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

Кафедра «Информационная безопасность автоматизированных систем»

РАБОЧАЯ ПРОГРАММА

по дисциплине Б.1.1.23 «Основы управления информационной безопасностью»

направления подготовки
10.03.01 «Информационная безопасность»
Профиль «Безопасность автоматизированных систем»

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 2
часов в неделю – 2
всего часов – 72
лекции – 16
коллоквиумы - 2
практические занятия – 18
самостоятельная работа – 36
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

Задачи изучения дисциплины:
1) изучение основных понятий и методологий управления информационной безопасностью;
2) получение знаний и навыков в области оценки рисков информационной безопасности;
3) изучение методологии проведения аудита информационной безопасности;
4) приобретение обучаемыми необходимого объема знаний в области организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;
5) формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Основы управления информационной безопасностью» относится к числу дисциплин базовой части профессионального цикла.

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.

Знания и практические навыки, полученные при изучении дисциплины «Основы управления информационной безопасностью», используются при написании итоговой аттестационной работы.

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15);

Студент должен знать:

– значение управлением информационной безопасностью в условиях развития современного общества;

– содержание основных нормативно-правовых актов, регламентирующих вопросы в сфере управления информационной безопасностью;

– процедуры организации технологического процесса защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Студент должен уметь:

– применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

– применять нормативные правовые акты и нормативные методические документы в сфере управления информационной безопасностью;

– классифицировать действующие нормативные и методические документы ФСТЭК России, ФСБ России и Роскомнадзора в соответствии с их полномочиями;

– разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем;

– разрабатывать частные политики информационной безопасности информационной безопасности автоматизированных систем;

– определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем.

Студент должен владеть навыками:

– навыками формирования требований по защите информации;

– навыками работы с нормативными правовыми актами в области управления информационной безопасности;

– навыками работы с технологиями поиска нормативных правовых актов и нормативных методических документов в области управления информационной безопасности в глобальных компьютерных системах, сетях, в библиотечных фондах и в иных источниках информации;

– навыками мониторинга и аудита, выявления угроз информационной безопасности;

– навыками формирования требований по защите информации;

– методами управления информационной безопасностью.

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	Система управления информационной безопасностью	22/2	4	-	-	6/2	12
1	4	2	Политика информационной безопасности	26/10	6/6	2/2	-	6/2	12
2	8	3	Аудит информационной безопасности	24/8	6/6	-	-	6/2	12
Всего				72/20	16/12	2/2	-	18/6	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	Тема 1. Система управления информационной безопасностью. Системный подход к проектированию, внедрению и поддержанию системы обеспечения информационной безопасности на предприятии.	1, 2, 11, 12
1	2	2	Стандартизация в сфере управления информационной безопасностью (стандарты ГОСТ Р ИСО/МЭК 17799-2005, ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 27002-2012, ГОСТ Р ИСО/МЭК 27004-2011, ГОСТ Р ИСО/МЭК 27005-2010, ГОСТ Р ИСО/МЭК 27006-2008).	2, 5
1	2	3	Ресурсы предприятия, подлежащие защите. Комплекс методов и средств защиты информации как объект управления информационной безопасностью.	3, 11,
2	2	4	Тема 2. Политика информационной безопасности. Перечень нормативно-методических и организационно-распорядительных документов по защите информации на предприятии. Концепция безопасности предприятия.	2, 3, 4
2	2	5	Назначение и содержание политики информационной безопасности предприятия в целом, его структурных подразделений, частных политик безопасности.	3, 4
2	2	6	Разграничение полномочий и ответственности персонала, обеспечивающего реализацию положений нормативно-методических и организационно-распорядительных документов по защите информации на предприятии.	3, 6
3	2	7	Тема 3. Аудит информационной безопасности. Назначение, цели и виды аудита. Требования к аудитору, особенности взаимодействия между аудитором и заказчиком. Оценка	1, 6

			работы аудитора.	
3	2	8	Стандартизация в сфере аудита информационной безопасности. Содержание и организация процесса аудита. Оценка рисков. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита.	1, 6
3	2	9	Программные средства автоматизации процедур проведения аудита и анализа политики безопасности.	1, 5, 12, 13, 14

6. Содержание коллоквиумов

№ темы	Всего часов	№ коллоквиума	Тема коллоквиума. Вопросы, отрабатываемые на коллоквиуме	Учебно-методич обеспечение
1	2	3	4	5
1	2	1	Расчет класса защищенности информационной системы в соответствии с методическими документами ФСТЭК России	1-4
2	2	2	Выбор мер защиты информации и средств защиты ИС ПДн в соответствии с методическими документами ФСТЭК России	1-4

7. Перечень практических занятий

№ темы	Всего часов	Наименование практического занятия. Задания, вопросы, отрабатываемые на занятии	Учебно-методическое обеспечение
1	2	3	4
1	4	Использование модели информационных потоков. Инвентаризация информационных ресурсов.	1, 5, 6, 7, 17
2	4	Использование программного обеспечения «Кондор» для разработки политики безопасности автоматизированных систем	1, 5, 6, 7, 17
2	4	Расчет рисков невыполнения требований раздела «Политика безопасности» ГОСТ 17799	1, 5, 6, 7, 17
2	4	Расчет рисков невыполнения требований раздела «Непрерывность ведения бизнеса» ГОСТ 17799	1, 5, 6, 7, 17
3	8	Анализ рисков ИС на основе модели информационных потоков Расчет рисков по угрозам конфиденциальность и целостность. Расчет рисков по угрозе отказ в обслуживании. Задание контрмер	1, 5, 6, 7, 17
3	4	Построение модели информационной системы на основе модели угроз и уязвимостей	1, 5, 6, 7, 17
3	8	Анализ рисков информационной системы	1, 5, 6, 7, 17

		на основе модели угроз и уязвимостей	

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
1	20	Международные стандарты в сфере управления информационной безопасностью	6, 8, 9, 10, 11
2	14	Программные средства автоматизации процедур проведения аудита информационной безопасности и анализа политики информационной безопасности	5, 12-16
3	20	Программные средства поддержки процессов управления информационной безопасностью	5, 12-16

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

№ темы	Вид СРС	Вид контроля СРС	График контроля (№ недели)
8 семестр			
1	Работа с печатными источниками, разбор типовых заданий	Рубежный контроль, промежуточный контроль, самоконтроль	Промежуточная аттестация, зачет
2,3	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 [17].

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)

В процессе освоения образовательной программы формируется отдельные элементы компетенций ПК-4, ПК-15. Содержание лекционного курса и практических занятий формируют на рассматриваемом этапе элементы компетенций в части, касающейся управления информационной безопасности, необходимых для решения научно-практических задач, стоящих перед отраслью.

Процедура оценивания знаний, умений и навыков проводится в соответствии со следующими методическими материалами и заключается в проведении устного экзаменационного опроса в виде диалога преподавателя со студентом, цель которого – систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала; отчетов по лабораторным работам, для оценки способности студента применить полученные ранее знания для организации системы управления информационной безопасностью, в проведении модулей и коллоквиумов, как способов межсессионной проверки знаний, умений, навыков студента в середине семестра по пройденным темам изучаемого предмета.

Показателем оценивания степени усвоения знаний этого элемента компетенции, является оценка, полученная на зачете при ответе на вопросы для зачета. Оценка выставляется по четырехбалльной шкале, соответствующей оценкам «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и осуществляется путем анализа ответа на вопросы для зачета. При этом руководствуются следующими критериями.

Оценка	**Критерии оценивания результатов обучения (дескрипторы)**
Отлично	заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой, усвоивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой.
Хорошо	заслуживает обучающийся, обнаруживший полное знание учебного материала, усвоивший основную литературу, рекомендованную в программе. Оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.
Удовлетворительно	заслуживает обучающийся, обнаруживший знания основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей

	работы по профессии, знакомых с основной литературой, рекомендованной программой. Оценка выставляется обучающимся, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя.
Неудовлетворительно	выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебного материала. Оценка ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании образовательного учреждения без дополнительных занятий по рассматриваемой дисциплине.

Умения и навыки, приобретенные студентом на этапе освоения указанных частей компетенций при преподавании рассматриваемой дисциплины, оцениваются по результатам выполнения лабораторных работ, включающих одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описание результата, который нужно получить. Показателем оценивания степени усвоения знаний элементов компетенций, является оценка, полученная при ответе на лабораторных работах. Оценка выставляется по четырехбальной шкале, соответствующей оценкам «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и осуществляется путем анализа представленного материала в ответ на практические контрольные задания. При этом руководствуются следующими критериями:

Оценка	**Критерии оценивания результатов обучения (дескрипторы)**
Отлично	выставляется студенту, если задание выполнено в полном объёме с соблюдением необходимой последовательности. Студенты работают полностью самостоятельно: подбирают необходимые для выполнения предлагаемых работ в задании источники знаний, показывают необходимые для проведения практической работы теоретические знания, практические умения и навыки.
Хорошо	выставляется студенту, если задание выполнено в полном объёме и самостоятельно. Допускаются отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Студенты используют указанные преподавателем источники знаний, включая страницы атласа, таблицы из приложения к учебнику, страницы из справочной литературы по

	предмету. Задание показывает знание учащихся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Могут быть неточности и небрежность в оформлении результатов работы.
Удовлетворительно	выставляется студенту, если задание на лабораторную работу выполняется и оформляется студентами при помощи преподавателя или хорошо подготовленных и уже выполненных на «отлично» данную работу студентов. На выполнение задания затрачивается много времени (можно дать возможность доделать работу дома). Студенты показывают знания теоретического материала, но испытывают затруднение при решении конкретной задачи.
Неудовлетворительно	выставляется, если студенты показывают плохое знание теоретического материала и отсутствие умения применить знания к решению практической задачи. Руководство и помощь со стороны преподавателя и хорошо подготовленных студентов неэффективны по причине плохой подготовки студента.

Оценки «отлично», «хорошо» и «удовлетворительно» служит основанием для зачета знаний, умений и навыков по дисциплине с простановкой в ведомости «зачтено».

Вопросы для зачета

1. Проблема человеческого фактора в ИБ. Типы внутренних угроз.
2. Понятие уязвимости. Формирование ландшафта уязвимых точек.
3. Моделирование и классификация угроз ИБ.
4. Понятие риска в ИБ. Способы оценки информационных рисков.
5. Программные средства анализа и управления рисками.
6. Основные положения стандарта ГОСТ 17799.
7. Создание системы менеджмента информационной безопасности (ГОСТ 27001). Процедура сертификации.
8. Аудит информационной безопасности: цели, виды, этапы проведения, результаты.
9. Цели и задачи формирования политики безопасности. Структура документа.
10. Основные положения стандарта ГОСТ 15408 «Критерии оценки безопасности информационных технологий»
11. Требования, учитываемые при выборе мер противодействия. Многоуровневая защита.

Тестовые задания по дисциплине

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

Примеры тестовых заданий:

Политика безопасности организации это:

a) совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов
b) комплекс мер, направленных на обеспечение информационной безопасности организации
c) набор программно-аппаратных средств и административных распоряжений, предназначенных для реализации и обеспечения защиты информации в информационной системе предприятия

Для чего предназначены средства управления доступом?

a) специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами);
b) для идентификации субъектов;
c) для управления реляционными базами данных.

Какие криптографические системы называются симметричными?

a) Используют один и тот же ключ как для зашифрования, так и для расшифрования информации;
b) применяются *пары ключей*: *открытый* (*public key*), который зашифровывает данные, и соответствующий ему *закрытый* (*private key*), который их расшифровывает;
c) Метод криптозащиты представляет собой контрольное суммирование информации

Что такое Токен?

a) это предмет (устройство), владение которым подтверждает подлинность пользователя
b) Устройства контроля биометрических характеристик
c) Криптографическая система

Что такое криптография?

a) это наука о методах обеспечения секретности и подлинности (идентичности) данных при их передаче по линиям связи или хранении;
b) это наука о методах раскрытия или подделки данных;
c) методы скрытия самого факта передачи сообщения.

Что такое протоколирование?

a) сбор и накопление информации о событиях, происходящих в информационной системе предприятия;
b) принудительное управление доступом;
c) обмен данными между различными сервисами

7.**Что такое аудит?**

a) это анализ накопленной информации, проводимый оперативно, (почти) в реальном времени, или периодически (например, раз в день);
b) это множество обратимых преобразований формы открытого текста;

c) это атака на шифр, раскрытие шифра со стороны взломщика.

Под политикой безопасности мы будем понимать:

a) совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов
b) Формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей
c) управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности.

Какие устройства шифрования обеспечивают более высокое качество защиты информации?

a) Аппаратные;
b) Программно-аппаратные;
c) Программные.

Код аутентификации сообщения (MAC) позволяет:

1. защитить сообщение так, что никто не сможет прочитать электронный документ, кроме того, кому он действительно предназначается.
2. проверить хеш-значение электронного документа.
3. проверить, что электронный документ прислал именно тот человек, который обозначен как автор, и что документ по пути не изменился.
4. доказать третьему лицу, что электронный документ получен именно от того человека, который обозначен как автор, и что документ по пути не изменился.

Электронная цифровая подпись (ЭЦП) позволяет:

1. проверить, что электронный документ получил именно тот человек, который обозначен как получатель, и что документ по пути не изменился.
2. обеспечить целостность электронных документов, передаваемых по незащищенным телекоммуникационным каналам общего пользования, с гарантированной идентификацией ее автора (лица, подписавшего документ).
3. доказать третьему лицу, что электронный документ создан (или обрабатывался) на конкретной ЭВМ.
4. защитить сообщение так, что никто не сможет прочитать электронный документ, кроме того, кому он действительно предназначается.

Стандарт ГОСТ 28147-89 определяет:

1. алгоритм криптографического преобразования для систем обработки информации в сетях ЭВМ, отдельных вычислительных комплексах и ЭВМ, который определяет правила шифрования данных и выработки имитовставки.
2. алгоритм вычисления хэш-функции для любой последовательности двоичных символов.
3. алгоритм формирования и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
4. общие технические требования по криптографической защите информации.

Какой из приведенных ниже вариантов совместного использования межсетевого экрана (МЭ) и VPN-шлюза на границе между локальной сетью и Интернет является наиболее безопасным:

1. Интернет → МЭ → VPN-шлюз → Локальная сеть.

2. Интернет → VPN-шлюз → МЭ → Локальная сеть.
3. Совмещение функций МЭ и VPN-шлюза в одном устройстве.
4. Наличие VPN-шлюза образует брешь в защите МЭ, т.к. пользователь, обладающий доступом к VPN, имеет возможность проникнуть в сеть в обход МЭ. Поэтому совместное использование МЭ и VPN-шлюза не рекомендуется.

Какая из перечисленных функций не применяется в VPN-комплексах при передаче информации через открытые каналы связи (Интернет):
1. аутентификация (установление подлинности) взаимодействующих сторон.
2. шифрование передаваемых данных.
3. подтверждение подлинности и целостности доставленной информации.
4. распределение пропускной способности канала связи между приложениями.

Какой из перечисленных VPN-комплексов теоретически является наиболее уязвимым для атак злоумышленников:
1. VPN-комплекс на основе специализированного программного обеспечения.
2. VPN-комплекс, совмещенный с аппаратной частью маршрутизатора.
3. VPN-комплекс, являющийся частью аппаратного межсетевого экрана.
4. Специализированный программно-аппаратный VPN-комплекс.

Какой из Законов РФ является основным в структуре федеральных законодательных актов по защите информации?
a) «О безопасности»
b) «О государственной тайне»
c) «Об участии в международном информационном обмене»
d) «Об информации, информатизации и защите информации»

Конфиденциальная информация – это:
a) документированная информация, доступ к которой ограничен в соответствии с законодательством РФ
b) документированная информация, доступ к которой ограничен её владельцем
c) документированная информация, доступ к которой ограничен её пользователем
d) информация, составляющая государственную тайну

Несанкционированный доступ – это:
a) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами выч. техники или автоматизированной системы
b) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием внештатных средств, выходящих за рамки допустимых средств воздействия, предоставляемых средствами выч. техники или автоматизированной системы
c) доступ к информации, нарушающий установленные правила разграничения доступа, с привлечением вредоносных программно-аппаратных средств

Существует несколько уровней возможностей, предоставляемых потенциальному нарушителю штатными средствами выч. техники или автоматизированной системы. К какому уровню Вы отнесёте себя в соответствии со своими должностными обязанностями?
a) 0-й уровень
b) 1-й уровень
c) 2-й уровень

d) 3-й уровень
e) 4-й уровень

Какие из нижеперечисленных вредоносных программ требуют обязательного наличия программы-носителя?

a) Троянские кони
b) Бактерии
c) Вирусы
d) Сетевые черви

Какую из нижеперечисленных программ по методам воздействия напоминает спам?

a) Троянские кони
b) Бактерии
c) Вирусы
d) Сетевые черви
e) Логические бомбы

Какого типа брандмауэров не существует?

a) Экранирующий маршрутизатор
b) Шлюз сеансового уровня
c) Шлюз прикладного уровня
d) Шлюз физического уровня

Какая из нижеперечисленных функций межсетевым экраном не выполняется?

a) Идентификация и аутентификация пользователей
b) Фильтрация информационных потоков
c) Разграничение доступа к ресурсам внутренней сети
d) Шифрование исходящей информации

Внутренняя аналитика приложений информационных 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

Основными угрозами для информацилнных систем являются следующие причины:

1. Секретные данные в открытом виде;
2. Небезопасные каналы передачи информации;
3. Внедрение SQL-операторов;
4. Управление сессиями

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

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.

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

Лидирующей атакой для банковских систем является

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

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.

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.

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.

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 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 22 ч.

15. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Обязательные издания

1. Милославская Н.Г. Проверка и оценка деятельности по управлению информационной безопасностью [Электронный ресурс]: учебное пособие/ Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 166 с.— Режим доступа: http://www.iprbookshop.ru/12032.— ЭБС «IPRbooks», по паролю
2. Основы управления информационной безопасностью [Электронный ресурс]: учебное пособие/ А.П. Курило [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 244 с.— Режим доступа: http://www.iprbookshop.ru/12021.— ЭБС «IPRbooks», по паролю
3. Милославская Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью [Электронный ресурс]: учебное пособие/ Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 214 с.— Режим доступа: http://www.iprbookshop.ru/12056.— ЭБС «IPRbooks», по паролю

Дополнительные издания

4. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.— Режим доступа: http://www.iprbookshop.ru/15845.— ЭБС «IPRbooks», по паролю
5. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность [Электронный ресурс]/ Петренко С.А.— Электрон. текстовые данные.— М.: ДМК Пресс, 2007.— 384 с.— Режим доступа: http://www.iprbookshop.ru/7639.— ЭБС «IPRbooks», по паролю
6. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991.— ЭБС «IPRbooks», по паролю

Методические указания для обучающихся по освоению дисциплины

7. 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.

Периодические издания

8. Вестник СГТУ (http://lib.sstu.ru/index.php/menuskrellib/91-mperiodizdan)

9. Инновационная деятельность (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsionnaya-deyatelnost/)
10.Журнал «Инновации + Паблисити» (http://www.sstu.ru/nauka/nauchnye-izdaniya/innovatsii-pablisiti/)
11.Информационная безопасность регионов (http://www.seun.ru/content/nauka/5/1/index.php).

Интернет-ресурсы

12.Искусство управления информационной безопасностью. URL:http://iso27000.ru/ (дата обращения: 1.06.2015).
13.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).
14.Архив изданий по информационной безопасности. URL:http://www.itsec.ru/ (дата обращения: 1.06.2015).
15.Информационный ресурс по безопасности. URL:http://www.securrity.ru (дата обращения: 1.06.2015).
16.Информационная безопасность вашего бизнеса. URL:http://www.leta.ru (дата обращения: 1.06.2015).

Источники ИОС

17.Весь лекционный материал размещен в электронной форме в ИОС направления ИБС интернет-ресурсов СГТУ имени Гагарина Ю.А.
https://portal.sstu.ru/Fakult/FETIP/IBS/c3116/default.aspx.

16. Материально-техническое обеспечение дисциплины.

Для проведения лекционных занятий требуется комплект технических средств обучения в составе:
– персональный компьютер (в конфигурации не хуже: процессор Intel Core 2 Duo, 2 Гбайта ОЗУ, 500 Гбайт НЖМД);
– проектор (разрешение не менее 1280x1024);
– экран для проектора.

Для проведения практических занятий требуется компьютерный класс, оборудованный ПЭВМ в конфигурации не худшей чем: процессор Pentium IV 3 ГГц, ОЗУ 2 Гбайта, НЖМД 200 Гбайт.

При проведении лабораторных занятий в качестве инструментальных средств используется: Программное обеспечение «Digital Security Office 2006 – Академическая версия».