	Обзор библиотек Android API, для работы с которыми необходимо наличие цифровой подписи: - библиотеки Runtime API - библиотеки Android Application API - библиотеки Android Cryptography API (Secure Messaging, Secure Connection, Keystore, Certificate, Encoder, ASN1, OID, Primitives) Получение регистрационного кода для доступа к средствам подписи Android APIs.	1, 2, 3, 5, 6, 7, 8
4	2	8	Использование средств Android Java Development Environment для: - отправки запроса на получение цифровой подписи кода приложения с помощью средства Android Signature Tool; - отправки запроса на получение цифровой подписи через прокси-сервер; - проверки статуса отправленных запросов. Проверка цифровой подписи приложения во время установки приложения и в процессе его работы.	1, 2, 3, 5, 6, 7, 8

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методическое обеспечение
1	2	3	4	5
4	2	1	Использование средств Android Signing Authority Tool для разграничения доступа к защищенным API и данным (хранящимся в persistent store, runtime store или базе данных SQLite). Управление сертификатами, хранящимися в мобильном устройстве.	1, 2, 3, 5, 6, 7, 8

7. Перечень практических занятий

Практические занятия учебным планом не предусмотрены.

8. Перечень лабораторных работ

№ темы	Всего часов	Наименование лабораторной работы. Задания, вопросы, отрабатываемые на лабораторном занятии	Учебно-методическое обеспечение
1	2	4	3
2	2	Настройка параметров безопасности в мобильных устройствах Android. Разновидности ключей шифрования. Настройка разрешений для приложений, устанавливаемых пользователем.	1, 2, 3, 5, 6, 7, 8
3	4	Установка и настройка Android Java Plug-in в среде разработки Eclipse. Разработка тестового мобильного приложения в Eclipse. Запуск недоверенного приложения в среде Android Smartphone Simulator.	1, 2, 3, 5, 6, 7, 8
3	4	Разработка мобильного приложения, использующего ANDROID Cryptographic API для шифрования и проверки целостности данных.	1, 2, 3, 5, 6, 7, 8
4	4	Разработка мобильного приложения, осуществляющего передачу данных через защищенное HTTPS-соединение (по протоколу TLS).	1, 2, 3, 5, 6, 7, 8
4	4	Использование Android Signing Authority Tool для подписывания кода приложения. Запуск подписанного приложения в среде Android Smartphone Simulator. Настройка параметров аутентификации для доверенного приложения.	1, 2, 3, 5, 6, 7, 8

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое

			обеспечение
1	**2**	**3**	**4**
1	8	Обзор стандарта PKCS RSA Encryption	25
2	10	Обзор стандарта Internet X.509 Public Key Infrastructure	10
3	8	Обзор стандарта Online Certificate Status Protocol	2-4
4	10	Изучение структуры библиотеки J2security Element Cryptography API	25

Виды, график контроля СРС, (по решению кафедры УМКС/УМКН).

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
8 семестр			
1-3	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация), зачет
4,5	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	Зачет

10. Расчетно-графическая работа

Расчетно-графическая работа учебным планом не предусмотрена.

11. Курсовая работа

Курсовая работа учебным планом не предусмотрена.

12. Курсовой проект

Курсовой проект учебным планом не предусмотрен.

13. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Изучение дисциплины направлено на формирование следующей компетенции: ПК-3.

Карта компетенции ПК-3: способностью использовать языки, системы и инструментальные средства программирования в профессиональной деятельности.

№ п/п	Части компонентов	Технологии формирования	Средства и технологии оценки
1	3	4	5
1	Знает:	Лекции	Тестирование

	− процедуру формирования цифровой подписи кода приложения, необходимой для доступа и использования различных функций безопасности мобильных устройств Android; − правила, процедуры, практические приемы для управления информационной безопасностью.	Самостоятельная работа Семинары	
	Умеет: − разрабатывать модели угроз и нарушителей информационной безопасности в процессе разработки, распространения и эксплуатации защищенных мобильных приложений; − рационально выбирать методы и средства для реализации процессов разработки, распространения и эксплуатации защищенных мобильных приложений; − составлять комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.	Лабораторные работы с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
	Владеет: − навыками в области разработки, распространения и эксплуатации защищенных мобильных приложений для OS Android; − методами организации и управления деятельностью служб защиты информации на предприятии.	Лекции Лабораторные занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Зачет

Формирование профессиональных компетенций по дисциплине производится на лабораторных и лекционных занятиях (75%); закрепление достигается при проведении промежуточной аттестации (10%) и сдаче зачета (15%).

При выставлении оценок при приеме зачета преподаватель руководствуется следующим:

- оценки «зачтено» заслуживает студент, обнаруживший знания основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, успешно выполняющий предусмотренные в программе задания, знакомый с основной и дополнительной литературой, рекомендованной программой, продемонстрировавший умения и навыки в рамках формируемых компетенций на вполне достаточном уровне освоения.

- оценка «не зачтено» выставляется студенту, обнаружившему пробелы в знаниях основного учебно-программного материала, допустившего принципиальные ошибки в выполнении предусмотренных программой заданий, не освоивший умений и навыков в рамках формируемых компетенций на достаточном уровне освоения. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

Вопросы для зачета

1. Специфика угроз и уязвимостей для мобильных устройств.
2. Угрозы, связанные с установкой сторонних приложений.
3. Способы снижения рисков.

4. Особенности планирования сетевой инфраструктуры для повышения безопасности сети.
5. Настройка параметров безопасности в мобильных устройствах Android.
6. Архитектура пакета JavaME, функциональные возможности его компонент.
7. Разновидности ключей для защиты данных. Шифрование данных при передаче между JavaME и устройством.
8. Настройка глобальной политики безопасности с помощью JavaME.
9. Настройка политики безопасности для сторонних приложений.
10. Особенности процедур надежного удаления данных (Scrubbing).
11. Способы защиты данных с помощью шифрования при блокировке смартфона.
12. Возможности библиотеки Security and Trust Services API (SATSA) для разработки защищенных мобильных приложений.
13. Создание защищенного канала для взаимодействия со смарт-картами.
14. Формирование ЭЦП для авторизации пользователей и транзакций.
15. Проверка разрешений и политика контроля доступа к API SATSA.
16. Концепция доверенных приложений в спецификации MIDP v.2.0.
17. Особенности выполнения непроверенных приложений.
18. Разрешения для защищенных API и функций отдельных классов.
19. Понятие защищенного домена (Protection Domain).
20. Применение инфраструктуры открытых ключей (PKI) для подписи и верификации мобильных приложений.
21. Создание и выдача сертификата открытого ключа (формат X.509v3) удостоверяющим центром.
22. Генерация ЭЦП на базе алгоритмов SHA-1 и RSA.
23. Проверка подлинности и действительности полученного сертификата, построение пути сертификации до корневого удостоверяющего центра.
24. Окончание срока действия и аннулирование сертификатов.
25. Особенности процедуры проверки подлинности ЭЦП jar-файла мобильного приложения.
26. Проверка цифровой подписи приложения во время установки приложения и в процессе его работы.
27. Управление сертификатами, хранящимися в мобильном устройстве.

Вопросы для экзамена

Экзамен учебным планом не предусмотрен.

Тестовые задания по дисциплине

Для проведения тестирования используются тестовые материалы, разработанные в среде АСТ-Тест.

Примеры тестовых заданий:

1. Внутренняя аналитика мобильных приложений это:
1. анализ поведения пользователей внутри приложения и работа самого приложения
2. количество установок приложения, его продвижение
3. сбор и анализ данных об использовании мобильных приложений
4. продвижение приложения в сети

2. Основными угрозами для мобильных приложений являются следующие причины:
1. Секретные данные в открытом виде;

2. Небезопасные каналы передачи информации;
3. Внедрение SQL-операторов;
4. Управление сессиями

3. В чем отличие криптографических протоколов SSL и TLS

1. Вместо алгоритма (MAC, который использовался в SSL, в TLS используется HMAC.
2. Добавлены новые alert сообщения.
3. TLS не поддерживает шифрование и обмен ключами Fortezza.
4. TLS использует асимметричную криптографию для аутентификации

4. Стресс-тестирование программного обеспечения

1. один из видов тестирования программного обеспечения, которое оценивает надёжность и устойчивость системы в условиях превышения пределов нормального функционирования.
2. тестирование, которое проводится с целью определения, как быстро работает вычислительная система или её часть под определённой нагрузкой.
3. подвид тестирования производительности, сбор показателей и определение производительности и времени отклика программно-технической системы или устройства в ответ на внешний запрос с целью установления соответствия требованиям, предъявляемым к данной системе (устройству).
4. процесс исследования, испытания программного продукта, чтобы выявить ситуации, в которых поведение программы является неправильным, нежелательным или не соответствующим спецификации.

5. Основные риски популярных приложений социальных сетей:

1. Не использует шифрование для обмена данными (отправляет данные в открытом виде).
2. Имеет доступ к книге контактов пользователя и данным о его расположении и отправляет координаты расположения в незашифрованном виде.
3. Ненадежный алгоритм шифрования паролей
4. Используется незащищенный протокол передачи данных

6. Лидирующей атакой для мобильного ПО является

1. SMS-троян
2. Backdoor
3. Троян-шпион
4. Другое

7. Вирус android.bbridge.a:

1. крадет информацию о телефоне (модель, версию OS, список приложений и т. д.) и пользователе (пароли, логины, sms), но, прежде всего, отправляет текстовые сообщения на премиум-номера
2. крадет данные кредитных карт, а также может отправлять и стирать sms-сообщения, добавлять номера в черный список и осуществлять несанкционированное подключение.
3. способен извлекать и изменять закладки, изменять стартовую страницу, отображать уведомлений push, подменять ссылки и модифицировать результаты поиска.

4. является специализированным вирусом и, скорее всего, создает ботнеты. После установки передает наш Android под контроль владельца сервера, который может удаленно управлять нашим устройством.

8. Вирус android.bankbot.34.origin:

1. крадет информацию о телефоне (модель, версию OS, список приложений и т. д.) и пользователе (пароли, логины, sms), но, прежде всего, отправляет текстовые сообщения на премиум-номера

2. крадет данные кредитных карт, а также может отправлять и стирать sms-сообщения, добавлять номера в черный список и осуществлять несанкционированное подключение.

3. способен извлекать и изменять закладки, изменять стартовую страницу, отображать уведомлений push, подменять ссылки и модифицировать результаты поиска.

4. является специализированным вирусом и, скорее всего, создает ботнеты. После установки передает наш Android под контроль владельца сервера, который может удаленно управлять нашим устройством.

9. Вирус android.counterclank:

1. крадет информацию о телефоне (модель, версию OS, список приложений и т. д.) и пользователе (пароли, логины, sms), но, прежде всего, отправляет текстовые сообщения на премиум-номера
2. крадет данные кредитных карт, а также может отправлять и стирать sms-сообщения, добавлять номера в черный список и осуществлять несанкционированное подключение.
3. способен извлекать и изменять закладки, изменять стартовую страницу, отображать уведомлений push, подменять ссылки и модифицировать результаты поиска.
4. является специализированным вирусом и, скорее всего, создает ботнеты. После установки передает наш Android под контроль владельца сервера, который может удаленно управлять нашим устройством.

10. Классы безопасности компьютерных систем определяются в соответствии со стандартом

1. ГОСТ 15408.
2. Оранжевая книга(TCSEC).
3. Гармонизированные критерии европейских стран.
4. Концепция защиты от НСД Гостехкомиссии РФ.

11. Главной причиной роста количества угроз для Android, является открытость основного …этой операционной системы. (исходного кода)

12. Наиболее популярные на рынке мобильных приложений On-demand (по требованию) сервисы это…

1. Услуги, которые пользователь может получить настолько быстро, насколько это возможно.
2. Приложения с быстрой логикой.
3. Интернет-ресурсы с быстрым доступом.
4. Приложения без предварительной установки.

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВПО в рамках учебного курса предусмотрены активные и интерактивные формы проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

В связи с этим предусмотрено применение мультимедийных средств и презентаций, обсуждение докладов студентов, лекции с элементами деловых игр, тестирование, консультации, решение ситуационных задач, дискуссии.

Общее количество занятий, проводимых в интерактивных формах, не менее 8 часов.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обязательные издания

1. Алешин Л.И. Информационные технологии: учеб. пособие / Л.И.Алешин. - М.: Маркет ДС, 2011. - 384 с. Экземпляры всего: 22.
2. Хлебников А.А. Информационные технологии: учебник / А.А. Хлебников. - М.: Кнорус, 2014. - 472 с. Экземпляры всего: 4.
3. Заика А. Компьютерная безопасность / А. Заика. - М.: РИПОЛ Классик, 2013. - 160 с. Экземпляры всего: 1.
4. Информационная безопасность и защита информации [Электронный ресурс] : учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. - 5-е изд., стер. - Электрон. текстовые дан. - М.: ИЦ "Академия", 2011. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/Ld_154.pdf
5. Губенков А.А. Обеспечение безопасности персональных данных: учеб. пособие для студ. направления 090303.65 "Информационная безопасность автоматизированных систем" и бакалавров направления 090900.62 "Информационная безопасность" / А.А. Губенков. - Саратов: СГТУ, 2015. - 84 с. Экземпляры всего: 3.
6. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.— ЭБС «IPRbooks», по паролю.
7. Малюк А.А. Введение в информационную безопасность [Электронный ресурс]: учебное пособие/ Малюк А.А., Горбатов В.С., Королев В.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 288с.— Режим доступа: http://www.iprbookshop.ru/11979.— ЭБС «IPRbooks», по паролю.

8. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Е.Б. Белов [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 558 с. — Режим доступа: http://www.iprbookshop.ru/12014.— ЭБС «IPRbooks», по паролю.
9. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю

Дополнительные издания

10.Пластун И.Л. Технология построения защищенных автоматизированных систем и сетей: учеб. пособие / И.Л. Пластун; Саратовский гос. техн. ун-т. - Саратов: СГТУ, 2010. - 96 с. Экземпляры всего: 40.
11. Пластун И.Л. Технология построения защищенных автоматизированных систем и сетей [Электронный ресурс]: учеб. пособие / И.Л. Пластун; Саратовский гос. техн. ун-т. - Электрон. текстовые дан. - Саратов : СГТУ, 2010. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/zak 260_10.pdf
12.Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов : СГТУ, 2009. - 88 с. Экземпляры всего: 5.
13. Губенков, А. А. Информационная безопасность вычислительных сетей [Электронный ресурс]: учеб. пособие / А.А. Губенков; Сарат. гос. техн. ун-т (Саратов). - Электрон. текстовые дан. - Саратов: СГТУ, 2009. - 1 эл. опт. диск (CD-ROM). Режим доступа: http://lib.sstu.ru/books/zak 479_09.pdf
14. Терещенко С. Н. Информационная безопасность и защита информации : учеб. пособие / С. Н. Терещенко. - Саратов : СГТУ, 2009. - 136 с. Экземпляры всего: 5.
15.Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. – М.: Академия, 2006. – 240 с. Экземпляры всего: 19.
16.Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф. - Электрон. текстовые данные. - М.:ДМК Пресс, 2010. - 544 с. Режим доступа: http://www.iprbookshop.ru/7943
17.Методы и средства защиты информации в компьютерных системах : учеб. пособие / П. Б. Хорев. - 2-е изд., стер. - М. : ИЦ "Академия", 2008. - 256 с. Экземпляры всего: 23.
18.Модели безопасности компьютерных систем : учеб. пособие для вузов / П.Н. Девянин. - М.: ИЦ "Академия", 2005. - 144 с. Экземпляры всего: 12.
19.Правовое обеспечение информационной безопасности : учеб. пособие для вузов / С.Я. Казанцев, О.Э. Згаздай, Р.М. Оболенский и др.; под ред. С.Я. Казанцева. - М.: ИЦ "Академия", 2008. - 240 с. Экземпляры всего: 9.

20.Защита от утечки информации по техническим каналам : учеб. пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. - М. : Горячая линия - Телеком, 2005. - 416 с. Экземпляры всего: 5.
21.Системный анализ в защите информации: учеб. пособие / А. А. Шумский, А.А. Шелупанов. - М.: Гелиос АРВ, 2005. - 224 с. Экземпляры всего: 10.
22.Основы информационной безопасности: учеб. пособие / С.П. Расторгуев. - М.: ИЦ "Академия", 2007. - 192 с. Экземпляры всего: 8.

Методические указания для обучающихся по освоению дисциплины

23.Программное обеспечение анализа информационных рисков "Гриф". Использование модели угроз и уязвимостей [Электронный ресурс]: метод. указания / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - Режим доступа: http://lib. sstu.ru/books/zak 88_08.pdf.
24.Программное обеспечение анализа информационных рисков "Гриф". Использование модели угроз и уязвимостей [Текст]: метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - 16 с. Экземпляры всего: 5.
25. Программное обеспечение анализа информационных рисков "Гриф". Использование модели информационных потоков [Электронный ресурс] : метод. указания / Сарат. гос. техн. ун-т; сост.: А.А. Губенков. - Саратов: СГТУ, 2008. - Режим доступа: http://lib.sstu.ru/books/zak 87_08.pdf.
26.Программное обеспечение анализа информационных рисков "Гриф". Использование модели информационных потоков [Текст] : метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т ; сост.: А.А. Губенков. - Саратов : СГТУ, 2008. - 18 с. Экземпляры всего: 5.
27.Использование программного обеспечения "КОНДОР" для разработки политики безопасности автоматизированных систем [Электронный ресурс] : метод. указания / Сарат. гос. техн. ун-т; сост. А.А. Губенков. - Саратов: СГТУ, 2009. - 1 эл. опт. диск (CD-ROM). - Режим доступа: http://lib. sstu.ru/books/zak 149_09.pdf.
28. Использование программного обеспечения "КОНДОР" для разработки политики безопасности автоматизированных систем [Текст] : метод. указания к выполнению лаб. работ / Сарат. гос. техн. ун-т (Саратов) ; сост. А.А. Губенков. - Саратов : СГТУ, 2009. - 16 с. Экземпляры всего: 5.

Периодические издания

29.Вестник Саратовского государственного технического университета: науч.-техн. журнал. - Саратов: Изд-во СГТУ, (2003-2015). - ISSN 1999-8341. Режим доступа: http://lib.sstu.ru/index.php/menuskrellib/91-mperiodizdan
30.Инновационная деятельность: науч.-аналит. журнал. - Саратов: Саратовский ГТУ им. Ю. А. Гагарина, (2010-2015). - ISSN 2071-5226.

Режим доступа: http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsionnaya-deyatelnost/
31.Журнал «Инновации + Паблисити». Режим доступа: http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsii-pablisiti/
32.Информационная безопасность регионов. Режим доступа: http://www.seun.ru/content/nauka /5/1/index.php.

Интернет-ресурсы

33. Искусство управления информационной безопасностью. URL:http://iso27000.ru/ (дата обращения: 1.06.2015).
34. SecurityLab.ru - информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. URL:http://www.securitylab.ru/ (дата обращения: 1.06.2015).
35. Архив изданий по информационной безопасности. URL:http://www.itsec.ru/ (дата обращения: 1.06.2015).
36. Информационный ресурс по безопасности. URL:http://www.securrity.ru (дата обращения: 1.06.2015).
37. Информационная безопасность вашего бизнеса. URL:http://www.leta.ru (дата обращения: 1.06.2015).

Источники ИОС

38. Весь лекционный материал размещен в электронной форме в ИОС направления ИВЧТ интернет-ресурсов СГТУ имени Гагарина Ю.А. https://portal.sstu.ru/Fakult/FETIP/IBS/b3362_/default.aspx - лекционный материал за 8 семестр.

16. Материально-техническое обеспечение дисциплины.

Для проведения лекционных занятий используется типовая лекционная аудитория со стандартным мультимедийным оснащением.

Для проведения лекционных занятий требуется комплект технических средств обучения в составе:

- персональный компьютер (в конфигурации не хуже: процессор Intel Pentium или AMD 2 ГГц, 2 ОЗУ Гбайта, 320 Гбайт НЖМД);
- проектор (разрешение не менее 1024x768);
- экран для проектора.

Для проведения лабораторных занятий и самостоятельной работы студентов используется компьютерный класс или учебная лаборатория каф. ИБС, оснащенная компьютерами.

Для проведения лабораторных занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор Intel Pentium или AMD 2 ГГц, ОЗУ 2 Гбайта, НЖМД 80 Гбайт. Компьютеры должны иметь подключение к локальной сети СГТУ и доступ к сети Интернет.

При проведении лабораторных занятий в качестве инструментальных средств используется следующее программное обеспечение:

1. Операционные системы: Windows XP/7 в составе DreamsPark Premium MS ИНЭТМ (Windows, Visual Studio), Ubuntu Linux.
2. Средства разработки программ: Microsoft Visual Studio Express в составе DreamsPark Premium MS ИНЭТМ, среда разработки NetBeans.
3. Антивирусные средства защиты Kaspersky Endpoint Security для Windows, Антивирус Касперского 6.0 для Windows Workstations.
4. Свободно распространяемые средства построения виртуальных машин. Например: VMWare Player или Virtual Box.
5. Архиватор RARLabs WinRAR.
6. Офисный пакет Microsoft Office Профессиональный плюс 2007 для подготовки и оформления отчетов.

Для проведения тестирования используется система тестирования знаний Ast-Test версия 3.