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

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине

«С.1.3.8.1 Обеспечение информационной безопасности организаций банковской системы»

специальности подготовки
10.05.03 "Информационная безопасность автоматизированных систем"
Специализация №9 "Создание автоматизированных систем в защищенном исполнении"

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 2
часов в неделю – 2
всего часов – 72,
в том числе:
лекции – 16
практические занятия – 16
самостоятельная работа – 40
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: обучение студентов основам проектирования, построения и анализа защищенных банковских систем, принципам и методам защиты информации в банковских сетях, а также содействие фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Задачи изучения дисциплины:

- изучение архитектуры защищенных банковских систем;
- изучение программно-аппаратных и технических средств создания защищенных банковских систем;
- изучение основных методов и программных инструментов, используемых для обеспечения информационной защищённости банковских систем;
- изучение правил организационной, технической и правовой защиты банковских систем;
- знакомство с методологией обследования и анализа защищенности банковских систем;
- получение базовых знаний и практических навыков по поиску и анализу уязвимостей банковских систем.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Обеспечение информационной безопасности организаций банковской системы» относится к числу дисциплин по выбору блока С.1.

Для успешного усвоения данной дисциплины 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 следующих компетенций:

- способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27).

Студент должен знать:

- методологические и технологические основы обеспечения информационной безопасности банковских систем;
- угрозы и методы нарушения информационной безопасности банковских систем;
- типовые модели атак, направленных на преодоление защиты банковских систем, условия их осуществимости, возможные последствия, способы предотвращения;
- роль человеческого фактора в обеспечении безопасности банковских систем;
- возможности, способы и правила применения основных программных и аппаратных средств защиты банковских систем;
- принципы функционирования основных сетевых протоколов (HTTP, SSL, TLS);
- основы применения межсетевых экранов для защиты банковских систем;
- методы создания защищённых банковских систем.

Студент должен уметь:

- проводить анализ банковских систем с точки зрения обеспечения информационной безопасности;
- разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;
- применять защищенные протоколы и межсетевые экраны, необходимые для реализации систем защиты банковских систем;

− реализовывать меры противодействия выявленным угрозам безопасности банковских систем с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения;
− реализовывать системы защиты банковских систем в соответствии со стандартами Банка России.

Студент должен владеть:
− навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, веб-серверов с учетом требований по обеспечению информационной безопасности;
− навыками проектирования защищенных банковских систем;
− навыками комплексного анализа защищенности банковских систем.

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

№ Мо-ду-ля	№ Не де ли	№ Те мы	Наименование темы	Часы/ Из них в интерактивной форме					
				Всего	Лек-ции	Коллок-виумы	Лабора-торные	Практичес-кие	СРС
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
8 семестр									
1	1	1	Введение	2	2	-	-	-	-
1	2	2	Основные направления защиты информации в банковских системах	20/2	4/2	-	-	2	14
1	6	3	Нормативно-правовая база защиты информации в кредитно-финансовых организациях	28/8	4/4	-	-	8/4	16
2	10	4	Организация службы информационной безопасности в кредитно-финансовых организациях	22/4	6/2	-	-	6/2	10
Всего				72/14	16/8	-	-	16/6	40

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. Общие положения обеспечения информационной безопасности современных автоматизированных банковских систем	1, 2, 3, 4, 5, 6, 7, 8, 25
2	2	2	Состав компонент комплексной системы обеспечения информационной безопасности банковских систем. Сущность и общее содержание комплексной системы обеспечения безопасности информационных технологий кредитно-финансовой организации. Факторы, влияющие на организацию системы защиты информационных ресурсов банка. Цель, задачи и методологические основы защиты информации АБС. Этапы работы по выявлению защищаемой информации. Основные этапы разработки системы защиты информационных технологий. Определение состава носителей защищаемой информации. Особенности защиты различных носителей информации. Персонал и информационная технология организации как объект защиты	2, 3, 4, 5, 6, 7, 9, 25
2	2	3	Определение и нормативное закрепление состава защищаемых информационных ресурсов. Классификация защищаемой информации. Порядок нормативного закрепления состава защищаемой информации. Система охраны интеллектуальной собственности, патентное законодательство и авторское право. Практика договорных правоотношений. Определение и виды рисков, их анализ. Экономический ущерб от случайных негативных воздействий	
3	2	4	Нормативно-правовая база информационной безопасности АБС. Структура и содержание нормативно-правовой базы информационной безопасности банковской системы. Закон РФ «О коммерческой тайне». Государственная система лицензирования и сертификации деятельности в области защиты информации Требования стандартов Банка России «Обеспечение информационной безопасности организаций банковской системы РФ». Основные положения стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения».	4, 5, 6, 7, 8, 9, 10, 11, 12, 25

			Конкретизация и развитие требований стандарта для обеспечения информационной безопасности банковских систем. Экономические аспекты защиты информации. Международные и отечественные стандарты и другие нормативные акты в области информационной безопасности	
3	**2**	**5**	Концепция обеспечения информационной безопасности банка. Концепция безопасности кредитно-финансовой организации как научно обоснованная система взглядов на определение основных направлений, условий и порядка экономичного решения задач защиты банковского дела от противоправных действий и влияния негативных факторов. Документы уполномоченных государственных организаций, их требования. Разработка концепции построения информационной системы в защищенном исполнении для обеспечения информационной безопасности банка (формирование модели угроз, модели ресурсов и модели нарушителя, выработка требований безопасности по всем подсистемам защиты). Понятие и методика построения политики информационной безопасности автоматизированной системы банка. Принципы безопасности систем и средств с банковскими картами	
4	**2**	**6**	Организация службы ИБ банка. Определение, классификация и общая характеристика организационно-технических задач службы информационной безопасности. Сущность и роль административных аспектов информационной безопасности. Человек как главное звено в системе защиты информации и как злоумышленник	11, 12, 13, 14, 15, 16, 17, 18, 25
4	**2**	**7**	Формирование правил и подразделений службы ИБ. Особенности создания правил и подразделений службы ИБ банка. Структура подразделений, ответственных за информационную безопасность банка, их функции. Оценка и выбор рациональной структуры службы ИБ банка. Документы, обеспечивающие правовую защиту информационных технологий в организациях различных форм собственности	
4	**2**	**8**	Комплексное обеспечение информационной безопасности АБС. Основные методы структурного подхода, особенности и этапы создания комплексной подсистемы обеспечения информационной безопасности банка. Методы и средства создания политики информационной безопасности банка и его АБС Критерии комплексности обеспечения информационной безопасности банков различных форм собственности. Угрозы и риски. Каналы утечки информации. Визуальные и	

			акустические каналы. Технические закладки. Способы обнаружения. Методы оценки степени опасности. Способы и методы перекрытия каналов утечки информации. Особенности защиты информации ПЭВМ. Определение и основные цели защиты современных объектов информатики. Технические средства обеспечения защиты банковского объекта: определение, системная классификация, общий анализ. Технические средства и системы охраны территории, зданий и помещений, а также наблюдения и контроля за перемещением людей и предметов. Технические средства и системы опознавания людей, управления доступом на территорию, в здания и помещения, к средствам обработки и хранения информации. Безопасность инфраструктуры пластиковых карт	

6. Содержание коллоквиумов

Коллоквиумы учебным планом не предусмотрены.

7. Перечень практических занятий

№ темы	Всего часов	№ занятия	Тема практического занятия. Задания, вопросы, отрабатываемые на практическом занятии	Учебно-методическое обеспечение
1	2	3	4	5
2	2	1	Определение состава защищаемой информации банка с учетом влияния различных факторов. Построение схемы архитектуры автоматизированной банковской системы.	1, 2, 3, 4, 5, 6, 7, 8, 25
3	4	2	Построение модели угроз для информационных ресурсов банка.	1, 2, 3, 4, 5, 6, 7, 8, 25
3	4	3	Разработка типовой политики безопасности автоматизированной банковской системы	1, 2, 3, 4, 5, 6, 7, 8, 25
4	2	4	Использование VPN на базе протокола IPSec в автоматизированных банковских системах	1, 2, 3, 4, 5, 6, 7, 8, 25
4	4	5	Выявление и блокирование каналов несанкционированного доступа к информации АБС	1, 2, 3, 4, 5, 6, 7, 8, 25

8. Перечень лабораторных работ

Лабораторные работы учебным планом не предусмотрены.

9. Задания для самостоятельной работы студентов

№ темы	Всего Часов	Задания, вопросы, для самостоятельного изучения (задания)	Учебно-методическое обеспечение
1	2	3	4
2	4	Обзор стандарта PKCS RSA Encryption	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 28

2	6	Обзор стандарта Internet X.509 Public Key Infrastructure	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 28
2	4	Обзор стандарта Online Certificate Status Protocol	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 28
3	6	Анализ действующих нормативно-правовых документов по защите информации	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 28
3	4	Обзор стандарта PCI DSS	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 28
3	6	Особенности страхования ущерба от компьютерных преступлений	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 28
4	10	Обнаружение каналов утечки информации	1, 2, 3, 5, 6, 7, 8, 18, 19, 20, 21, 22, 28

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

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
8 семестр			
1-2	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	8 (промежуточная аттестация), зачет
3-4	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	Зачет

Методические указания по самостоятельному изучению отдельных разделов дисциплины приведены в соответствующем разделе ИОС [28].

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 (модулю)

Изучение дисциплины направлено на формирование следующих компетенций: ОПК-6, ПК-20, ПК-27.

Карта компетенции ОПК-6: способность применять нормативные правовые акты в профессиональной деятельности

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
1	С.1.3.8.1 «Обеспечение информационной безопасности организаций банковской системы»	Знает: - принципы функционирования основных сетевых протоколов (HTTP, SSL, TLS); - методы создания защищённых банковских систем: - возможности, способы и правила применения основных программных и аппаратных средств защиты банковских систем;	Лекции Самостоятельная работа Семинары	Тестирование
		Умеет: - реализовывать системы защиты банковских систем в соответствии со стандартами по оценке защищенных систем;	Практические работы с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
		Владеет: - навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, веб-серверов с учетом требований по обеспечению информационной безопасности; - навыками проектирования защищенных банковских систем;	Лекции Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Зачет

Карта компетенции ПК-20: способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
1	С.1.3.8.1 «Обеспечение информационной безопасности организаций банковской системы»	Знает: - принципы функционирования основных сетевых протоколов (HTTP, SSL, TLS); - методы создания защищённых банковских систем; - угрозы и методы нарушения информационной безопасности банковских систем;	Лекции Самостоятельная работа Семинары	Тестирование
		Умеет: - проводить анализ банковских систем с точки зрения обеспечения информационной безопасности;	Практические работы с использованием активных и интерактивных приемов обучения.	Тестирование рефераты

		- разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;	Самостоятельная работа	
		Владеет: - навыками комплексного анализа защищенности банковских систем; - навыками проектирования защищенных банковских систем.	Лекции Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Зачет

Карта компетенции ПК-27: способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы

№ п/п	Наименование дисциплины и код по базовому учебному плану	Части компонентов	Технологии формирования	Средства и технологии оценки
1	2	3	4	5
1	С.1.3.8.1 «Обеспечение информационной безопасности организаций банковской системы»	Знает: - принципы функционирования основных сетевых протоколов (HTTP, SSL, TLS); - методы создания защищённых банковских систем; - угрозы и методы нарушения информационной безопасности банковских систем;	Лекции Самостоятельная работа Семинары	Тестирование
		Умеет: - проводить анализ банковских систем с точки зрения обеспечения информационной безопасности; - разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;	Практические работы с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Тестирование рефераты
		Владеет: - навыками комплексного анализа защищенности банковских систем; - навыками проектирования защищенных банковских систем.	Лекции Практические занятия с использованием активных и интерактивных приемов обучения. Самостоятельная работа	Зачет

Формирование профессиональных компетенций по дисциплине производится на практических 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. Состав компонент комплексной системы обеспечения информационной безопасности банковских систем.
2. Сущность и общее содержание комплексной системы обеспечения безопасности информационных технологий кредитно-финансовой организации. Факторы, влияющие на организацию системы защиты информационных ресурсов банка.
3. Цель, задачи и методологические основы защиты информации АБС. Этапы работы по выявлению защищаемой информации.
4. Основные этапы разработки системы защиты информационных технологий.
5. Определение состава носителей защищаемой информации. Особенности защиты различных носителей информации.
6. Персонал и информационная технология организации как объект защиты.
7. Классификация защищаемой информации. Порядок нормативного закрепления состава защищаемой информации. Система охраны интеллектуальной собственности, патентное законодательство и авторское право.
8. Определение и виды рисков, их анализ. Экономический ущерб от случайных негативных воздействий.
9. Структура и содержание нормативно-правовой базы информационной безопасности банковской системы. Закон РФ «О коммерческой тайне».
10. Государственная система лицензирования и сертификации деятельности в области защиты информации.
11. Структура семейства стандартов Банка России «Обеспечение информационной безопасности организаций банковской системы РФ».
12. Основные положения стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения».

13. Международные и отечественные стандарты и другие нормативные акты в области информационной безопасности.
14. Концепция обеспечения информационной безопасности банка.
15. Концепция безопасности кредитно-финансовой организации как научно-обоснованная система взглядов на определение основных направлений, условий и порядка экономичного решения задач защиты банковского дела от противоправных действий и влияния негативных факторов.
16. Разработка концепции построения информационной системы в защищенном исполнении для обеспечения информационной безопасности банка (формирование модели угроз, модели ресурсов и модели нарушителя, выработка требований безопасности по всем подсистемам защиты).
17. Понятие и методика построения политики информационной безопасности автоматизированной системы банка. Принципы безопасности систем и средств с банковскими картами.
18. Стандарты информационной безопасности (ГОСТ 17799, ГОСТ 15408-99).
19. Этапы жизненного цикла подсистемы ИБ. Связи, существующие между жизненным циклом АБС и жизненным циклом подсистемы ИБ.
20. Определение, классификация и общая характеристика организационно-технических задач службы информационной безопасности. Сущность и роль административных аспектов информационной безопасности. Человек как главное звено в системе защиты информации и как злоумышленник.
21. Формирование правил и подразделений службы ИБ. Особенности создания правил и подразделений службы ИБ банка.
22. Структура подразделений, ответственных за информационную безопасность банка, их функции. Оценка и выбор рациональной структуры службы ИБ банка. Документы, обеспечивающие правовую защиту информационных технологий в организациях различных форм собственности.
23. Основные методы структурного подхода, особенности и этапы создания комплексной подсистемы обеспечения информационной безопасности банка. Методы и средства создания политики информационной безопасности банка и его АБС.
24. Каналы утечки информации. Визуальные и акустические каналы. Технические закладки. Способы обнаружения. Методы оценки степени опасности. Способы и методы перекрытия каналов утечки информации. Особенности защиты информации ПЭВМ. Определение и основные цели защиты современных объектов информатики.
25. Технические средства и системы охраны территории, зданий и помещений, а также наблюдения и контроля за перемещением людей и предметов.
26. Технические средства и системы опознавания людей, управления доступом на территорию, в здания и помещения, к средствам обработки и хранения информации.
27. Безопасность инфраструктуры пластиковых карт.

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:

Внутренняя аналитика приложений банковских систем это:

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

2. Основными угрозами для банковских систем 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 банковских систем 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.

14. Образовательные технологии

Для реализации компетентностного подхода в соответствии с требованиями ФГОС ВО 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 14 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. Мельников В.П. 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
3. 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.
4. Губенков А.А. Обеспечение безопасности персональных данных [Электронный ресурс]: учеб. пособие для студ. направления 090303.65 "Информационная безопасность автоматизированных систем" и бакалавров направления 090900.62 "Информационная безопасность" / А.А. Губенков; Саратовский гос. техн. ун-т. - Электрон. текстовые дан. - Саратов : СГТУ, 2015. - 1 эл. опт. диск (CD-ROM). - ISBN 978-5-7433-2786-7. Электронный аналог печатного издания. Режим доступа: http://lib.sstu.ru/books/zak 51_15.pdf

Дополнительные издания

5. 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.
6. 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
7. Губенков А.А. Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов : СГТУ, 2009. - 88 с. Экземпляры всего: 2.
8. 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
9. Терещенко С. Н. Информационная безопасность и защита информации : учеб. пособие / С. Н. Терещенко. - Саратов : СГТУ, 2009. - 136 с. Экземпляры всего: 3.
10.Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. – М.: Академия, 2006. – 240 с. Экземпляры всего: 19.
11. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие / П. Б. Хорев. - М. : ИЦ "Академия", 2005, 2006, 2007, 2008. - 256 с. Экземпляры всего: 33.
12. Девянин П.Н. Модели безопасности компьютерных систем : учеб. пособие для вузов / П.Н. Девянин. - М.: ИЦ "Академия", 2005. - 144 с. Экземпляры всего: 12.
13. 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: 10.
14. Бузов Г.А. 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.
15. Шумский А.А. Системный анализ в защите информации: учеб. пособие / А.А. Шумский, А.А. Шелупанов. - М.: Гелиос АРВ, 2005. - 224 с. Экземпляры всего: 10.
16. Расторгуев С.П. Основы информационной безопасности: учеб. пособие / С.П. Расторгуев. - М.: ИЦ "Академия", 2007. - 192 с. Экземпляры всего: 8.

Методические указания для обучающихся по освоению дисциплины

17. 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.
18. 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

19.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
20.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/
21.Журнал «Инновации + Паблисити». Режим доступа: http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsii-pablisiti/
22. Журнал «BIS Journal - Информационная безопасность банков». Режим доступа: https://journal.ib-bank.ru.

Интернет-ресурсы

23. Искусство управления информационной безопасностью. URL:http://iso27000.ru/ (дата обращения: 1.06.2015).
24. 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).
25. Архив изданий по информационной безопасности. URL:http://www.itsec.ru/ (дата обращения: 1.06.2015).
26. Информационный ресурс по безопасности. URL:http://www.securrity.ru (дата обращения: 1.06.2015).
27. Информационная безопасность вашего бизнеса. URL:http://www.leta.ru (дата обращения: 1.06.2015).

Источники ИОС

28. Весь лекционный материал размещен в электронной форме в ИОС специальности ИБС интернет-ресурсов СГТУ имени Гагарина Ю.А. https://portal3.sstu.ru/Facult/MFPIT/MFPIT-IBS/10.05.03/C.1.3.7.1/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, 4 Гбайта ОЗУ, 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 ИНПИТ (Windows, Visual Studio), Ubuntu Linux.
2. Средства разработки программ: Microsoft Visual Studio Express в составе DreamsPark Premium MS ИНПИТ, 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 2007 для подготовки и оформления отчетов.

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