Федеральное государственное автономное образовательное учреждение высшего образования
"Национальный исследовательский университет "Высшая школа экономики"

МИЭМ
Департамент прикладной математики

Рабочая программа дисциплины
Системы обнаружения атак

для образовательной программы 10.05.01 «Компьютерная безопасность»
направления подготовки 10.05.01 «Компьютерная безопасность»
специалитет

Разработчики программы:
Лось Алексей Борисович, к.т.н., доцент, e-mail: alos@hse.ru
Сорокин Александр Владимирович, asorokin@hse.ru

Одобрена на заседании Кафедры компьютерной безопасности «28» августа 2017 г.

Зав. Кафедрой А. Б. Лось _____

Рекомендована Академическим советом образовательной программы
«28» августа 2017 г., № протокола 6

Утверждена «28» августа 2017 г.
Академический руководитель образовательной программы
А. Б. Лось _____

Москва, 2017

1 Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает минимальные требования к знаниям и умениям студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и студентов специальности 10.05.01 «Компьютерная безопасность», обучающихся по специализации Математические методы защиты информации, изучающих дисциплину Системы обнаружения атак.

Программа разработана в соответствии с:

- ОС ВО НИУ ВШЭ по специальности 10.05.01. «Компьютерная безопасность»;
- Образовательной программой специальности 10.05.01 «Компьютерная безопасность»;
- Рабочим учебным планом университета по специальности 10.05.01. «Компьютерная безопасность», утвержденным в 2017 г.

2 Цели освоения дисциплины

Целью освоения дисциплины Системы обнаружения атак является формирование у студентов следующих навыков, необходимых для решения предусмотренных программой специальности 10.05.01. "Компьютерная безопасность" профессиональных задач:

- Сбор и анализ исходных данных для проектирования систем защиты информации;
- Разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием;
- Применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
- Проведение инструментального мониторинга защищенности компьютерных систем;
- Поиск рациональных решений при разработке средств защиты информации с учетом требований качества, надежности и стоимости, а также сроков исполнения;
- Установка, настройка, эксплуатация и обслуживание аппаратно-программных средств защиты информации;
- Обеспечение эффективного функционирования средств защиты информации с учетом требований по обеспечению защищенности компьютерной системы.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

Знать:

- Уязвимости традиционных средств зашиты информации;
- Принципы организации и проведения копьютерных атак злоумышленниками;
- Классы систем обнаружения атак и их назначение;
- Принципы размещения узлов систем обнаружения атак;
- Реальные возможности систем обнаружения атак;
- Свойства систем обнаружения атак, имеющие значение при выборе конкретного продукта.

Уметь:

- Определять наиболее вероятные атаки в защищаемой системе;
- Выбирать наиболее подходящий класс или классы систем обнаружения атак для защищаемой системы;
- Выбирать конкретный продукт для защиты информационной системы.

- Оценивать качество работы системы обнаружения атак.

Иметь навыки (приобрести опыт):

- Инструментальной проверки системы на наличие уязвимостей;
- Развертывания и начальной настройки системы обнаружения атак;
- Администрирования системы обнаружения атак.

В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код по Код по ОС/ЕК	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
Способность работать с программными средствами общего и специального назначения, учитывая современные тенденции развития вычислительной техники и информационных технологий	ПК-10/ ИК-С4	РБ Знает основные принципы развертывания и эксплуатации систем обнаружения атак СД Способен установить и использовать для обнаружения сетевых атак СОА Snort и Suricata, программное средство WireShark Способен осуществлять настройку и написание собственных правил для СОА Snort и Suricata	Лабораторный практикум
Способность обеспечивать защиту информации в компьютерных сетях	ПК-17/ ИК-С11	РБ Знает принципы обнаружения компьютерных атак при помощи сетевых СОА Знает признаки атак, осуществляемых в компьютерных сетях Знает уязвимости периметровых средств защиты компьютерных сетей СД Способен осуществлять установку и анстройку сетевых СОА Snort и Suricata Способен использовать специализированное ПО для контроля параметров сетевых пакетов, обнаружения аномалий и признаков компьютерных атак	Все виды занятий по дисциплине
Способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем	ПК-21/ ИК-С15	РБ Знает основные уязвимости традиционных средств защиты информации Знает основные признаки компьютерных атак СД Способен оценить возможность нарушителя по реализации компьютерных атак в конкретной компьютенной системе Способен оценить достаточность мер по защите информации	Лекционные занятия

Компетенция	Код по Код по ОС/ЕК	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции
		Способен оценить необходимость использования СОА для обеспечения защищенности компьютерной системы Способен осуществить выбор необходимых параметров СОА для конкретной компьютерной системы Способен оценить правильность выбора и размещения СОА в проекте защиты компьютерной системы от компьютерных атак МЦ Способен обосновать важность СОА в системе защиты информации Способен обосновать недостаточность защиты компьютерной системы при использовании только традиционных средств защиты информации	
Способность проводить инструментальный мониторинг технической защиты информации и инструментальный мониторинг защиты от атак в компьютерных системах	ПК-23/ ИК-С17	РБ Знает принципы оценки защищенности компьютерных систем Знает принципы использования систем анализа защищенности и систем поиска уязвимостей СД Умеет использовать инструментальные средства поиска уязвимостей и анализа защищенности МЦ Спсобено обосновать важность регулярного применения СОА категории средств анализа защищенности для предотвращения возможных компьютерных атак	Лекционные занятия и лабораторный практикум
Способность осуществлять эксплуатацию (производить установку, наладку, тестирование и обслуживание) прикладных программных и программно-аппаратных средств и современного общего и специального программного обеспечения	ПК-26/ ИК-С20	РБ Знает основные принципы развертывания и эксплуатации систем обнаружения атак СД Способен установить и использовать для обнаружения сетевых атак СОА Snort и Suricata, программное средство WireShark Способен осуществлять настройку и написание собственных правил для СОА Snort и Suricata	Лабораторный практикум

4 Место дисциплины в структуре образовательной программы

Дисциплина «Системы обнаружения атак» относится к числу дисциплин вариативной части профессионального цикла.

Изучение данной дисциплины базируется на следующих дисциплинах:

- Языки программирования;
- Операционные системы;
- Сети и системы передачи информации;
- Основы информационной безопасности;

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями и компетенциями:

- Знание принципов разработки программного обеспечения;
- Знание протоколов передачи данных различных уровней системы OSI;
- Знание основных принципов построения компьютерных сетей и работы сетевого оборудования;
- Знание традиционных средств защиты информации – межсетевых экранов и системы разграничения прав доступа с системой идентификации и аутентификации.

Основные положения дисциплины могут быть использованы в дальнейшем при:

- Прохождении преддипломной практики;
- Выполнении выпускной квалификационной работы.

5 Тематический план учебной дисциплины

№	Название раздела	Всего часов	Аудиторные часы			Самостоятельная работа
			Лекции	Семинары	Практические занятия	
1.	Уязвимости традиционных средств защиты	8	2			4
2.	Анатомия атаки, этапы осуществления атаки	12	4			8
3.	Задача обнаружения атак	8	2			6
4.	Основные принципы обнаружения атак	10	4			6
5.	Обнаружение следов атак	8	2			6
6.	Классификация систем обнаружения атак	10	4			6
7.	Выбор системы обнаружения атак	10	2			8
8.	Размещение системы обнаружения атак	10	2			8
9.	Методы развертывания и эксплуатации систем обнаружения атак	50	14		36	20

6 Формы контроля знаний студентов

Тип контроля	Форма контроля	1 год				Параметры
		1	2	3	4	
Текущий (неделя)	Контрольная работа					Письменные работы по 20 минут
Текущий (неделя)	Домашнее задание		4			Задание на самостоятельный анализ сетевого трафика
Промежуточный	Экзамен		+			Устный теоретический экзамен
Итоговый	Экзамен				+	Устный теоретический экзамен

6.1 Критерии оценки знаний, навыков

На текущем контроле знаний в объеме изученного материала, студент должен продемонстрировать знание основных принципов обнаружения атак, методов построения автоматизированных систем обнаружения атак, принципы работы с такими системами.

При выполнении контрольной работы в форме небольших (20 минут) работ, составляющих части общей контрольной работы, студент должен продемонстрировать:

- Знание уязвимостей межсетевого экрана и системы идентификации и авторизации пользователей;
- Знание основных этапов проведения атак злоумышленниками;
- Знание основных принципов обнаружения готовящихся, осуществляемых и уже совершенных компьютерных атак.

Домашнее задание выдается на 4 недеде второго модуля и представляет собой подготовленый вариант, включающий набор записей журнала регистрации, регистрирующих движение сетевых пакетов в компьютерной сети. Студентам предлагается на основе изученного материала обнаружить в предложенных записях признаки компьютерных атак, сделать предположения о характере действий нарушителя, определить его параметры.

На промежуточном и итоговом контроле знаний студент должен продемонстрировать знания:

- Принципов построения систем обнаружения атак – их задач и возможностей;
- Классификацию систем обнаружения атак, особенности и назначение различных классов таких систем;
- Принципы выбора, размещения в защищаемой системе и развертывания систем обнаружения атак различных классов.
- Различия в уровне защищенности при использовании различных систем обнаружения атак и комплексов из них.

Экзамены проводятся в виде устного опроса преподавателем по вопросам билета и прочим вопросам, вынесенным на экзамен. Список вопросов, выносимых на экзамен, выдается преподавателем не позднее окончания 7 недели 2 модуля и 9 недели 4 модуля, причем в случае, если какой-либо вопрос или вопросы не были изучены в ходе лекций или лабораторных работ, он обязан быть исключен из списка вопросов, выносимых на экзамен. На итоговом экзамене к теоретическим вопросам добавляются вопросы, касающиеся практической части курса.

На промежуточном экзамене билет содержит 3 вопроса, относящихся ко всем разделам изучаемой дисциплины. Преподаватель, принимающий экзамен, оценивает ответ на каждый из

вопросов оценкой от 0 до 3 баллов. В этом случае оценки означают: 0 – ответ отсутствует или ответ свидетельствует о том, что соответствующий раздел дисциплины студентом не освоен, 1 – ответ студента свидетельствует об удовлетворительном освоении соответствующего раздела дисциплины, 2 – ответ студента свидетельствует о качественном освоении им соответствующего раздела дисциплины, 3 – ответ студента свидетельствует об отличном освоении им соответствующего раздела дисциплины, понимании материала, свободном владении им. Для уточнения оценки за ответ по конкретному вопросу преподаватель может задавать студенту дополнительные вопросы из списка вопросов, выносимых на экзамен, относящихся к тому же разделу изучаемой дисциплины, либо оценить уровень подготовки студента по конретному вопросу билета, предложив 3 кратких и конкретных вопроса по вопросу билета, оценивая верный ответ на каждый из них 1 баллом, в результате чего студент имеет возможность получить за ответ на вопрос билета также от 0 до 3 баллов. Таким образом, оценка студента за ответ на вопросы билета может составить от 0 до 9 баллов. К данному результату студента, приступившего к ответу на вопросы билета, прибавляется 1 балл, так что итоговая оценка за экзамен составляет от 1 до 10 баллов. Оценка «0» выставляется при нарушении студентом норм академической этики либо в случае, если студент отказался от ответа после взятия билета.

На итоговом экзамене билет содержит 3 вопроса, относящихся ко всем разделам изучаемой дисциплины. Преподаватель, принимающий экзамен, оценивает ответ на каждый из вопросов оценкой от 0 до 2 баллов. В этом случае оценки означают: 0 – ответ отсутствует или ответ свидетельствует о том, что соответствующий раздел дисциплины студентом не освоен, 1 – ответ студента свидетельствует об удовлетворительном или хорошем освоении соответствующего раздела дисциплины, 2 – ответ студента свидетельствует об отличном освоении им соответствующего раздела дисциплины, понимании материала, свободном владении им. Для уточнения оценки за ответ по конкретному вопросу преподаватель может задавать студенту дополнительные вопросы из списка вопросов, выносимых на экзамен, относящихся к тому же разделу изучаемой дисциплины либо оценить уровень подготовки студента по конретному вопросу билета, предложив 2 кратких и конкретных вопроса по вопросу билета, оценивая верный ответ на каждый из них 1 баллом, в результате чего студент имеет возможность получить за ответ на вопрос билета также от 0 до 2 баллов. Таким образом, оценка студента за ответ на вопросы билета может составить от 0 до 6 баллов. После этого студенту задается 4 дополнительных вопроса по материалам лаботарторных работ 2 полугодия (3 и 4 модули), каждый из которых оценивается в 0 или 1 балл, где 1 – полностью верный, аргументированный ответ, 0 – в ином случае (как правило, вопросы не предполагают частично верного ответа). Итоговая оценка за экзамен определяется простым суммированием оценок за все вопросы и составляет 0 – 10 баллов Студент, по любой причине не приступивший к выполнению заданий экзамена, получает за экзамен оценку 0 баллов.

7 Содержание дисциплины

Разделы	**Темы**	
1		Уязвимости традиционных средств защиты
	1.1	Уязвимости стека протоколов TCP/IP
	1.2	Слабости МЭ, и способы его обхода
	1.3	Уязвимости системы аутентификации и авторизации
2.		Анатомия атаки, этапы осуществления атаки
	2.1	Классификация уязвимостей
	2.2	Модель атаки
	2.3	Этапы реализации атаки
	2.4	Классификация атак
3		Задача обнаружения атак
	3.1	Понятие системы обнаружения атак
	3.2	Реальные возможности систем обнаружени атак и пределы их возможностей

	3.3	Схема работы системы обнаружения атак
4		Основные принципы обнаружения атак
	4.1	Признаки атак
	4.2	Источники информации об атаках
	4.3	Технологии и подходы к обнаружению атак
5		Обнаружение следов атак
	5.1	Контроль изменений файлов
	5.2	Анализ журналов регистрации
	5.3	Анализ сетевого трафика
6		Классификация систем обнаружени атак
	6.1	Системы анализа защищенности
	6.2	Анализаторы журналов регистрации
	6.3	Обманные системы
	6.4	Системы контроля целостности
7		Выбор системы обнаружения атак
	7.1	Предварительный анализ
	7.2	Критерии оценки
	7.3	Тестирование
8		Размещение системы обнаружения атак
	8.1	Размещение сенсоров
	8.2	Использование сетевых сенсоров коммутируемых сетях
	8.3	Размещение системы анализа защищенности
		Размещение системы контроля целостности
		Системы виртуальных ловушек (Honey Pot и Padded Cell)
9		Методы развертывания и эксплуатации СОА
	9.1	Общие проблемы
	9.2	Сетевые системы
	9.3	Узловые системы
	9.4	Практикум по работе с СОА Snort и Suricata

8 Образовательные технологии

Для проведения практических занятий применяется дисплейных класс с компьютерами под управлением ОС семейств Windows и Linux, установочные пакеты сетевой СОА Snort, СОА Suricata и сетевого анализатора WireShark. Установка и настройка указанных программ проводится студентами в рамках работ лабораторного практикума.

9 Порядок формирования оценок по дисциплине

Преподаватель оценивает работу студентов на различнх формах текущего контроля (1 и 2 модули) и лабораторных работах (3 и 4 модули): оценивается выолнение заданий, выдаваемых для аудиторного выполнения (контрольная работа) $O_{к/р.}$ и домашнего задания $O_{д.з..}$. Оценка за контрольную работу $O_{к/р.}$ вычисляется как среднее арифметическое 4 работ, проводимых на занятиях 1 и 2 модулей. Во втором полугодии (3 и 4 модули) оценивается выполнение работ из лабораторного практикума. По окончании 2 и 4 модуля определяется накопленная оценка, которая объявляется студентам и применяется при определении оценок промежуточного и итогового контроля. По окончании 4 модуля также определяется оценка за лабораторные работы - $O_{лаб.\ работы}$.

Оценка за лабораторные работы определяется как среднее арифметическое оценок за все лабораторные работы модуля. Работы, не выполнявшиеся и/или не сдававшиеся студентом включаются в расчет $O_{лаб.\ работы}$ с оценкой «0», способ округления – арифметический (с недостатком при значениях первой цифры дробной части от «0» до «4» и с избытком при значениях первой цифры дробной части от «5» до «9»).

Накопленная оценка 1 полугодия $O_{накопленная1}$, исполтьзуемая для вычисления промежуточной оценки по дисциплине, определяется как взвешенная сумма оценок за контрольную работу и домашнее задание ($\boldsymbol{O_{к/р.}}$ и $\boldsymbol{O_{д.з.}}$ соответственно):

$$O_{накопленная1} = 0{,}7 \cdot O_{к/р} + 0{,}3 \cdot O_{д/з}$$

Способ округления накопленной оценки: арифметический.

Итоговая оценка промежуточного контроля рассчитывается по формуле:

$$O_{промежуточная} = 0{,}6 * O_{накопленная1} + 0{,}4 *\cdot O_{экзамен}$$

Во 2 полугодии накопленная оценка $O_{накопленная\ 2}$ равна оценке за лабораторные работы.

Результирующая оценка итогового контроля $O_{итоговая}$ рассчитывается следующим образом:

$$O_{итоговая} = 0{,}7 * O_{накопленная} + 0{,}3 *\cdot O_{экзамен}$$

Способ округления результирующей оценки итогового контроля в форме экзамена: арифметический.

Итоговая оценка за дисциплину равна результирующей оценке итогового контроля.

На экзамене или пересдаче студенту не предоставляется возможность получить дополнительный балл для компенсации оценки за текущий контроль.

На экзамене студент, по уважительной причине не выполнявший контрольную работу, при условии, что им выполнено домашнее задание, а написание контрольной работы на оценку 6 баллов приводит к тому, что накопленная оценка становится не ниже 8 баллов, может получить право выполнить все ее части во время экзамена, при этом о таком намерении он обязан сообщить преподавателю до взятия билета. В этом случае студенту выдается вариант контрольной работы вместо экзаменационного билета и он приступает к выполнению контрольной работы. В случае выполнения работы на оценку 6 и более баллов, студент, с его согласия, может быть освобожден от экзамена, при этом его накопленная оценка пересчитывается с учетом

оценки за контрольную работу, ему выставляется результирующая оценка за экзамен, равная накопленной оценке.

10 Учебно-методическое и информационное обеспечение дисциплины

10.1 Основная литература

1. Шелухин О.И., Сакалема Д.Ж., А.С. Филинова, Обнаружение вторжений в компьютерные сети, М., Горячая линия – Телеком, 2013, 220 с.
2. Лукацкий А.В. Обнаружение атак. — СПб: БХВ-Петербург, 2003. — 596 с.
3. Лукацкий А. В. Атака из Internet. — М.: Издательство СОЛОН - Р, 2002. — 368 стр.
4. Польман Н., Кразерс Т. Архитектура брандмауэров для сетей предприятия. — М.: Вильямс, 2003. — 432 стр.
5. Столингс В. Компьютерные сети, протоколы и технологии Интернета. — СПб: Издательство: БХВ-Петербург, 2005. — 832 стр.
6. Таненбаум Э. Компьютерные сети. — СПб: Издательство: Питер, 2003. — 992 стр.

10.2 Дополнительная литература

1. Галатенко В. А. Стандарты информационной безопасности. Курс лекций. — М.: Издательство: Интернет-университет информационных технологий, 2004. — 328 стр.
2. Норткатт С., Новак Дж., Маклахлен Д. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу. — М: Издательство “Лори”, 2001. — 384 с.

11 Материально-техническое обеспечение дисциплины

При проведении отдельных семинарских занятий используется дисплейных класс с компьютерами под управлением ОС семейств Windows и Linux, установочные пакеты сетевой СОА Snort, СОА Suricata и сетевого анализатора WireShark.

12 Примерный перечень вопросов к экзаменам:

1. Уязвимости стека протоколов TCP/IP
2. Уязвимости межсетевого экрана и методы его обхода нарушителем
3. Уязвимости системы разграничения доступа
4. Классификация уязвимостей автоматизированных систем
5. Этапы реализации атак на автоматизированные системы
6. Модели атак на автоматизированные системы
7. Основные классы атак на автоматизированные системы
8. Принципы поиска следов атак в автоматизированной системе
9. Контроль изменений файлов автоматизированной системы
10. Анализ журналов регистрации автоматизированной системы
11. Анализ сетевого трафика автоматизированной системы
12. Анализ процессов, сервисов и портов автоматизированной системы
13. Задачи, решаемые системами обнаружения атак
14. Ожидаемые и фактические возможности систем обнаружения атак
15. Признаки атак на автоматизированную систему

16. Принципы обнаружения атак
17. Классификация систем обнаружения атак
18. Системы анализа защищенности
19. Системы обнаружения вторжений
20. Системы обнаружения реализованных атак
21. Обманные системы
22. Критерии выбора системы обнаружения атак
23. Критерии оценки системы обнаружения атак
24. Аспекты размещения системы обнаружения атак в защищаемой системе
25. Размещение сенсоров системы обнаружения атак
26. Размещение систем анализа защищенности и обманных систем
27. Последовательность действий при развертывании системы обнаружения атак
28. Основные принципы работы сетевой системы обнаружения атак Snort
29. Основные принципы работы системы обнаружения атак Suricata