Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

В. В. Подтопельный

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности
10.05.03 «Информационная безопасность
автоматизированных систем», специализация
«Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 004.056(076)

Рецензент
кандидат физико-математических наук, доцент, доцент кафедры информационной безопасности института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет»
Н. Я. Великите

Подтопельный, В. В.
Информационная безопасность открытых информационных систем: учебно-методическое пособие по изучению дисциплины для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем». – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2025. – 47 с.

Учебно-методическое пособие включает в себя рассмотрение теоретических вопросов в области защиты информации по дисциплине «Информационная безопасность открытых информационных систем». В учебно-методическом пособии приведен тематический план изучения дисциплины. Представлены методические указания по изучению дисциплины. Даны рекомендации по подготовке к промежуточной аттестации в форме зачёта и экзамена, по выполнению самостоятельной работы. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы модуля. Пособие предназначено для студентов 5-го курса специальности 10.05.03 «Информационная безопасность автоматизированных систем».
Табл. 2, список лит. – 14 наименований

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 26 мая 2025 г., протокол № 4

УДК 004.056(076)

ОГЛАВЛЕНИЕ

Введение…….....….....4
1. Тематический план……..…….....…….....……....6
2. Содержание дисциплины и указания к изучению……..…8
3. Методические рекомендации по подготовке к лабораторным занятиям……36
4. Методические указания по самостоятельной работе ……37
5. Требования к аттестации по дисциплине…….……...40
Заключение…….....……...…….....….....44
Список литературы…….....……....….....44

ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем», изучающих дисциплину «Информационная безопасность открытых информационных систем».

Целью освоения дисциплины «Информационная безопасность открытых информационных систем» является: выявление уязвимостей и угроз безопасности, их нейтрализацию в открытых информационных системах (в их программном обеспечении, аппаратных средствах, средствах связи), в том числе при взаимодействии с удаленными системами, разработку и внедрение открытых систем в защищенном исполнении, а также средств защиты для них, обеспечение контроля и управления установленными средствами защиты информации.

Компетенции:

– ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации:

– ОПК-5.1. Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;

– ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем.

В результате освоения дисциплины обучающийся должен:

знать:

– общие принципы построения открытых систем в защищенном исполнении;

– особенности политики безопасности и способы ее внедрения на предприятии;

– основные этапы процесса проектирования и методы, используемые при построении проектируемой системы и способы нарушения информационной безопасности при работе автоматизированных систем обработки информации;

уметь:

– выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем (открытых ИС) обработки информации и описывать их с учетом методических рекомендаций регуляторов в области защиты информации;

– выявлять известные уязвимости открытых информационных систем;

владеть:

– навыком формирования перечня мероприятий по предотвращению угроз безопасности информации автоматизированных систем (открытых ИС);

– навыком разработки модели угроз безопасности информации и нарушителей в автоматизированных системах.

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествуют «Безопасность вычислительных сетей», «Безопасность систем баз данных», «Безопасность операционных систем.

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных лабораторных работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины, возможно, вам потребует больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе Содержание дисциплины приведены подробные сведения об изучаемых вопросах по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету и/или экзамену.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

Программное обеспечение

Программное обеспечение, распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU, по которой автор передаёт программное обеспечение в общественную собственность):

– Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом);
– Ethereal (Программы перехвата и анализа сетевых пакетов);
– NMAP (Программа сканирование сетевых ресурсов);
– MySQL (Система управления базами данных).

Типовое ПО на всех ПК:

1. Операционная система Windows 10 (получаемая по программе Microsoft «Open Value Subscription»).
2. Офисное приложение MS Office Standard 2016 (получаемое по программе Microsoft «Open Value Subscription»).
3. Операционная система Astra Linux SE.
4. Офисное приложение LibreOffice.
5. Google Chrome (GNU).
6. Oracle VM VirtualBox (GNU/Linux, macOS и Windows).

1. ТЕМАТИЧЕСКИЙ ПЛАН

Таблица 1 – Тематический план

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
Лекции (А семестр -32 ч ауд.)				
1.1	Сетевые угрозы	Тема 1.1 Ошибки в программном обеспечении	8	
1.2	Сетевые угрозы	Тема 1.2 Типичные сценарии и уровни атак	8	25
1.3	Сетевые угрозы	Тема 1.3 Сканирование карты сети. Атаки уровней OSI	8	25
1.4	Сетевые угрозы	Тема 1.4 Распределенные атаки «отказ в обслуживании»	8	23,85
Лекции (В семестр – 40 ч ауд.)				
2.1	Защита от сетевых угроз	Тема 2.1 Методы отражения вторжений	6	10
2.2	Защита от сетевых угроз	Тема 2.2 Классификация методов отражения вторжений	6	10
2.3	Защита от сетевых угроз	Тема 2.3 Политика безопасности интернет-сети	6	10
2.4	Защита от сетевых угроз	Тема 2.4 Системы обнаружения вторжений и межсетевые экраны	6	10
2.5	Защита от сетевых угроз	Тема 2.5 Классификация систем обнаружения вторжений.	6	10
2.6	Защита от сетевых угроз	Тема 2.6 Размещение сетевых систем обнаружения вторжений	6	10
2.7	Защита от сетевых угроз	Тема 2.7 Порядок реагирования на вторжения в интернет-сети и организационно-правовые вопросы	4	32
			72	**165,85**
	Лабораторные занятия (А семестр – 32 ч ауд.)			
Сетевые угрозы		Изучение трафика	8	-

Сетевые угрозы	Nmap-сканирование	8	-
Сетевые угрозы	Аудит сетевой инфраструктуры средствами PowerShell	8	-
Сетевые угрозы	Работа с препроцессорами (preprocessor) Snort	8	-
Лабораторные занятия (В семестр – 40 ч. ауд.)			
Защита от сетевых угроз	Сигнатурный анализ и обнаружение аномалий	8	-
Защита от сетевых угроз	Аудит информационной безопасности веб-приложений	8	-
Защита от сетевых угроз	OSSEC HIDS	8	-
Защита от сетевых угроз	Настройка работы IPsec	8	-
Защита от сетевых угроз	Программное логирование сетевых пакетов в файл	8	-
	Всего за семестр:	**72**	**-**

Курсовая работа (проект)		
Контрольная точка 1. Раздел проекта 1	-	-
Контрольная точка 2. Раздел проекта 2	-	-
Оформление проекта. Защита	-	-
	0	**0**

РЭ - 14
КА - 1,4

Рубежный (текущий) и итоговый контроль		
Контроль 1 (не предусмотрен)	-	-
Контроль 2 (не предусмотрен)	34,75	-
Итоговый контроль (зачет)		
Итоговый контроль (экзамен)		
	0	**0**

Всего	**178,75**	**165,85**

ИТОГО

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

Раздел 1. Сетевые угрозы
Тема 1.1 Введение. Ошибки в программном обеспечении

Перечень изучаемых вопросов

1. Ошибки в программном обеспечении.
2. Уязвимости системных утилит, команд и сетевых служб.
3. Перехват паролей.
4. Перехват незащищенного трафика.
5. Конфигурация системы.

Методические указания к изучению

Открытые информационные системы, обладая высокой степенью доступности и интеграции, сталкиваются с повышенными рисками нарушения конфиденциальности, целостности и доступности данных. Одним из ключевых аспектов изучения информационной безопасности таких систем является анализ ошибок в программном обеспечении (ПО), которые могут стать катализатором уязвимостей.

1. Ошибки в программном обеспечении

Ошибки в программном коде – распространённая причина утечек данных и несанкционированного доступа. Они возникают из-за человеческого фактора, несовершенства процессов разработки или недостаточного тестирования. Например, переполнение буфера, некорректная обработка исключений или логические ошибки в алгоритмах способны открыть злоумышленникам доступ к критическим компонентам системы. Такие ошибки часто эксплуатируются через вредоносные скрипты или внедрение кода.

2. Уязвимости системных утилит, команд и сетевых служб

Стандартные системные утилиты и сетевые службы, даже будучи частью доверенного ПО, могут содержать скрытые уязвимости. Например, неправильная обработка входных данных в утилитах командной строки или ошибки в настройках сетевых демонов (таких как SSH или HTTP-серверы) позволяют злоумышленникам выполнять произвольные команды или получать доступ к закрытым разделам системы. Анализ логов и своевременное обновление ПО – ключевые меры для минимизации таких рисков.

3. Перехват паролей

Слабые механизмы аутентификации и хранения паролей делают системы уязвимыми к перехвату учетных данных. Злоумышленники используют методы фишинга, подбора паролей (брутфорс) или атаки «человек посередине» (MITM). Особую опасность представляют незашифрованные пароли, передаваемые по открытым каналам связи. Внедрение многофакторной аутентификации и использование хеширования с «солью» значительно повышают устойчивость системы.

4. Перехват незащищённого трафика

Данные, передаваемые без шифрования (HTTP, FTP), могут быть перехвачены и модифицированы. Например, злоумышленник, подключившийся к публичной Wi-Fi-сети, способен анализировать пакеты и извлекать конфиденциальную информацию. Решение этой проблемы – использование протоколов с шифрованием (HTTPS, SFTP) и VPN-технологий для защиты трафика.

5. Конфигурация системы

Некорректная настройка параметров безопасности – частая причина компрометации систем. Открытые порты, стандартные пароли, избыточные права доступа к файлам или сервисам создают лазейки для атак. Регулярный аудит конфигураций, применение принципа минимальных привилегий и использование инструментов автоматизации (например, Ansible для настройки серверов) помогают снизить риски.

Литература

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст: электронный (гл. 5).

2. Киренберг, Г. А._Информационная безопасность современных операционных систем: учеб. пособие / Киренберг, Г. А. – Кемерово: КузГТУ им. Т. Ф. Горбачева, 2022. – 138 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/295736 (дата обращения: 06.12.2024). – ISBN 978-5-00137-320-9. – Текст : электронный (гл. 1).

3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный (гл. 1, 4).

4. Епишкина, А. В. Нормативное регулирование в области защиты информации: Конспект лекций: учеб. пособие / А. В. Епишкина, С. В. За-печников. – Москва: НИЯУ МИФИ, 2021. – 116 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/284345 (дата обращения: 09.10.2024). – ISBN 978-5-7262-2807-5. – Текст : электронный (с. 15–28).

Контрольные вопросы

1. Приведите ошибки в программном обеспечении.
2. Приведите классификации программных средств защиты.
3. Охарактеризуйте классификации, категории ФСТЭК уязвимости системных утилит, команд и сетевых служб.

Тема 1.2 Сетевые угрозы

Перечень изучаемых вопросов

1. Типичные сценарии и уровни атак.
2. Методы, используемые нападающими для проникновения в интернет-сети.

Методические указания к изучению

Открытые информационные системы, интегрированные в глобальные сети, сталкиваются с многоуровневыми угрозами, требующими глубокого понимания как сценариев атак, так и технических методов их реализации. Анализ этих аспектов позволяет разрабатывать превентивные меры защиты и минимизировать риски компрометации данных.

1 Типичные сценарии и уровни атак

Атаки на открытые системы классифицируются по уровням модели взаимодействия (OSI) и целям воздействия. На физическом уровне злоумышленники могут перехватывать данные через незащищённые каналы связи. На сетевом уровне распространены DDoS-атаки, направленные на перегрузку каналов, и ARP-спуфинг для перенаправления трафика. На транспортном уровне эксплуатируются уязвимости протоколов (например, TCP SYN-флуд), а на прикладном – атаки на веб-приложения (SQL-инъекции, XSS). Фишинг и социальная инженерия направлены на человеческий фактор, обходя технические защиты.

Методические указания: изучите модель OSI, сопоставляя каждый уровень с конкретными типами атак. Проведите анализ кейсов (например, атака Mirai для понимания DDoS) и используйте симуляторы вроде GNS3 или CORE для визуализации сетевых угроз.

2. Методы, используемые для проникновения в интернет-сети

Злоумышленники комбинируют технические и психологические методы. К первым относятся:

A. **Эксплуатация уязвимостей ПО** – использование ошибок в коде для внедрения вредоносных скриптов или получения прав администратора.

B. **Сканирование и фингерпринтинг** – идентификация активных узлов, открытых портов и ПО для поиска слабых мест.

C. **Спуфинг и подмена данных** – маскировка под доверенные ресурсы (IP, DNS) для обхода систем аутентификации.

D. **Социальная инженерия** – манипуляции с целью получения паролей или доступа к системе (например, фишинговые письма). *Методические указания:* Освойте инструменты пентестинга (Metasploit, Burp Suite) в лабораторных условиях. Проведите практикум по созданию фишинговых сценариев (в этических рамках) для понимания тактик социальной инженерии.

Литература

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим

доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст : электронный (гл. 3, 16).

2. Киренберг, Г. А. Информационная безопасность современных операционных систем: учеб. пособие / Киренберг, Г. А. – Кемерово: КузГТУ им. Т. Ф. Горбачева, 2022. – 138 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/295736 (дата обращения: 06.12.2024). – ISBN 978-5-00137-320-9. – Текст : электронный (гл. 1).

Контрольные вопросы

1. Какие типы ошибок в программном обеспечении наиболее опасны для информационной безопасности и почему?
2. Приведите пример уязвимости в системной утилите, которая может привести к выполнению произвольного кода.
3. Как переполнение буфера влияет на безопасность открытых информационных систем?
4. Какие сетевые службы чаще всего становятся мишенью для атак из-за ошибок в их реализации?
5. Объясните, как атака «человек посередине» позволяет перехватить пароли.
6. Почему многофакторная аутентификация считается эффективным методом защиты от перехвата учетных данных?
7. Какие риски возникают при передаче данных через незащищённые протоколы (например, HTTP)?
8. Как технология VPN помогает предотвратить перехват трафика в открытых сетях?
9. Какие последствия могут возникнуть из-за некорректной настройки прав доступа к файлам на сервере?
10. Почему использование стандартных паролей в настройках системы считается критической уязвимостью?
11. Как регулярное обновление ПО способствует устранению уязвимостей в сетевых службах?
12. Опишите роль аудита конфигураций в поддержании безопасности информационной системы.

Тема 1.3 Сканирование карты сети. Атаки уровней OSI

Перечень изучаемых вопросов

1. Сканирование карты сети.
2. Нападения с использованием алгоритмов сетевых протоколов.
3. SYN-бомбардировка.
4. Спуфинг.

Методические указания к изучению

Требуется обратить внимание на:

Открытые информационные системы, функционирующие в распределённых сетях, подвержены угрозам, связанным с исследованием их структуры и эксплуатацией уязвимостей сетевых протоколов. Понимание методов сканирования сети и атак на различных уровнях модели OSI критически важно для построения устойчивой защиты.

1. Сканирование карты сети

Сканирование сети – процесс обнаружения активных устройств, сервисов и топологии сети. Злоумышленники используют инструменты вроде Nmap, Ping или Traceroute для идентификации узлов, открытых портов и операционных систем. Это позволяет определить точки входа для атак. Для защиты рекомендуется сегментировать сеть, настраивать межсетевые экраны и маскировать ответы на запросы (например, отключение ICMP-эхо).

Методические указания: Изучите базовые команды сетевого сканирования на практике, используя тестовые стенды. Анализируйте логи сканирования для выявления подозрительной активности.

2. Атаки с использованием алгоритмов сетевых протоколов

Сетевые протоколы, такие как ARP, DNS или ICMP, содержат алгоритмы, которые могут быть использованы для атак. Например, ARP-spoofing позволяет перенаправить трафик через устройство злоумышленника, а поддельные ICMP-пакеты – вызвать отказ в обслуживании. Уязвимости возникают из-за доверительных отношений между узлами или отсутствия проверки подлинности пакетов.

Методические указания: Разберитесь в механике работы протоколов на примере Wireshark. Настройте защитные механизмы: статические ARP-таблицы, DNSSEC или фильтрацию пакетов.

3. SYN-бомбардировка

SYN-флуд – атака на транспортный уровень (TCP), при которой злоумышленник отправляет множество SYN-запросов, переполняя очередь соединений сервера. Это приводит к отказу в обслуживании легитимных пользователей. Защита включает использование SYN cookies, ограничение числа одновременных подключений и настройку систем обнаружения вторжений (IDS).

Методические указания: Смоделируйте SYN-флуд в изолированной среде (например, с помощью hping3). Изучите реакцию IDS/IPS и методы восстановления сервиса.

4. Спуфинг

Спуфинг – подмена источника данных для обхода аутентификации. Распространённые виды: IP-спуфинг (подделка IP-адреса отправителя), DNS-спуфинг (фальсификация DNS-ответов) и MAC-спуфинг (изменение MAC-адреса). Атаки направлены на маскировку злоумышленника под доверенный объект. Противодействие включает использование криптографических протоколов (IPsec, HTTPS), мониторинг аномалий в трафике и фильтрацию пакетов на уровне сети.

Методические указания: Проведите лабораторную работу по обнаружению спуфинга с помощью анализа сетевого трафика. Настройте правила iptables для блокировки подозрительных пакетов.

Контрольные вопросы

1. Какие цели преследует злоумышленник при сканировании карты сети?
2. Объясните, как сегментация сети снижает риски, связанные с её сканированием.
3. Почему ARP-spoofing эффективен в локальных сетях и как его обнаружить?
4. Какие уязвимости протокола ICMP эксплуатируются в атаках типа Ping of Death?
5. Опишите механизм SYN-бомбардировки и её последствия для целевого сервера.
6. Как SYN cookies помогают mitigate SYN-флуд атаки?
7. Чем отличается IP-спуфинг от DNS-спуфинга? Приведите примеры сценариев их использования.
8. Какие методы защиты применяются против MAC-спуфинга в беспроводных сетях?
9. Почему спуфинг-атаки часто используются в сочетании с другими методами (например, MITM)?
10. Как инструменты вроде Wireshark помогают в обнаружении сетевых аномалий?
11. Какие настройки межсетевого экрана могут предотвратить спуфинг IP-адресов?
12. Объясните роль DNSSEC в противодействии DNS-спуфингу.

Литература

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст: электронный (гл. 3, 7, 16).

2. Киренберг, Г. А. Информационная безопасность современных операционных систем: учеб. пособие / Г. А. Киренберг. – Кемерово: КузГТУ им. Т. Ф. Горбачева, 2022. – 138 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/295736 (дата обращения: 06.12.2024). – ISBN 978-5-00137-320-9. – Текст : электронный (гл. 1).

3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-

библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный (гл. 2).

Тема 1.4 Сетевые угрозы

Перечень изучаемых вопросов

1. Распределенные атаки «отказ в обслуживании».
2. ARP-spoofing или ложный ARP-сервер.
3. IP Hijacking.
4. Нападения на основе протокола ICMP.

Методические указания к изучению

Открытые информационные системы, функционирующие в глобальных сетях, сталкиваются с разнообразными угрозами, способными нарушить их работоспособность, конфиденциальность и целостность. В рамках изучения сетевых угроз особое внимание уделяется атакам, эксплуатирующим фундаментальные механизмы сетевого взаимодействия. Ниже представлен детальный анализ ключевых угроз, их механизмов, последствий и методов противодействия, а также рекомендации для эффективного изучения темы.

1. Распределённые атаки типа «отказ в обслуживании» (DDoS)

Суть угрозы: DDoS-атаки направлены на перегрузку ресурсов целевой системы (серверов, сетевых каналов) путём координации атакующих запросов с множества устройств, объединённых в ботнет. Злоумышленники используют уязвимости протоколов (например, DNS amplification) или приложений для генерации аномального трафика. Пример: атака ботнета Mirai в 2016 году, которая парализовала сервисы Dyn, вызвав каскадный сбой крупных платформ, включая Twitter и Netflix.

- Технические аспекты:
- Виды DDoS:
  - Объёмные атаки (UDP/ICMP-флуд) – перегрузка канала связи.
  - Протокольные атаки (SYN-флуд, Ping of Death) – эксплуатация слабостей сетевых стеков.
  - Прикладные атаки (HTTP-флуд) – имитация легитимных запросов к веб-серверам.
- Источники: Ботнеты из IoT-устройств, серверов или ПК, заражённых вредоносным ПО.
- Методы защиты:
- Использование CDN (Content Delivery Network) для распределения нагрузки.
- Внедрение систем анализа трафика (например, Arbor Networks) для фильтрации аномальных пакетов.
- Настройка лимитов запросов и blackhole-маршрутизации.
- Методические указания:

- Создайте тестовый стенд с использованием виртуальных машин для симуляции DDoS через инструменты LOIC или hping3.
- Изучите кейс атаки на GitHub (2018), где трафик достиг 1.35 Тбит/с, и проанализируйте применённые методы смягчения.
- Освойте настройку Cloudflare или AWS Shield для защиты веб-приложений.

2. ARP-spoofing (ложный ARP-сервер)

Суть угрозы: ARP-spoofing – подмена MAC-адресов в ARP-таблицах сетевых устройств для перенаправления трафика через злоумышленника. Это позволяет перехватывать данные, проводить атаки "человек посередине" (MITM) или блокировать связь между узлами. Например, злоумышленник может перенаправить трафик жертвы через свой компьютер, перехватывая пароли или сессии.

Технические аспекты:

Механизм работы: Отправка поддельных ARP-ответов, связывающих IP-адрес жертвы с MAC-адресом атакующего.

Уязвимые среды: Локальные сети (LAN), где ARP-протокол не требует аутентификации.

Методы защиты:

- Внедрение статических ARP-таблиц на критических узлах.
- Использование протокола DHCP snooping для валидации DHCP-транзакций.
- Настройка инструментов обнаружения (Arpwatch, XArp).

Методические указания: проведите лабораторную работу с использованием Ettercap для перехвата трафика в локальной сети.

- Проанализируйте логи Wireshark для выявления аномальных ARP-пакетов.
- Настройте порты безопасности на коммутаторах (802.1X) для блокировки несанкционированных устройств.

3. IP Hijacking (перехват IP-трафика)

- Суть угрозы: IP Hijacking — манипуляция таблицами маршрутизации (чаще через протокол BGP) для перенаправления интернет-трафика через несанкционированные узлы. Например, в 2008 г. пакистанский провайдер случайно «захватил» IP-префиксы YouTube, вызвав глобальный сбой доступа к сервису.

Технические аспекты:

BGP-уязвимости: Отсутствие аутентификации в BGP-протоколе позволяет злоумышленникам рассылать ложные маршрутные объявления.

Цели: Шпионаж, цензура, перехват криптовалютных транзакций.

Методы защиты:

- Внедрение RPKI (Resource Public Key Infrastructure) для цифровой подписи маршрутов.
- Использование BGPsec – расширения BGP с криптографической аутентификацией.
- Фильтрация BGP-объявлений на уровне провайдеров.

Методические указания:

- Смоделируйте хайджек BGP в эмуляторе GNS3, изучив механизм распространения ложных маршрутов.
- Проанализируйте инцидент с Amazon Route 53 (2020), где ошибка маршрутизации вызвала сбой множества сервисов.

4. Нападения на основе протокола ICMP

Суть угрозы: ICMP (Internet Control Message Protocol) предназначен для диагностики сети, но часто используется в атаках. Примеры:

- Ping of Death – отправка фрагментированных ICMP-пакетов, вызывающих переполнение буфера.
- ICMP-флуд – генерация огромного числа запросов (ping) для перегрузки канала.
- ICMP-сканирование – выявление активных узлов и топологии сети.

Методы защиты:

- Отключение ответов на ICMP-запросы на критических серверах.
- Настройка межсетевых экранов для блокировки подозрительных ICMP-пакетов (например, больших или фрагментированных).
- Использование IDS/IPS для обнаружения аномальной ICMP-активности.

Методические указания:

- Создайте фрагментированные ICMP-пакеты с помощью Scapy и проанализируйте их влияние на целевую систему.
- Настройте iptables для фильтрации ICMP-трафика на Linux-сервере.

Литература

3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный (гл. 1, 4).

Контрольные вопросы

1. Объясните, как DNS amplification увеличивает масштаб DDoS-атаки. Приведите пример уязвимого протокола.
2. Какие особенности архитектуры IoT-устройств делают их идеальными целями для ботнетов в DDoS-атаках?
3. Опишите пошаговый механизм ARP-spoofing. Как злоумышленник перенаправляет трафик через своё устройство?
4. Какие признаки в сетевых логах могут указывать на ARP-spoofing?
5. Почему BGP считается ненадёжным протоколом с точки зрения безопасности? Какие решения предлагает RPKI?
6. Какие последствия для глобального интернета может иметь хайджек IP-префиксов крупного CDN-провайдера?
7. Чем отличается Ping of Death от ICMP-флуда? Как ОС защищаются от этих атак?

8. Какие настройки Cisco IOS предотвращают ICMP-флуд на маршрутизаторе?

9. Почему злоумышленники используют ICMP-сканирование перед атакой? Какие инструменты они применяют?

10. Как статические ARP-записи снижают риск MITM-атак в корпоративной сети?

11. Опишите этические дилеммы, возникающие при изучении инструментов для симуляции DDoS.

12. Приведите пример комбинированной атаки, использующей ICMP и ARP-spoofing.

Раздел 2. Защита от сетевых угроз

Тема 2.1 Эволюция методов отражения вторжений

Перечень изучаемых вопросов

1. Системы обнаружения вторжений.
2. Межсетевые экраны.
3. Системы шифрования трафика.

Методические указания к изучению

Открытые информационные системы, функционирующие в условиях постоянного роста киберугроз, требуют непрерывного совершенствования методов защиты. Эволюция технологий отражения вторжений отражает ответ на усложнение атак: от базовых фильтров до интеллектуальных систем, сочетающих анализ трафика, шифрование и прогнозирование угроз. Рассмотрим ключевые компоненты этой эволюции, их развитие и современные подходы к обеспечению безопасности.

1. Системы обнаружения вторжений (IDS)

Первые системы обнаружения вторжений появились в 1980-х годах как реакция на рост сетевых атак. IDS предназначены для мониторинга активности в режиме реального времени и выявления подозрительных действий. Они делятся на два типа: **сетевые (NIDS)**, анализирующие трафик между узлами, и **хостовые (HIDS)**, отслеживающие события на отдельных устройствах. Современные IDS используют сигнатурный анализ (сравнение с шаблонами известных атак) и поведенческие методы (машинное обучение для обнаружения аномалий). Например, инструменты вроде Snort или Suricata позволяют настраивать правила для детектирования DDoS-атак, сканирования портов или SQL-инъекций.

Методические указания

- Установите Suricata в тестовой среде и настройте правила для обнаружения подозрительного трафика (например, множественные SSH-подключения).
- Изучите кейс применения IDS в финансовом секторе: как системы помогли предотвратить атаку на платёжный шлюз.
- Проанализируйте ложные срабатывания (false positives) и методы их минимизации через тонкую настройку алгоритмов.

2. Межсетевые экраны (Firewalls)

Межсетевые экраны эволюционировали от простых пакетных фильтров до многоуровневых систем. Ранние решения (например, статические ACL на маршрутизаторах) блокировали трафик по IP-адресам и портам. Современные next-generation firewalls (NGFW) интегрируют глубокий анализ пакетов (DPI), контроль приложений и защиту от угроз на уровне содержимого. Такие системы, как Palo Alto Networks или Cisco Firepower, способны блокировать вредоносные URL, предотвращать утечки данных и анализировать зашифрованный трафик через SSL-инспекцию.

Методические указания:

- Создайте виртуальную сеть в GNS3 и настройте межсетевой экран (pfSense) для фильтрации трафика по протоколам (например, запрет ICMP).
- Исследуйте работу NGFW на примере блокировки доступа к фишинговым сайтам через чёрные списки.
- Проведите аудит правил фаервола в корпоративной среде, устранив избыточные разрешения (принцип минимальных привилегий).

3. Системы шифрования трафика

Шифрование – основа защиты данных в открытых сетях. Ранние методы (например, протокол SSL 1.0) имели критические уязвимости, что привело к развитию TLS и его современных версий (TLS 1.3). Шифрование применяется на разных уровнях:

- **Транспортный уровень** HTTPS, SSH) – защита данных между клиентом и сервером.
- **Сетевой уровень** (IPsec, VPN) – создание зашифрованных туннелей для передачи трафика между сетями.
- **Прикладной уровень** (PGP, S/MIME) – шифрование электронной почты и файлов. Современные решения, такие как Let’s Encrypt, обеспечивают автоматизацию выдачи сертификатов, а WireGuard предлагает упрощённую и высокопроизводительную реализацию VPN.

Методические указания:

A. Настройте HTTPS на веб-сервере с помощью Let’s Encrypt, проанализировав процесс рукопожатия TLS в Wireshark.

B. Создайте VPN-туннель между двумя сетями с использованием OpenVPN или WireGuard.

C. Изучите атаки на устаревшие протоколы (например, POODLE для SSL 3.0) и методы их предотвращения.

Литература

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст: электронный (гл. 2, 3, 7, 8).

2. Киренберг, Г. А. Информационная безопасность современных операционных систем: учеб. пособие / Г. А. Киренберг. – Кемерово: КузГТУ

им. Т. Ф. Горбачева, 2022. – 138 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/295736 (дата обращения: 06.12.2024). – ISBN 978-5-00137-320-9. – Текст : электронный (гл. 3, параграфы 3.3, 3.8).

3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный. (Главы 2, 3, 4)

Контрольные вопросы

1. Чем отличается сигнатурный анализ IDS от поведенческого? Приведите примеры использования каждого метода.
2. Почему NGFW считаются более эффективными, чем традиционные межсетевые экраны?
3. Как SSL-инспекция в NGFW помогает анализировать зашифрованный трафик? Какие риски это несёт?
4. Опишите сценарий, при котором HIDS обнаруживает несанкционированное изменение системных файлов.
5. Какие преимущества предоставляет TLS 1.3 по сравнению с предыдущими версиями?
6. Почему статические пакетные фильтры недостаточны для защиты от современных угроз?
7. Как VPN на основе WireGuard обеспечивает безопасность данных в публичных сетях?
8. Какие уязвимости присущи ранним протоколам шифрования (например, SSL 2.0)?
9. Объясните роль машинного обучения в снижении числа ложных срабатываний IDS.
10. Как Let’s Encrypt решает проблему доверия к самоподписанным сертификатам?
11. Какие этические аспекты возникают при мониторинге трафика через IDS в корпоративной сети?
12. Предложите комплексную стратегию защиты открытой системы, сочетающую IDS, NGFW и шифрование.

Тема 2.2 Классификация методов отражения вторжений

Перечень изучаемых вопросов

1. Классификация методов отражения вторжений.
2. Предотвращение вторжения.
3. Противодействие вторжению.
4. Сдерживание вторжения.

5. Отклонение вторжения.
6. Обнаружение вторжений.

Методические указания к изучению:

1. Классификация методов отражения вторжений

Методы защиты от вторжений делятся на категории, основанные на их целях и этапах применения: **предотвращение, противодействие, сдерживание**, **отклонение** и **обнаружение**. Каждая категория решает специфические задачи: от недопущения атак до минимизации ущерба после их успешного выполнения. Например, предотвращение фокусируется на устранении уязвимостей, а обнаружение – на оперативном выявлении активных угроз.

Методические указания

- Изучите стандарты NIST (SP 800-53) и MITRE ATT&CK, которые классифицируют методы защиты в контексте жизненного цикла атак.
- Проведите сравнительный анализ решений Cisco, Palo Alto и Fortinet, определив, какие категории методов они реализуют.

2. Предотвращение вторжения

Предотвращение направлено на устранение условий, позволяющих злоумышленнику начать атаку. Это включает:

- **Устранение уязвимостей** – регулярное обновление ПО и закрытие известных эксплойтов (например, патчи для CVE-2021-44228 в Log4j).
- **Конфигурационная безопасность** – настройка межсетевых экранов, отключение ненужных служб, применение принципа минимальных привилегий.
- **Шифрование данных** – использование TLS для защиты трафика, VPN для удалённого доступа.

Методические указания:

- Проведите аудит конфигурации веб-сервера (например, Apache/Nginx) с помощью инструментов Lynis или OpenVAS.
- Смоделируйте сценарий, где отсутствие обновления ПО приводит к эксплуатации уязвимости (на примере EternalBlue).

3. Противодействие вторжению

Противодействие – активные меры по блокировке атаки в реальном времени.

Примеры:

- **Системы предотвращения вторжений (IPS)** – автоматическая блокировка подозрительного трафика (например, Snort в режиме IPS).
- **Динамическая изоляция заражённых узлов** – перемещение атакуемого устройства в карантинную сеть (средствами NAC – Network Access Control).

Методические указания:

- Настройте Suricata в режиме IPS для блокировки сканирования портов.
- Изучите кейс реагирования на атаку WannaCry, где своевременное обновление правил IPS предотвратило шифрование данных.

4. Сдерживание вторжения

Сдерживание ограничивает распространение атаки, если она уже проникла в систему:

- **Сегментация сети** – разделение на VLAN, использование микросегментации для изоляции критических ресурсов.
- **Контейнеризация** – запуск приложений в изолированных средах (Docker, Kubernetes) для предотвращения lateral movement.

Методические указания:

- Разработайте схему сегментации сети для компании, где бухгалтерия и IoT-устройства изолированы от общей инфраструктуры.
- Проанализируйте инцидент с Target (2013), где отсутствие сегментации позволило хакерам проникнуть в платёжную систему через HVAC-сеть.

5. Отклонение вторжения

Отклонение дезориентирует злоумышленников, усложняя выбор целей:

- **Honeypots** – создание ложных систем для отвлечения атакующих (например, проекты Cowrie или Canarytokens).
- **Динамическое изменение сетевых параметров** – ротация IP-адресов, использование Moving Target Defense (MTD).

Методические указания:

- Разверните honeypot на базе Elasticsearch для имитации уязвимой базы данных и анализа методов атакующих.
- Изучите кейс банка, где MTD снизил количество успешных атак на 70 % за счёт постоянного изменения конфигураций.

6. Обнаружение вторжений

Обнаружение фокусируется на выявлении активных или уже состоявшихся атак:

- **Сигнатурный анализ** – сравнение событий с шаблонами известных угроз (например, правила YARA).
- **Анализ аномалий** – машинное обучение для выявления отклонений в поведении пользователей или трафика.

Методические указания:

- Настройте ELK-стек (Elasticsearch, Logstash, Kibana) для агрегации и визуализации логов с IDS.
- Проведите расследование инцидента на основе искусственно созданных логов, имитирующих атаку на Active Directory.

Литература

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст: электронный (гл. 2, 3, 7, 8).

2. Киренберг, Г. А. Информационная безопасность современных операционных систем: учеб. пособие / Г. А. Киренберг. – Кемерово: КузГТУ им. Т. Ф. Горбачева, 2022. – 138 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/295736 (дата обращения: 06.12.2024). – ISBN 978-5-00137-320-9. – Текст : электронный (гл. 3, параграфы 3.3, 3.8).

3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный (гл. 2–4).

Контрольные вопросы

1. Чем отличается предотвращение вторжений от противодействия? Приведите примеры инструментов для каждой категории.
2. Как принцип минимальных привилегий способствует предотвращению атак?
3. Опишите сценарий, при котором IPS блокирует атаку на уровне приложения (например, SQL-инъекцию).
4. Почему сегментация сети считается ключевым методом сдерживания? Какие риски она устраняет?
5. Как honeypots помогают в сборе разведданных о тактиках злоумышленников?
6. Объясните, как Moving Target Defense усложняет проведение целевых атак.
7. Какие преимущества даёт комбинация сигнатурного и поведенческого анализа в системах обнаружения?
8. Почему контейнеризация не гарантирует полной защиты от lateral movement?
9. Как динамическая изоляция узлов через NAC предотвращает распространение ransomware?
10. Какие этические проблемы возникают при использовании honeypots?

Тема 2.3 Политика безопасности интернет-сети

Перечень изучаемых вопросов

1. Политика безопасности интернет-сети.
2. Сетевой аудит.
3. Место систем обнаружения вторжений в защите интернет-сети и интрасетей.

Методические указания к изучению

Открытые информационные системы, взаимодействующие через интернет и интрасети, требуют комплексного подхода к обеспечению безопасности. Политика безопасности, аудит и системы обнаружения вторжений формируют триаду, которая обеспечивает защиту от угроз, контроль соответствия стандартам и оперативное реагирование на инциденты. Рассмотрим каждый компонент в контексте их взаимодополняемости и практического применения.

1. Политика безопасности интернет-сети

Политика безопасности – это формализованный свод правил, процедур и стандартов, определяющих, как организация защищает свои сетевые ресурсы. Её цель – минимизировать риски за счёт чётких регламентов управления доступом, обработки данных и реагирования на угрозы. Ключевые элементы включают:

a. **Управление доступом**. Разграничение прав пользователей на основе ролей (RBAC), использование многофакторной аутентификации.

b. **Шифрование данных**. Применение TLS для веб-трафика, VPN для удалённого доступа, защита конфиденциальных данных в хранилищах.

c. **Процедуры реагирования**. Алгоритмы действий при утечках данных, DDoS-атаках или компрометации учётных записей.

d. **Обновления и патчи**. Регламент регулярного обновления ПО и сетевого оборудования.

Пример: Политика компании Google требует обязательного использования аппаратных ключей безопасности для сотрудников, работающих с критической инфраструктурой.

Методические указания

A. Изучите шаблоны политик NIST или ISO 27001, адаптируя их под гипотетическую компанию.

B. Проведите анализ уязвимостей в политике условной организации, где отсутствует регламент шифрования почты.

2. Сетевой аудит

Сетевой аудит – систематическая проверка сетевой инфраструктуры на соответствие политике безопасности и выявление уязвимостей. Этапы аудита включают:

A. **Инвентаризацию активов**. Составление карты сети, идентификация устройств, сервисов и точек входа.

B. **Анализ конфигураций**. Проверка настроек межсетевых экранов, роутеров и серверов на соответствие стандартам.

C. **Тестирование на проникновение**. Использование инструментов вроде Metasploit или Nessus для имитации атак.

1. **Формирование отчёта**: Рекомендации по устранению недостатков (например, закрытие незащищённых портов).

Пример: Аудит сети розничной сети Target в 2013 году не выявил слабых мест в системах HVAC, что привело к масштабной утечке данных.

Методические указания:

a. Проведите аудит тестовой сети с помощью Nmap для обнаружения открытых портов и Wireshark для анализа трафика.

b. Смоделируйте сценарий, где некорректная настройка DHCP-сервера позволяет провести ARP-spoofing.

3. Место систем обнаружения вторжений в защите интернет-сети и интрасетей

Системы обнаружения вторжений (IDS) играют роль «сторожевых псов», отслеживающих аномалии в режиме реального времени. Их функции в защите сетей включают:

a. **Мониторинг трафика**. Выявление подозрительных шаблонов (например, множественные попытки входа).

b. **Интеграцию с экосистемой безопасности**. Передача данных в SIEM-системы (Splunk, ELK) для корреляции событий.

c. **Поддержку политик безопасности**. Автоматизация блокировки IP-адресов при попытках сканирования портов.

Пример: В интрасети банка HIDS на серверах с данными клиентов обнаруживает несанкционированные изменения в системных файлах, предотвращая распространение ransomware.

Методические указания

a. Настройте Suricata для детектирования SQL-инъекций в веб-трафике.

b. Изучите кейс, где комбинация NIDS и HIDS помогла выявить APT-атаку через анализ аномалий в DNS-запросах.

Литература

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. — Текст: электронный (гл. 6).

2. Киренберг, Г. А. Информационная безопасность современных операционных систем: учеб. пособие / Г. А. Киренберг. – Кемерово: КузГТУ им. Т. Ф. Горбачева, 2022. – 138 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/295736 (дата обращения: 06.12.2024). – ISBN 978-5-00137-320-9. – Текст : электронный (гл. 3, параграфы 3.4, 3.5).

3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный (гл. 3).

Контрольные вопросы

1. Какие разделы должны быть включены в политику безопасности интернет-сети для обеспечения защиты от фишинга?

2. Объясните, как RBAC способствует реализации принципа минимальных привилегий.

3. Почему регулярный сетевой аудит важен даже при наличии IDS?

4. Опишите, как инструмент Nessus может быть использован для проверки соответствия политике шифрования данных.

5. Какие ограничения имеют сигнатурные методы обнаружения вторжений в сравнении с поведенческими?

6. Как интеграция IDS с SIEM улучшает реакцию на инциденты? Приведите пример.

7. Почему политика безопасности должна включать регламент обновления сетевого оборудования?

8. Какие риски возникают при отсутствии инвентаризации активов в процессе аудита?

9. Как HIDS помогает защитить интрасети от внутренних угроз?

10. Опишите сценарий, при котором аудит выявляет незакрытый порт, используемый для майнинга криптовалюты.

11. Какие этические аспекты необходимо учитывать при настройке IDS для мониторинга сотрудников?

12. Предложите стратегию, объединяющую политику безопасности, аудит и IDS для защиты облачной инфраструктуры.

Тема 2.4 Системы обнаружения вторжений и межсетевые экраны

Перечень изучаемых вопросов

1. Системы обнаружения вторжений и межсетевые экраны.

2. Порядок развертывания систем обнаружения вторжений.

Методические указания к изучению

1. Системы обнаружения вторжений и межсетевые экраны: основы и взаимодействие

Межсетевые экраны служат первым рубежом защиты, фильтруя входящий и исходящий трафик на основе предустановленных правил. Они оперируют на сетевом и транспортном уровнях модели OSI, блокируя нежелательные подключения по IP-адресам, портам или протоколам. Современные next-generation firewalls (NGFW) расширяют функционал, анализируя содержимое пакетов (DPI – Deep Packet Inspection) и блокируя угрозы на прикладном уровне, такие как SQL-инъекции или вредоносные URL.

Системы обнаружения вторжений (IDS) действуют как «интеллектуальные наблюдатели», выявляя аномалии и сигнатуры известных атак. В отличие от экранов, IDS не блокируют трафик, а генерируют оповещения. Они делятся на два типа:

a. **Сетевые (NIDS)**, анализирующие трафик в ключевых точках сети (например, на границе DMZ).

b. **Хостовые (HIDS)**, отслеживающие события на конкретных устройствах (изменения в системных файлах, подозрительные процессы).

Совместное использование межсетевых экранов и IDS создаёт синергию: экраны предотвращают очевидные угрозы, а IDS обнаруживают сложные и замаскированные атаки, такие как APT (Advanced Persistent Threats). Например, NGFW может блокировать трафик с подозрительных IP-адресов, а NIDS – детектировать шаблоны атак в разрешённом трафике, используя методы машинного обучения.

Методические указания:

a. Разверните виртуальную сеть с помощью GNS3, интегрировав pfSense в качестве межсетевого экрана и Suricata в роли NIDS. Настройте правила для блокировки SSH-подключений из определённых стран и детектирования сканирования портов.

b. Изучите кейс, когда комбинация IDS и NGFW помогла предотвратить утечку данных через анализ аномального исходящего трафика (например, передача больших объёмов данных в нерабочее время).

2. Порядок развертывания систем обнаружения вторжений

Развертывание IDS включает несколько этапов, направленных на интеграцию системы в существующую инфраструктуру без нарушения её работы:

1. **Планирование и анализ требований**: Определение целей (обнаружение внешних атак, мониторинг внутренних угроз), выбор между NIDS и HIDS, оценка производительности сети.

2. **Выбор инструментов**: Решения вроде Snort (для сетевого уровня) или OSSEC (для хостового) подходят для старта, тогда как коммерческие продукты (Cisco Firepower) предлагают расширенную аналитику.

3. **Размещение сенсоров**: Установка NIDS на граничных маршрутизаторах или внутри критических сегментов (например, между серверами баз данных и веб-приложениями). Для HIDS – развертывание агентов на всех узлах.

4. **Настройка правил и политик**:

a. Реализация сигнатурных правил для известных угроз (например, шаблоны атак из базы Emerging Threats).

b. Настройка поведенческого анализа для выявления отклонений (аномальное количество запросов к DNS-серверу).

5. **Интеграция с SIEM-системами**: Передача событий в Splunk или Elastic Stack для корреляции данных и генерации комплексных отчетов.

6. **Тестирование и калибровка**: Имитация атак (например, Metasploit) для проверки эффективности детектирования и настройки порогов ложных срабатываний.

Методические указания

a. Создайте тестовую среду с помощью VirtualBox, установите Security Onion (дистрибутив для IDS/IPS) и проведите пентест, используя Kali Linux.

b. Изучите документацию Suricata для настройки правил, блокирующих трафик, связанный с криптоджекингом.

Литература

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст: электронный (гл. 3, 13, 15).

2. Киренберг, Г. А. Информационная безопасность современных операционных систем: учеб. пособие / Киренберг, Г. А. – Кемерово: КузГТУ им. Т. Ф. Горбачева, 2022. – 138 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/295736 (дата обращения: 06.12.2024). – ISBN 978-5-00137-320-9. – Текст : электронный (гл. 3, параграфы 3.3, 3.8).

3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный (гл. 2–4).

Контрольные вопросы

1. Чем принципиально отличается функционал межсетевого экрана от IDS? Приведите пример сценария, где их совместное использование необходимо.
2. Почему NGFW эффективнее традиционных межсетевых экранов в борьбе с современными угрозами?
3. Опишите, как Deep Packet Inspection помогает предотвратить атаки на прикладном уровне.
4. Какие преимущества даёт использование HIDS в сравнении с NIDS для защиты серверов баз данных?
5. Как настройка поведенческого анализа в IDS снижает риск пропуска zero-day атак?
6. Почему размещение NIDS на границе сети недостаточно для обнаружения внутренних угроз?
7. Какие этапы включает процесс калибровки IDS после развертывания?
8. Объясните роль SIEM-систем в контексте работы IDS. Приведите пример корреляции событий.
9. Какие риски возникают при неправильной настройке порогов для ложных срабатываний?
10. Как инструменты вроде Metasploit используются для тестирования эффективности IDS?
11. Почему при развертывании IDS важно учитывать пропускную способность сети?

12. Предложите стратегию интеграции межсетевого экрана и IDS для защиты облачного окружения AWS.

Тема 2.5 Классификация систем обнаружения вторжений

Перечень изучаемых вопросов

1. Классификация систем обнаружения вторжений.
2. Эволюция систем обнаружения вторжения.

Методические указания к изучению

1. Классификация систем обнаружения вторжений

Системы обнаружения вторжений различаются по **типу мониторинга**, **методам анализа** и **месту развертывания**.

По типу мониторинга выделяют:

a. **Сетевые (NIDS)**, которые анализируют трафик на уровне пакетов, выявляя аномалии в сетевом взаимодействии. Пример: Suricata, обнаруживающая сканирование портов или DDoS-атаки.

b. **Хостовые (HIDS)**, отслеживающие события на отдельных устройствах: изменения в реестре, подозрительные процессы или доступ к критическим файлам. Инструменты вроде OSSEC фиксируют попытки модификации системных конфигураций.

По методам анализа:

a. **Сигнатурные СОВ** работают на основе шаблонов известных атак (например, правила Snort для SQL-инъекций). Их эффективность высока против известных угроз, но они уязвимы к zero-day атакам.

b. **Системы обнаружения аномалий** используют статистические модели или машинное обучение для выявления отклонений от нормального поведения. Например, Darktrace применяет ИИ для детектирования необычной активности в корпоративных сетях.

По уровню активности:

a. **Пассивные СОВ** только генерируют оповещения, не вмешиваясь в трафик.

b. **Активные СОВ (IPS)** автоматически блокируют подозрительные соединения, как это делает Cisco Firepower.

Специализированные решения включают гибридные системы (например, комбинация NIDS и HIDS) и облачные СОВ, такие как AWS GuardDuty, адаптированные для мониторинга виртуальных инфраструктур.

Методические указания

a. Установите Security Onion (дистрибутив с Suricata и Zeek) для анализа сетевого трафика. Настройте правила обнаружения сканирования Nmap.

b. Сравните логи OSSEC (HIDS) и Suricata (NIDS) при попытке несанкционированного доступа к серверу.

3. Эволюция систем обнаружения вторжений

а. Развитие СОВ отражает ответ на усложнение кибератак и технологический прогресс.

1980–1990-е: Эпоха сигнатурных систем

Первые СОВ, такие как Snort (1998), полагались на статические правила. Они эффективно блокировали известные угрозы, но требовали постоянного обновления баз сигнатур.

2000-е: Внедрение поведенческого анализа

С ростом числа атак на прикладном уровне появились системы, анализирующие контекст запросов. Пример: Bro (ныне Zeek), который коррелирует события сети для выявления сложных сценариев, например, цепочек HTTP-запросов, характерных для APT.

2010-е: Интеграция машинного обучения

Современные СОВ, такие как Vectra AI, используют алгоритмы для анализа больших данных. Они обучаются на исторических данных, выявляя аномалии в поведении пользователей или устройств. Например, внезапный всплеск исходящего трафика с сервера может указывать на утечку данных.

2020-е: Автономные системы и облачная интеграция

Развитие облачных технологий привело к созданию решений вроде Microsoft Azure Sentinel, которые объединяют данные из различных источников (логи, метрики, трафик) и применяют AI для прогнозирования угроз.

Методические указания:

1. Изучите эволюцию Snort: от сигнатурных правил до поддержки Lua-скриптов для кастомизации.

2. Проанализируйте кейс компании Target (2013), где отсутствие поведенческого анализа позволило хакерам длительно оставаться незамеченными.

Литература

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст: электронный (гл. 3, 13, 15).

Контрольные вопросы

1. Чем принципиально отличаются сетевые и хостовые СОВ? Приведите примеры задач, которые решает каждая из них.

2. Почему сигнатурные системы неэффективны против zero-day атак? Как эту проблему решают современные СОВ?

3. Опишите сценарий, при котором HIDS обнаруживает ransomware на ранней стадии шифрования файлов.

4. Какие преимущества даёт использование машинного обучения в системах обнаружения аномалий?

5. Как облачные СОВ, такие как AWS GuardDuty, адаптированы для работы в виртуальных средах?

6. Почему пассивные СОВ до сих пор используются, несмотря на развитие активных решений (IPS)?

7. Объясните роль Zeek (ранее Bro) в анализе сетевых протоколов. Приведите пример детектирования APT.

8. Какие этические риски возникают при использовании ИИ в СОВ для мониторинга сотрудников?

9. Как интеграция СОВ с SIEM-системами улучшает реагирование на инциденты?

10. Опишите, как Microsoft Azure Sentinel использует облачные вычисления для прогнозирования угроз.

11. Почему в гибридных системах сочетают NIDS и HIDS? Приведите пример синергии.

12. Какие тенденции в развитии СОВ можно ожидать в ближайшие 5–10 лет?

Тема 2.6 Размещение сетевых систем обнаружения вторжений

Перечень изучаемых вопросов

1. Размещение сетевых систем обнаружения вторжений.
2. Интеллектуальное и поведенческое обнаружение вторжений.
3. Системное и сетевое обнаружение вторжений.

Методические указания к изучению

Открытые информационные системы, функционирующие в условиях постоянного взаимодействия с внешними сетями, требуют тщательно продуманного подхода к обнаружению угроз. Эффективность систем обнаружения вторжений (СОВ) зависит не только от их алгоритмов, но и от корректного размещения, а также интеграции методов анализа. Рассмотрим ключевые аспекты их развертывания, эволюцию методов обнаружения и различия между сетевыми и системными решениями.

1. Размещение сетевых систем обнаружения вторжений (NIDS)

Размещение NIDS – стратегический процесс, определяющий, насколько полно система сможет отслеживать угрозы. Ключевые принципы включают:

a. **Граничные точки**. Установка сенсоров на периметре сети (например, за межсетевым экраном) позволяет детектировать атаки на этапе проникновения. Это критически важно для выявления сканирования портов или DDoS-флуда.

b. **Внутренние сегменты**. Размещение NIDS между критическими зонами (например, между серверами баз данных и веб-приложениями) помогает обнаруживать lateral movement – перемещение злоумышленников внутри сети после первоначального взлома.

c. **Точки с высокой пропускной способностью**. Для анализа трафика в магистральных каналах используются аппаратные ускорители (например, FPGA-платы) или облачные решения, такие как Amazon VPC Traffic Mirroring.

Пример: В сетях с сегментацией по VLAN сенсоры NIDS размещаются на каждом транке, соединяющем VLAN, чтобы отслеживать межсегментный трафик.

Методические указания

a. Создайте тестовую сеть в GNS3 с DMZ, внутренней сетью и WAN-сегментом. Разместите Suricata в каждой зоне и сравните данные о подозрительной активности.

b. Изучите кейс компании Cloudflare, где корректное размещение NIDS позволило снизить время обнаружения BGP-хайджека с часов до минут.

2. Интеллектуальное и поведенческое обнаружение вторжений

Современные СОВ вышли за рамки сигнатурного анализа, внедрив методы, которые адаптируются к новым угрозам:

a. **Интеллектуальное обнаружение**. Использование машинного обучения (ML) и искусственного интеллекта (AI) для прогнозирования атак. Например, Darktrace анализирует паттерны поведения устройств и пользователей, выявляя аномалии, такие как необычный доступ к файлам в нерабочее время.

b. **Поведенческое обнаружение**. Системы строят базовый профиль «нормальной» активности (например, частоту запросов к DNS-серверу) и сигнализируют о отклонениях. Решения вроде Cisco Stealthwatch используют потоковый анализ (NetFlow) для детектирования скрытого майнинга криптовалюты.

Методические указания

a. Настройте Elastic Stack (ELK) для агрегации логов и создания поведенческих профилей сетевой активности.

b. Проведите эксперимент: смоделируйте атаку на основе TTPs (Tactics, Techniques, Procedures) из базы MITRE ATT&CK и оцените, как ML-модель в Security Onion её классифицирует.

3. Системное и сетевое обнаружение вторжений

Системное (HIDS) и сетевое (NIDS) обнаружение дополняют друг друга, обеспечивая многоуровневую защиту:

a. **Системное обнаружение (HIDS)**: Мониторит события на уровне ОС: изменения в реестре Windows, подозрительные процессы в Linux (например, скрытые криптомайнеры). Инструменты вроде Wazuh интегрируются с аудит-логами для отслеживания прав доступа.

b. **Сетевое обнаружение (NIDS)**: Анализирует сырой трафик, выявляя аномалии в протоколах. Например, Zeek (ранее Bro) детектирует нестандартные HTTP-заголовки, характерные для эксплуатации уязвимостей веб-приложений.

Синергия достигается за счет интеграции HIDS и NIDS в SIEM-системы. Например, подозрительный исходящий трафик, обнаруженный NIDS, может быть сопоставлен с логами HIDS о запуске неизвестного процесса на сервере.

Методические указания:

a. Установите Wazuh (HIDS) на виртуальную машину и настройте оповещения о попытках изменения файла /etc/passwd.

b. Сравните логи Suricata (NIDS) и Wazuh при атаке на веб-сервер: как каждый инструмент фиксирует разные этапы компрометации.

Литература:

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст: электронный (гл. 6, 8).

Контрольные вопросы

1. Почему размещение NIDS на границе сети недостаточно для защиты от внутренних угроз? Приведите пример атаки, которую можно пропустить.
2. Как машинное обучение улучшает детектирование аномалий по сравнению с сигнатурными методами?
3. Опишите сценарий, при котором поведенческий анализ обнаруживает APT-атаку через аномальные DNS-запросы.
4. Какие преимущества даёт использование FPGA-плат в высоконагруженных сетях для NIDS?
5. Чем отличается роль HIDS и NIDS в обнаружении ransomware?
6. Почему интеграция HIDS и SIEM критически важна для расследования инцидентов?
7. Как Amazon VPC Traffic Mirroring решает проблему анализа трафика в облачных средах?
8. Какие риски возникают при некорректной настройке базового профиля «нормальной» активности?
9. Объясните, как Zeek обнаруживает эксплуатацию уязвимости в веб-приложении через анализ HTTP-заголовков.
10. Почему HIDS эффективен для мониторинга действий привилегированных пользователей?
11. Какие ограничения имеют облачные NIDS при работе с зашифрованным трафиком?
12. Предложите стратегию размещения NIDS и HIDS в гибридной инфраструктуре (облако + локальные серверы).

Тема 2.7 Порядок реагирования на вторжения в интернет-сети и организационно-правовые вопросы

Перечень изучаемых вопросов

1. Порядок реагирования на вторжения в интернет-сети и организационно-правовые вопросы.

2. Сохранение доказательств вторжения

Методические указания к изучению

Открытые информационные системы, подверженные кибератакам, требуют не только технической защиты, но и чётко регламентированных процедур реагирования на инциденты. Успешное устранение последствий вторжения и минимизация ущерба зависят от слаженных действий технических специалистов, юристов и руководства, а также от соблюдения правовых норм. Рассмотрим этапы реагирования, юридические аспекты и методы сохранения доказательств, критически важные для расследования и предотвращения будущих атак.

1. Порядок реагирования на вторжения в интернет-сети и организационно-правовые вопросы

Реагирование на инциденты делится на этапы, закреплённые в стандартах (NIST SP 800-61, ISO/IEC 27035):

1. Подготовка

На этом этапе разрабатываются планы реагирования, назначаются ответственные лица и проводятся учения. Пример: компания Microsoft регулярно тестирует свои Incident Response (IR) команды через симуляции атак на Azure. Организационно-правовая подготовка включает:

a. **Соглашения с третьими сторонами**. Договоры с CERT-командами, юристами и правоохранительными органами.

b. **Соответствие регуляторным требованиям**. GDPR, CCPA, ФЗ-152 «О персональных данных» – нарушение этих норм может привести к штрафам до 4 % глобального оборота компании.

2. Обнаружение и анализ

Использование SIEM-систем (Splunk, IBM QRadar) для агрегации логов и выявления аномалий. Например, необычные исходящие подключения с сервера могут указывать на утечку данных. Юридический аспект: необходимость уведомления регуляторов в течение 72 ч (по GDPR) при утечке персональных данных.

3. Сдерживание и ликвидация

Технические меры: изоляция заражённых узлов через NAC, блокировка злонамеренных IP-адресов. Организационные: привлечение юристов для оценки рисков судебных исков. Пример: после атаки на Colonial Pipeline (2021) компания временно отключила ИТ-системы, чтобы остановить распространение ransomware.

4. Восстановление

Восстановление данных из бэкапов, проверка их целостности. Правовой аспект: обязательство уведомить клиентов о компрометации, как это сделала British Airways после утечки данных 380 тыс. клиентов в 2018 г.

5. Пост-инцидентный анализ

Составление отчёта с рекомендациями по улучшению безопасности. Юридический фокус: документирование действий для защиты от исков (например, доказательство выполнения «разумных мер» защиты).

Методические указания:

a. Проведите ролевую игру: смоделируйте инцидент утечки данных и отработайте взаимодействие между IR-командой, юристами и PR-отделом.

b. Изучите кейс Equifax (2017), где задержка в уведомлении регуляторов привела к штрафу в $ 700 млн.

2. Сохранение доказательств вторжения

a. Сохранение цифровых доказательств требует соблюдения процессуальных норм, чтобы они были допустимы в суде. Ключевые принципы:

b. **Целостность данных**

c. **Использование криптографических хешей**: Запись хешей (SHA-256) файлов и логов до и после изъятия.

d. **Работа с образами дисков**: Инструменты вроде FTK Imager или dd создают бит-в-бит копии носителей без изменения оригиналов.

e. **Документирование цепочки владения (Chain of Custody)** Каждый этап работы с доказательствами фиксируется в журнале: кто, когда и с какой целью получил доступ. Пример: при расследовании взлома Sony Pictures (2014) цепочка владения помогла установить причастность хакерской группы Lazarus.

Правовые требования

1. Соответствие стандартам. Руководство NIST SP 800-86 по сбору цифровых доказательств.

2. Международное сотрудничество. Если атака производится, требуется взаимодействие с Interpol или Europol.

Методические указания

a. Создайте образ жёсткого диска виртуальной машины, заражённой ransomware, используя FTK Imager. Задокументируйте процесс в Chain of Custody.

b. Разберите кейс атаки на Uber (2016), где попытка скрыть факт взлома привела к уголовному преследованию руководства.

Литература:

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст: электронный (гл. 8–10).

2. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный (гл. 5).

Контрольные вопросы

1. Какие этапы реагирования на инцидент предусмотрены стандартом NIST SP 800-61? Опишите организационные задачи на каждом этапе.
2. Почему GDPR требует уведомлять регуляторов о утечке данных в течение 72 часов? Какие последствия несёт нарушение этого срока?
3. Как система NAC помогает в сдерживании распространения ransomware в корпоративной сети?
4. Опишите правовые риски, возникающие при восстановлении данных из незашифрованных бэкапов.
5. Какие методы обеспечения целостности доказательств используются при создании образа диска?
6. Почему цепочка владения (Chain of Custody) критически важна для судебного разбирательства?
7. Как юристы участвуют в пост-инцидентном анализе на примере кейса British Airways?
8. Какие инструменты применяются для документирования сетевой активности во время инцидента?
9. Почему попытка скрыть факт взлома, как в случае с Uber, усугубляет юридические последствия?
10. Как международное право регулирует расследование зафиксированных кибератак? Приведите пример сотрудничества стран.
11. Какие ошибки в сохранении доказательств могут сделать их недопустимыми в суде?
12. Предложите процедуру взаимодействия IR-команды и PR-отдела при публичном уведомлении о взломе.

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

Лабораторные занятия направлены на углубление знаний и закрепление основных понятий и методов, изучаемых в рамках дисциплины. Основная цель занятий – научиться применять теоретические знания для решения прикладных задач.

Рекомендации к подготовке

1. Изучение лекционного материала и конспектов:

– перед лабораторными занятиями необходимо проработать соответствующие разделы лекционного материала;

– рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом лабораторного занятия.

2. Проработка учебной литературы:

– используйте основные учебники и методические пособия, рекомендованные преподавателем;

– для глубокого понимания теории рекомендуется обращаться к дополнительной литературе.

3. Решение типовых задач:

– проработать примеры и типовые задачи из учебных материалов, методических указаний;

– выполните задачи, предложенные преподавателем для самостоятельной работы, что обеспечит лучшее понимание методов и подходов к решению задач.

4. Подготовка вопросов:

– составьте список вопросов по материалу, вызвавшему затруднения;

– обсуждение этих вопросов на лабораторном занятии поможет устранить пробелы в знаниях.

5. Вопросы для самоконтроля:

– перед каждым занятием рекомендуется проверять себя с помощью вопросов для самоконтроля из методических указаний к лекционным занятиям. Это позволит оценить уровень своей подготовки.

Тематический план лабораторных занятий приводится в разделе «Тематический план» (таблица 1).

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста):
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

– систематизации и закрепления полученных теоретических знаний и практических умений студентов;

– углубления и расширения теоретических знаний;

– формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

– развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

– изучить рекомендуемые литературные источники:

– изучить основные понятия, представленные в глоссарии;

– ответить на контрольные вопросы:

– решить предложенные задачи, кейсы, ситуации;

– выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам.

2. Выполнение письменных контрольных и курсовых работ.

3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов.

4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) – важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых проектов и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента не регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знании:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудиовидеозаписей):
- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;

- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена;

Для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений:
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- создание проспектов, проектов, моделей;
- экспериментальная работа, участие в НИР;
- рефлексивный анализ профессиональных умений с использованием аудиовидеотехники и компьютерных расчетных программ, и электронных практикумов;
- подготовка курсовых проектов и дипломных работ;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

5. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Текущая аттестация

Преподаватель вправе выбрать методику оценивания знаний студентов: традиционная зачетно-экзаменационная либо балльно-рейтинговая**.** Выбрана традиционная зачетно-экзаменационная методика оценивания знаний. Предусматриваются: зачет, экзамен.

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации: контроль самостоятельной работы по темам дисциплины, контроль выполнения лабораторных работ.

К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов.

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости. В отдельных случаях (при не прохождении всех видов текущего контроля) зачет может быть проведен в виде тестирования.

Экзамен может проводиться как в традиционной форме, так и в виде экзаменационного тестирования. Тестовые задания для проведения экзаменационного тестирования приведены в фонде оценочных средств по дисциплине.

Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100-балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / **Критерий**				
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно- корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию,	Может найти необходимую информацию	Может найти, интерпретиро-	Может найти, систематизировать

Система оценок / Критерий				
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
	либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	в рамках поставленной задачи	вать и систематизировать необходимую информацию в рамках поставленной задачи	необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно-корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/не зачтено («зачтено» – 41–100 % правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» – менее 40 % правильных ответов; оценка «удовлетворительно» – от 41 до 60 % правильных ответов; оценка «хорошо» – от 61 до 80 % правильных ответов; оценка «отлично» – от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

Завершающим этапом изучения дисциплины является итоговая аттестация, представляющая собой экзамен.

Допуск к итоговой аттестации возможен при:

– наличии всех выполненных, сданных (проверенных, защищенных) лабораторных работах, наличии отчётов по ним;

– наличии показателей приемлемого уровня освоения материалов курса: более 50 % посещений от общего числа требуемых по учебному плану.

Примерные вопросы к зачету/экзамену по дисциплине

Вопросы к зачету

1. Раскрыть структурные особенности системы обнаружения вторжений.
2. Раскрыть особенности защиты интрасетей.
3. Раскрыть особенности политики безопасности интрасети.
4. Раскрыть особенности сетевого аудит.
5. Раскрыть особенности определения места систем обнаружения вторжений в защите интрасетей.
6. Охарактеризовать особенности функционирования и организации межсетевых экранов.
7. Привести порядок развертывания систем обнаружения вторжений.
8. Назвать и охарактеризовать методы отражения вторжений.
9. Привести классификация методов отражения вторжений.
10. Привести причины, способствующие атакам.
11. Привести ошибки в программном обеспечении используемые для сетевых атак.
12. Привести особенности конфигурирования системы защиты сети.
13. Привести особенности атаки «перехват паролей».
14. Привести особенности атаки «перехват незащищенного трафика».
15. Привести недостатки ос unix и протоколов.
16. Привести слабости системных утилит, команд и сетевых служб.
17. Раскрыть принцы проведения и указать особенности удаленных атак на интрасети.
18. Указать способы проникновения нарушителей в интрасети и проанализировать их.
19. Указать типичные сценарии и уровни атак.
20. Указать методы, используемые нападающими для сканирования карты сети.
21. Указать особенности проведения и блокирования атаки на переполнение буфера и rdist.

Вопросы к экзамену

1. Раскрыть структурные особенности системы обнаружения вторжений.
2. Раскрыть особенности защиты интрасетей.
3. Раскрыть особенности политики безопасности интрасети.
4. Раскрыть особенности сетевого аудит.

5. Раскрыть особенности определения места систем обнаружения вторжений в защите интрасетей.

6. Охарактеризовать особенности функционирования и организации межсетевых экранов.

7. Привести порядок развертывания систем обнаружения вторжений.

8. Назвать и охарактеризовать методы отражения вторжений.

9. Привести классификация методов отражения вторжений.

10. Привести причины, способствующие атакам.

11. Привести ошибки в программном обеспечении используемые для сетевых атак.

12. Привести особенности конфигурирования системы защиты сети.

13. Привести особенности атаки «перехват паролей».

14. Привести особенности атаки «перехват незащищенного трафика».

15. Привести недостатки ос unix и протоколов.

16. Привести слабости системных утилит, команд и сетевых служб.

17. Раскрыть принцы проведения и указать особенности удаленных атак на интрасети.

18. Указать способы проникновения нарушителей в интрасети и проанализировать их.

19. Указать типичные сценарии и уровни атак.

20. Указать методы, используемые нападающими для сканирования карты сети.

21. Указать особенности проведения и блокирования атаки на переполнение буфера и rdist.

22. Указать и охарактеризовать нападения с использованием сетевых протоколов.

23. Указать особенности проведения и блокирования атаки «летучая смерть».

24. Указать особенности проведения и блокирования атаки «Syn-бомбардировка».

25. Указать особенности проведения и блокирования атаки «спуффинг».

26. Указать особенности «нападений на основе протокола icmp и методы противодействия данным нападениям.

27. Указать особенности проведения и блокирования атаки «arp-spoofing».

28. Указать особенности проведения и блокирования атаки «атака ip hijacking».

29. Указать особенности проведения и блокирования атаки XSS-атак.

30. Указать особенности проведения и блокирования атаки SQL- инъекций.

31. Указать особенности распределенных атак «отказ в обслуживании

32. Указать особенности обнаружения прослушивающих приложений в Windows XP.

33. Раскрыть методы и охарактеризовать средства нейтрализации угрозы атаки.

34. Раскрыть методы управления безопасностью сетей.

35. Охарактеризовать основные модели нарушителей.

36. Укажите стандарты, РД, применяемые при создании и эксплуатации средств поиска уязвимостей ЛВС.

ЗАКЛЮЧЕНИЕ

Правильная организация учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

ЛИТЕРАТУРА

Основные источники

1. Баланов, А. Н. Комплексная информационная безопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 400 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/414947 (дата обращения: 09.10. 2024). – ISBN 978-5-507-49250-3. – Текст : электронный.

2. Киренберг, Г. А. Информационная безопасность современных операционных систем: учеб. пособие / Г. А. Киренберг. – Кемерово: КузГТУ им. Т. Ф. Горбачева, 2022. – 138 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/295736 (дата обращения: 06.12.2024). – ISBN 978-5-00137-320-9. – Текст : электронный.

3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб. пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. – Ростов-на-Дону: ИУБиП, 2020. – 114 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/248747 (дата обращения: 09.10.2024). – Текст : электронный.

4. Епишкина, А. В. Нормативное регулирование в области защиты информации. Конспект лекций: учеб. пособие / А. В. Епишкина, С. В. Запечников. – Москва: НИЯУ МИФИ, 2021. – 116 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/284345 (дата обращения: 09.10.2024). – ISBN 978-5-7262-2807-5. – Текст : электронный.

Дополнительные источники

5. Кияев, В. Безопасность информационных систем. Курс: учеб. пособие / В. Кияев, О. Граничин. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429032 (дата обращения: 09.10.2024). – Текст : электронный.

6. Лозовецкий, В. В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей: учеб. пособие для вузов / В. В. Лозовецкий, Е. Г. Комаров, В. В. Лебедев; под ред. В. В. Лозовецкого. – 2-е изд., стер. – Санкт-Петербург: Лань, 2024. – 488 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/397355 (дата обращения: 09.10.2024). – ISBN 978-5-507-47615-2. – Текст : электронный.

7. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд., стер. – Санкт-Петербург: Лань, 2024. – 324 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/370967 (дата обращения: 09.10.2024). – ISBN 978-5-507-49077-6. – Текст : электронный.

8. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учеб. пособие / А. Г. Киренберг. – Кемерово: КузГТУ им. Т. Ф. Горбачева, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/257564 (дата обращения: 06.12.2024). – ISBN 978-5-00137-292-9. – Текст : электронный.

Периодические издания

9. «Безопасность информационных технологий», «Информационно-управляющие системы», «Информация и безопасность»

Учебно-методические пособия, нормативная литература

10. Подтопельный, В. В. Учебно-методическое пособие по изучению дисциплины «Информационная безопасность открытых информационных систем» / В. В. Подтопельный. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 28 с. – Режим доступа: для авториз. пользователей. – URL: https://eios.klgtu.ru/course/view.php?id=9308 (дата обращения: 09.10.2024). – Текст : электронный.

11. Подтопельный, В. В. Информационная безопасность открытых информационных систем: учебно-методическое пособие по выполнению лабораторных работ по дисциплине для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем». – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 200 с. – Режим доступа: для авториз. пользователей. – URL: https://eios.klgtu.ru/course/view.php?id=9308 (дата обращения: 09.10.2024). – Текст : электронный.

12. Информационная безопасность распределенных информационных систем: метод. указания по выполнению лабораторных работ для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения / Федер. агентство по рыболовству [и др.]; сост. В. В. Подтопельный. – Калининград: БГАРФ, 2020. – Текст : непосредственный. Ч. 1 / сост. В. В. Подтопельный. – 2020. – 61 с.

13. Информационная безопасность распределенных информационных систем: метод. указания по выполнению лаб. работ для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / Федер. агентство по рыболовству [и др.]; сост. В. В. Подтопельный. – Калининград: БГАРФ, 2020. – Текст : непосредственный. Ч. 2. – 2021. – 42 с.

14. Информационная безопасность автоматизированных информационных систем: метод. указания по выполнению лаб. работ для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» очной формы обучения / Федер. агентство по рыболовству [и др.]; авт.-сост. А. А. Бабаева. – (изд. 2-е, с доп. и изм.). – Калининград: БГАРФ, 2022. – 46 с. – Текст : непосредственный.

Локальный электронный методический материал

Владислав Владимирович Подтопельный

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 3,8. Печ. л. 3,0.

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1