СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Системы обнаружения атак***

Блок Б1, вариативная часть, Б1.В.ДВ.06.02
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

Разработчик (составитель)

Мифтахов Э. Н.
ученая степень, должность, ФИО

Стерлитамак 2023

1. Перечень компетенций с указанием этапов их формирования и описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Формируемая компетенция (с указанием кода)	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3				4
		неуд.	удовл.	хорошо	отлично	
Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)	1 этап: Знания	Отсутствие знаний в области основных требований к защите информации с применением математического аппарата для решения прикладных задач	Наличие частичных знаний, позволяющих организовать лишь основные аспекты защиты информации с применением математического аппарата для решения прикладных задач	Наличие знаний, позволяющих организовать основные аспекты защиты информации, однако применение математического аппарата для некоторых случаев представления может вызывать затруднения	Наличие знаний в области соблюдения требования по защите информации, включая использование математического аппарата для решения прикладных задач в общем их представлении	тестовые материалы
	2 этап: Умения	Отсутствие элементарных умений в области разработки и анализа структурных и функциональных схем защищенных компьютерных	Наличие элементарных умений в области разработки структурных и функциональных схем защищенных компьютерных систем в сфере	Наличие знаний, позволяющих проводить разработку и анализ структурных и функциональных схем защищенных компьютерных систем в в узком	Наличие знаний, позволяющих проводить разработку и анализ структурных и функциональных схем защищенных компьютерных систем в в массовом	лабораторные задания

		систем в сфере профессиональной деятельности.	профессиональной деятельности, однако отсутствие элементарных знаний в области анализа описанных схем	перечне сфер профессиональной деятельности.	сегменте сфер профессиональной деятельности.	
	3 этап: Владения (навыки / опыт деятельности)	Отсутствие знаний в области применения навыков оценивания оптимальности выбора программно-аппаратных средств защиты информации.	Наличие лишь основных знаний в области применения навыков оценивания оптимальности выбора программно-аппаратных средств защиты информации.	Наличие знаний в области применения навыков оценивания оптимальности, однако при выборе программно-аппаратных средств защиты информации могут возникать проблемы.	Наличие подлинного перечня в области применения навыков оценивания оптимальности, а также при выборе программно-аппаратных средств защиты информации.	лабораторные задания

2. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тестовый материал

Перечень вопросов для оценки уровня сформированности компетенции **ПК-4** на этапе «Умения»

1. Какой из типов нормативно-правовых документов регламентирует Информационную безопасность в Российской Федерации?
   a. Акты федерального законодательства
   b. Нормативно-методические документы государственных органов
   c. Стандарты информационной безопасности
   d. Все выше перечисленные
2. Что не считается персональными данными?
   a. Фамилия, Имя, Отчество
   b. год, месяц, дата и место рождения, адрес
   c. семейное, социальное, имущественное положение
   d. образование, профессия, доходы, другая информация
   e. здесь нет верного ответа
3. Основные задачи SOC (Security Operation Center): консолидация событий из множества источников
   a. проведение определенной аналитики
   b. оповещение уполномоченных сотрудников об инцидентах ИБ или иных происшествиях
   c. систематизированный сбор данных пользователей и предоставление к ним общего доступа
4. Обязанности сотрудников, обслуживающих SOC (Security Operation Center):
   a. проводят расследование
   b. принимают меры, чтобы исключить возможность повторения события
   c. прикладывают усилия для повторения события
   d. минимизируют потери
5. Выделяются 2 вида электронной подписи:
   a. ослабленная и сложная
   b. простая и сложная
   c. ослабленная и усиленная
   d. простая и усиленная
6. Основной функцией ФСТЭК являются:
   a. проведение единой технической политики и координация работ по защите информации
   b. организация и контроль над проведением работ по защите информации в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от НСД к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения
   c. поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации

d. поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в предоставлении общего доступа к персональным данным любого человека

7. В настоящее время рассматривается достаточно обширный перечень угроз ИБ АС, насчитывающий сотни пунктов. К наиболее характерным и часто реализуемым не относится:

a. несанкционированное копирование с носителей информации
b. использование разных носителей информации
c. неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной
d. игнорирование установленных правил при определении ранга системы

8. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и ни кто другой:

a. Конфиденциальность
b. Целостность
c. Доступность
d. Аутентичность
e. Аппелируемость

Лабораторные работы

Типовые задания для выполнения лабораторных работ

Перечень заданий работу для оценки уровня сформированности компетенции **ПК-4** на этапе «Умения»

Лабораторная работа №1

Сетевая защита с помощью межсетевого экрана

Цель работы: получение практических навыков настройки межсетевых экранов.

Задачи работы:

1. Научиться настраивать общие политики безопасности межсетевого экрана

2. Научиться создавать новые правила фильтрации сетевого трафика. 3. Научиться определять правила фильтрации, необходимые для решения поставленных задач.

Обеспечивающие средства: компьютер с установленной операционной системой Windows XP/2000, программа Agnitum Outpost Firewall Pro, методика создания правил фильтрации.

Вводная информация Сетевую защиту с помощью межсетевого экрана будем изучать на примере программы Agnitum Outpost Firewall Pro.

Политика фильтрации пакетов по умолчанию устанавливается выбором команды меню Параметры/ Политики.

Новые правила добавляются командой меню Параметры/Системные, раздел Общие правила (кнопка Параметры).

Чтобы добавить новое правило, нужно нажать кнопку Добавить. При добавлении правила нужно задать информацию во всех разделах окна Правило:

выбрать событие, по которому устанавливается правило,

выбрать действие, которое производится

задать имя нового правила

При выборе события для правила щелчком мыши отмечаем выбранную позицию (Где направление, Где протокол, Где удаленный порт). В поле Описание правила после этого появится надпись Не определено.

Каждый из основных протоколов TCP и IP имеют свой список портов. При выборе протокола TCP порт (или соответствующий протокол) нужно выбирать, отметив флажком позицию «Где удаленный порт». При выборе протокола IP позиция «Где удаленный порт» блокирована, и нужный порт/протокол выбирается при щелчке мышью на надписи Не определено после слов IP-протокол

Настройка параметров подключаемых модулей (DNS, детектора атак, фильтрации почтовых вложений и остальных) производится при выборе соответствующей позиции в меню кнопки Параметры

Журнал событий выводится в правой панели программы при нажатии кнопки Показать журнал. Предварительно в левой панели нужно выбрать раздел, по которому мы хотим посмотреть журнал событий (Сетевая активность, Открытые порты, Разрешенные, Заблокированные)

Задание к лабораторной работе

Вариант 1 Настроить политику брандмауэра по умолчанию «что не разрешено, то запрещено». Настроить разрешающие правила таким образом, чтобы: Дать возможность пользователю работать в Интернете по протоколам HTTP и FTP Обеспечить возможность прохождения электронной почты в обоих направлениях Обеспечить возможность работы утилит PING, TRACERT

Вариант 2 Настроить политику брандмауэра по умолчанию «что не запрещено, то разрешено». Настроить запрещающие правила таким образом, чтобы: Полностью запретить связь по протоколу Telnet Установить защиту от атак SYN flood, UDP flood Запретить прием сообщений протокола ICMP, направленных на широковещательные адреса

Для протокола ICMP запретить эхо-запрос и перенаправление данных. Для протокола IP запретить работу по протоколу групповой рассылки IGMP

2. Настроить включение кэширования DNS, ограничить кэш 50 записями.

3. Настроить детектор атак таким образом, чтобы на 10 минут блокировать атакующий хост в случае обнаружения атаки, и блокировать локальный хост в случае DoS атаки.

4. Настроить блокирование доступа к сайту narod.ru

5. Настроить фильтрацию почтовых вложений таким образом, чтобы выдавалось сообщение, если письмо содержит любое приложение.

6. Сохранить конфигурацию брандмауэра в файле .cfg. В отчете по лабораторной работе показать список последних 10 подключений, блокированных межсетевым экраном.

7. Показать настроенные правила преподавателю и защитить лабораторную работу.

8. По окончании работы удалить все созданные бригадой правила фильтрации и отключить брандмауэр (главное меню, Параметры/ Политики/ Отключить).

Перечень заданий работу для оценки уровня сформированности компетенции **ПК-4** на этапе «Владение навыками»

Лабораторная работа №2

Система обнаружения атак Snort

Цель работы: получение практических навыков работы с системой обнаружения атак Snort.

Задачи работы: 1. Изучить команды IDS Snort в режиме командной строки. 2. Изучить возможности графического интерфейса IDS Snort. 3. Научиться настраивать IDS Snort на обнаружение различных видов атак. 4. Научиться анализировать полученные предупреждения об атаках

Обеспечивающие средства: компьютер с установленной операционной системой Windows XP/2000, установленная программа Snort, описание системы команд IDS Snort.

Вводная информация IDS Snort – свободно распространяемая программа (www.snort.org). Snort может работать, как обычный анализатор сетевых пакетов, перехватывая все пакеты сетевого трафика. Чтобы Snort работал как система обнаружения атак, нужно настроить файл правил регистрации пакетов (по умолчанию Snort.conf). Тогда Snort будет регистрировать только те пакеты, которые соотвествуют правилам. Правила должны описывать признаки, по которым мы можем считать, что происходит атака. Таким признаком чаще всего является некоторая последовательность данных, которая должна быть обнаружена в сетевом пакете.

Инсталляция и запуск системы Для нормальной работы системы Snort необходима предварительная установка свободно распространяемой библиотеки WinPCap. По умолчанию система инсталлируется в каталог C:\Snort. Исполняемый модуль находится в C:\Snort\bin. Программа не имеет графического интерфейса, вся работа происходит в режиме командной строки. Общий формат команды Snort: Snort [-options] <filter options> Список опций можно посмотреть командой snort -?

Режимы работы программы Snort Программа работает в трех режимах: 1. Сниффинг – режим перехвата сетевого трафика (простого прослушивания сетевого адаптера) с выводом протокола на экран 2. Режим записи в файл – программа записывает перехваченный трафик в указанный файл 3. Режим обнаружения атак (Network Intrusion Detection Mode, NIDS) – режим анализа сетевого трафика в соответствии с составленными пользователем правилами.

Для запуска программы в режиме простого сниффинга нужно задать команду: Snort –v Для запуска программы в режиме записи в файл нужно задать команду с указанием имени каталога, в который будем помещать файлы с протоколом трафика: Snort –dev -l <имя каталога>

В указанном каталоге программа создаст отдельный файл протокола для каждого IPадреса, пакеты с которого будут перехвачены. Если указанного в команде каталога не существует, программа выдаст сообщение об ошибке.

Для запуска программы в режиме NIDS нужно задать команду с указанием выходного каталога и имени файла конфигурации, например: Snort –dev -l c:\temp -c c:\snort\etc\snort.conf Файл c:\snort\etc\snort.conf создается по умолчанию при установке системы, и содержит стандартный набор правил фильтрации. В указанном каталоге программа создаст отдельный файл для протоколов каждого IP-адреса, и общий файл предупреждений Alert.ids.

Задание к лабораторной работе

1. Запустить программу Snort в режиме снифера. Программа должна перехватывать весь трафик, направленный на ваш компьютер, и выводить протокол в указанный каталог. Команду на запуск программы и часть полученного протокола поместить в отчет по лабораторной работе.

2. Запустить программу Snort в режиме обнаружения атак с использованием стандартного файла конфигурации. Программа должна перехватывать весь трафик, направленный на ваш компьютер, и выводить протокол и предупреждения в указанный каталог.

3. Сделать анализ полученного протокола предупреждений. Команду на запуск программы и часть полученного протокола поместить в отчет по лабораторной работе. В отчете по лабораторной работе указать, какие виды нарушений безопасности или подозрительных действий обнаружены программой Snort.

4. Создать свой собственный файл конфигурации, в котором указать ссылку только на правила обнаружения сканирования вашего компьютера scan.rules. Запустить Snort с этим файлом конфигурации. На соседнем компьютере запустить сканер Superscan, сканирующий ваш компьютер. Правильно настроенный Snort должен обнаружить сканирование. Полученные предупреждения о сканировании должны быть приведены в отчете по лабораторной работе.

5. Создать свой собственный файл конфигурации, в котором указать ссылку только на правила обнаружения подозрительного ICMP-трафика icmp.rules. Проверить, предупреждает ли программа Snort об исследовании маршрута к вашему компьютеру с помощью утилиты traceroute.

Перечень вопросов к зачету

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.

10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Рейтинг-план дисциплины

7 семестр

№ п/п	Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
				Минимальный	Максимальный
Модуль 1.				**0**	**50**
Текущий контроль				**0**	**25**
1) Аудиторная работа на практических занятиях (устный опрос)		1	8	0	8
2) Выполнение самостоятельной работы		1	5	0	5
3) Выполнение лабораторных работ		6	2	0	12
Рубежный контроль				**0**	**25**
Контрольная работа №1.		5	5	0	25
Модуль 2.				**0**	**50**
Текущий контроль				**0**	**25**
1) Аудиторная работа на практических занятиях (устный опрос)		1	8	0	8
2) Выполнение самостоятельной работы		1	5	0	5
3) Выполнение лабораторных работ		6	2	0	12
Рубежный контроль				**0**	**25**
Контрольная работа №2		5	5	0	25
Итоговый контроль				**0**	**0**
зачет		0	0	0	0

Итого:			**0**	**100**
Поощрительные баллы				**10**
Участие в научной конференции	5	1	0	5
Публикация тезиса, статьи	5	1	0	5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	-6
Посещение практических занятий			0	-10

Объем и уровень сформированности компетенций целиком или на различных этапах у обучающихся оцениваются по результатам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80 - 100%; «удовлетворительно» – выполнено 40 - 80%; «неудовлетворительно» – выполнено 0 - 40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

$$\text{Рейтинговый балл} = k \times \text{Максимальный балл}$$

$$\text{Рейтинговыйбалл} = \text{k} \cdot \text{Максимальныйбалл},$$

где k = 0,2 при уровне освоения «неудовлетворительно», $\text{k} = 0{,}6$ k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов БашГУ:

На экзамене и зачете с оценкой выставляется оценка:
- отлично - при накоплении от 80 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
- хорошо - при накоплении от 60 до 79 рейтинговых баллов,
- удовлетворительно - при накоплении от 45 до 59 рейтинговых баллов,
- неудовлетворительно - при накоплении менее 45 рейтинговых баллов.

На зачете выставляется оценка:
- зачтено - при накоплении от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
- не зачтено - при накоплении от 0 до 59 рейтинговых баллов.

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

$$\text{Рейтинговый балл} = k \times \text{Максимальный балл},$$

где $k = 0{,}2$ при уровне освоения «неудовлетворительно», $k = 0{,}4$ при уровне освоения «удовлетворительно», $k = 0{,}8$ при уровне освоения «хорошо» и $k = 1$ при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов УУНиТ:
На зачете выставляется оценка:

• зачтено - при накоплении от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

• не зачтено - при накоплении от 0 до 59 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.