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

В. В. Подтопельный

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

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 ФГБОУ ВО «Калининградский государственный технический университет» Н. Я. Великите

Подтопельный, В. В.
Безопасность вычислительных сетей: 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. – 78 с.

Учебно-методическое пособие включает в себя рассмотрение теоретических вопросов в области защиты информации по дисциплине «Безопасность вычислительных сетей». 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 3, 4 курсов специальности 10.05.03 «Информационная безопасность автоматизированных систем».
Табл. 2, список лит. – 26 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)

© Федеральное государственное бюджетное образовательное учреждение высшего образования «Калининградский государственный технический университет», 2025 г.
© Подтопельный В. В., 2025 г.

ОГЛАВЛЕНИЕ

Введение……4
1. Тематический план……6
2. Содержание дисциплины и указания к изучению……11
3. Методические рекомендации по подготовке к лабораторным занятиям……...60
4. Методические указания по самостоятельной работе……..61
5. Методические указания по курсовому проекту……..64
6. Требования к аттестации по дисциплине…….68
Примерные вопросы к зачету/экзамену по дисциплине…….71
Заключение……..73
Литература……...74

ВВЕДЕНИЕ

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

Цель изучения дисциплины: приобретение студентами навыков выявлять уязвимости и противодействовать сетевым атакам на распределенные системы**.**

Цели соответствуют компетенциям:

ОПК-12: Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем;

ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем.

В результате освоения дисциплины обучающийся должен:

знать:

– способы реализации угроз безопасности в вычислительных сетях;

– основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в вычислительных сетях;

– способы реализации угроз безопасности в вычислительных сетях;

– способы реализации угроз безопасности в автоматизированных системах;

– программно-аппаратные средства обеспечения защиты информации автоматизированных систем;

уметь:

– реализовывать определение комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты вычислительных сетей;

– классифицировать и оценивать угрозы безопасности информации для автоматизированной системы;

– анализировать возможные уязвимости информационных систем; выявлять известные уязвимости информационных систем;

владеть:

– навыком определения комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты информации автоматизированных систем;

– навыком выявлять уязвимости информационно технологических ресурсов автоматизированных систем;

– навыком проведения оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах;

– навыком определения оценки возможностей внешних и внутренних нарушителей.

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествуют «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 потребуется 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 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

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 самостоя-тельной работы, ч
		Лекции (6-й семестр – 32 ч ауд.)		
1.1	Сетевые угрозы	Тема 1. Принципы многоуровневой защиты корпоративной информации. Основы сетевого и межсетевого взаимодействия	8	15
1.2	Сетевые угрозы	Тема 1.2 Политика безопасности. Структура политики безопасности	4	15
1.3	Сетевые угрозы	Тема 1.3 Симметричные и ассиметричные системы шифрования. Функции хеширования. Электронная подпись	8	
1.4	Сетевые угрозы	Тема 1.4 Идентификация, аутентификация и управление доступом	4	
2.1	Защита от сетевых угроз	Тема 2.1 Доменные службы Active Directory. Структуры леса, доменных деревьев. Проектирование отношений и оптимизация аутентификации внутри леса	6	
2.2	Защита от сетевых угроз	Тема 2.2 Корпоративная информационная система. Сети периметра и стратегии удаленного доступа	2	7,85
		Всего за семестр:	32	37,85
		Лекции (7-й семестр – 48 ч ауд.)		

2.3	Защита от сетевых угроз	Тема 2.3 Обеспечение безопасности операционных систем. Локальные политики безопасности. Встроенные системы защиты операционных систем. Модель взаимодействия систем. Стек протоколов TCP/IP	10	10
2.4	Защита от сетевых угроз	Тема 2.4 Защита на канальном уровне – протоколы удаленного доступа	10	10
2.5	Защита от сетевых угроз	Тема 2.5 Протоколы IPSec, SSL, TSL, SOCKS. Защита на сетевом и сеансовом уровнях	10	10
2.6	Защита от сетевых угроз	Тема 2.6 Функционирование межсетевых экранов на различных уровнях модели OSI	10	10
2.7	Защита от сетевых угроз	Тема 2.7 Виртуальные частные сети	8	30
		Всего за семестр:	48	70
		Итого за курс	80	107,85

		лабораторные занятия (6-й семестр 32 ч)		
1	Сетевые угрозы	Аудит безопасности протокола SNMP	6	-
2	Сетевые угрозы	Аудит безопасности протокола STP	6	-
3	Сетевые угрозы	Виртуальные локальные сети IEEE 802.1	6	-
4	Сетевые угрозы	Базовые механизмы безопасности коммутаторов	6	-
5	Сетевые угрозы	Безопасность на основе сегментации трафика	6	-
6	Сетевые угрозы	Безопасность на основе протокола IEEE 802.1x	2	-

		Всего за семестр:	32	

		Лабораторные занятия (7-й семестр 48 ч)		
7	Сетевые угрозы	Списки контроля доступа ACL	8	-
8	Сетевые угрозы	Контроль доступа к коммутатору	8	-
9	Защита от сетевых угроз	Шифрование канала с использованием протокола WEP	8	-
10	Защита от сетевых угроз	Шифрование канала с использованием протокола WEP	8	-
11	Защита от сетевых угроз	Аутентификация беспроводных клиентов на основе учѐтных записей пользователей и аппаратных адресов компьютеров	8	-
12	Защита от сетевых угроз	Протокол PPPoE Технология Network Address Translation. Виртуальные частные сети	8	-
		Всего за семестр:	**48**	
		Итого за курс	160	

	Курсовая проект (7-й семестр)		
Название первого раздела	Контрольная точка 1. Раздел проекта 1	10,0	-
Название третьего раздела	Контрольная точка 2. Раздел проекта 2	24,75	-
	Оформление проекта. Защита	-	-
		34,75	**0**

Название второго раздела	Контроль 1 (не предусмотрен)	-	-
Название третьего раздела	Контроль 2 (не предусмотрен)	-	-
	Итоговый контроль (зачет)		
	Итоговый контроль (экзамен)		
		0	**0**
	КА	5,4	
	РЭ	16	
	Всего	**216,15**	**107,85**
	ИТОГО: 324		

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

2.1 Раздел 1. Сетевые угрозы

2.1.1 Тема 1. Принципы многоуровневой защиты корпоративной информации. Основы сетевого и межсетевого взаимодействия

Перечень изучаемых вопросов

1. Многоуровневая защита в сетевой безопасности.
2. Модель OSI и ее связь с сетевой безопасностью.
3. Безопасность межсетевого взаимодействия.
4. Управление сетевыми рисками.

Методические указания к изучению

1. Многоуровневая защита в сетевой безопасности

Многоуровневая защита, или Defense-in-Depth, представляет собой стратегический подход к обеспечению безопасности компьютерных сетей, при котором защитные механизмы распределяются по нескольким уровням, создавая серию барьеров для злоумышленников. Этот подход основан на понимании, что ни один защитный механизм не может быть абсолютно надежным, поэтому безопасность достигается за счет комбинации различных мер, работающих на физическом, сетевом, хостовом и прикладном уровнях. На физическом уровне защита включает ограничение доступа к сетевому оборудованию, например, размещение серверов в защищенных дата-центрах с биометрическим контролем доступа. Это предотвращает физическое вмешательство, такое как подключение злоумышленников к сетевым портам или кража оборудования. На сетевом уровне применяются межсетевые экраны и системы обнаружения и предотвращения вторжений (IDS/IPS), которые фильтруют входящий и исходящий трафик, выявляя аномалии, такие как попытки эксплуатации уязвимостей протоколов. Хостовый уровень предполагает использование антивирусных программ, регулярное обновление операционных систем и настройку политик безопасности, чтобы минимизировать уязвимости отдельных устройств. На прикладном уровне защита включает шифрование данных, управление доступом к приложениям и защиту от атак, таких как SQL-инъекции или XSS (межсайтовый скриптинг).

Особое значение многоуровневая защита приобретает при противодействии сложным атакам, таким как распределенные атаки типа «отказ в обслуживании» (DDoS). Эти атаки направлены на перегрузку сетевых ресурсов, что может привести к недоступности критически важных сервисов, таких как веб-сайты или корпоративные приложения. Многоуровневая защита

позволяет смягчить такие угрозы: межсетевые экраны ограничивают объем входящего трафика, системы IDS/IPS анализируют его на предмет аномалий, а облачные решения, такие как CDN (Content Delivery Network), распределяют нагрузку, предотвращая перегрузку серверов. Если один уровень защиты оказывается скомпрометирован, другие продолжают функционировать, обеспечивая резервирование. Например, даже если злоумышленник обходит сетевой файрвол, антивирус на хосте может заблокировать вредоносное ПО, а шифрование данных предотвратит их компрометацию. Такой подход минимизирует вероятность успешной атаки и снижает потенциальный ущерб, делая многоуровневую защиту краеугольным камнем сетевой безопасности. Вопрос о том, как этот подход предотвращает DDoS-атаки, подчеркивает его способность комбинировать различные технологии для обеспечения устойчивости сети, что особенно важно в условиях, когда атаки становятся все более изощренными.

2. Модель OSI и ее связь с сетевой безопасностью

Модель OSI (Open Systems Interconnection) является фундаментальным инструментом для понимания процессов передачи данных в компьютерных сетях и их защиты. Эта модель делит сетевые процессы на семь уровней – физический, канальный, сетевой, транспортный, сеансовый, представительный и прикладной, – каждый из которых имеет свои функции, уязвимости и методы защиты. Понимание этих уровней позволяет сетевым администраторам систематически анализировать угрозы и разрабатывать целенаправленные меры защиты, что делает модель OSI неотъемлемой частью проектирования безопасных сетей.

На физическом уровне, где данные передаются в виде электрических или оптических сигналов, угрозы включают в себя перехват сигналов или физическое вмешательство в кабели. Для защиты используются экранированные кабели, защищённые каналы связи и физическая охрана оборудования. Канальный уровень, отвечающий за передачу данных в пределах одной сети, уязвим для атак типа ARP-спуфинга, при которых злоумышленник подменяет MAC-адреса, чтобы перехватывать или перенаправлять трафик. Для предотвращения таких атак используются такие технологии, как динамическая проверка ARP или сегментация сети с помощью виртуальных локальных сетей (VLAN), которые изолируют трафик между группами устройств. На сетевом уровне, где происходит маршрутизация пакетов, основной угрозой является IP-спуфинг, когда злоумышленник подменяет IP-адреса для обхода фильтров или проведения атак. Защита включает настройку списков контроля доступа (ACL) на маршрутизаторах и использование протоколов, устойчивых к подделке, таких как BGP с RPKI. Транспортный уровень, обеспечивающий надежную доставку данных, подвержен атакам типа SYN-флуд, которые перегружают серверы

ложными запросами на соединение. Здесь используются межсетевые экраны с функцией отслеживания состояния соединений и ограничением количества запросов.

Высшие уровни модели OSI, такие как сеансовый, представительный и прикладной, также имеют свои уязвимости. Например, на прикладном уровне атаки, такие как фишинг или SQL-инъекции, нацелены на веб-приложения или пользовательские данные. Для защиты используются веб-файрволы (WAF) и шифрование данных, например, с помощью TLS. Понимание модели OSI позволяет администраторам точно определять, на каком уровне возникают угрозы, и внедрять соответствующие меры защиты. Например, для предотвращения атак на канальном уровне можно использовать аутентификацию устройств, а для защиты сетевого уровня – шифрование трафика через VPN. Таким образом, модель OSI выступает в качестве карты, которая направляет усилия по обеспечению сетевой безопасности, помогая проектировать системы, устойчивые к широкому спектру атак. Вопрос о том, как знание модели OSI помогает проектировать безопасные сети, подчеркивает ее роль в систематизации подходов к защите, что позволяет эффективно распределять ресурсы и минимизировать уязвимости.

3. Безопасность межсетевого взаимодействия

Межсетевое взаимодействие, обеспечивающее связь между различными сетями, является ключевым компонентом корпоративной инфраструктуры, но оно также создает значительные риски для сетевой безопасности. Протоколы маршрутизации, такие как OSPF (Open Shortest Path First) и BGP (Border Gateway Protocol), играют центральную роль в передаче данных между сетями, но их уязвимости могут быть использованы для серьезных атак. Например, атака типа BGP-перехвата позволяет злоумышленникам перенаправлять трафик через подконтрольные им маршрутизаторы, что может привести к перехвату данных, нарушению доступности сервисов или даже внедрению вредоносного кода. Для защиты от таких угроз используются механизмы аутентификации маршрутизаторов, такие как пароли или цифровые подписи, а также стандарты, например, RPKI, которые подтверждают легитимность объявлений о маршрутах. Эти меры обеспечивают целостность маршрутизации, предотвращая несанкционированные изменения в таблицах маршрутов.

Еще одним важным инструментом для обеспечения безопасности межсетевого взаимодействия является использование виртуальных частных сетей (VPN) на основе протокола IPSec. IPSec обеспечивает шифрование и аутентификацию данных, передаваемых между сетями, что особенно важно для компаний с географически распределенными офисами. Например, филиалы могут обмениваться конфиденциальной информацией через зашифрованные туннели, защищенные от перехвата. Однако безопасность

VPN зависит от правильной настройки, включая выбор надежных алгоритмов шифрования, таких как AES-256, и регулярное обновление ключей. Слабые ключи или устаревшие протоколы, такие как PPTP, могут стать уязвимостью, позволяющей злоумышленникам расшифровать трафик или получить доступ к сети.

Наиболее критичные угрозы межсетевого взаимодействия включают в себя не только технические атаки, такие как перехват BGP, но и организационные недочёты, например, отсутствие мониторинга сетевых устройств или недостаточная защита маршрутизаторов. Для минимизации этих рисков необходимо внедрять системы мониторинга, такие как NetFlow или SNMP, которые отслеживают аномалии в трафике, а также проводить регулярные проверки конфигурации сетевого оборудования. Обеспечение целостности и конфиденциальности межсетевого трафика требует комплексного подхода, включающего шифрование, аутентификацию и постоянный контроль. Только такой подход позволяет гарантировать надежность связи между сетями и минимизировать риски, связанные с нарушением межсетевого взаимодействия.

4. Управление сетевыми рисками

Управление сетевыми рисками является неотъемлемой частью стратегии сетевой безопасности, поскольку позволяет организациям систематически выявлять, оценивать и устранять угрозы, которые могут поставить под удар корпоративную инфраструктуру. Основные категории сетевых рисков включают перехват данных, несанкционированный доступ, атаки с использованием программ-вымогателей и фишинг, а также внутренние угрозы, связанные с действиями сотрудников. Для эффективного управления этими рисками применяются такие стандарты, как ISO/IEC 27001, которые обеспечивают структурированный подход к управлению информационной безопасностью. Этот стандарт помогает организациям проводить аудит сетевой инфраструктуры, выявлять уязвимости и разрабатывать стратегии по их устранению.

Процесс управления рисками начинается с идентификации активов, таких как маршрутизаторы, серверы, базы данных и сетевые приложения, которые могут стать мишенью для атак. Например, устаревшее программное обеспечение на маршрутизаторе может стать точкой входа для злоумышленников, что требует своевременного обновления прошивки. Далее проводится анализ угроз, включая их вероятность и потенциальный ущерб. Например, DDoS-атака может привести к недоступности критически важных сервисов, а перехват данных – к утечке конфиденциальной информации. На основе этого анализа разрабатываются меры защиты, такие как установка межсетевых экранов, внедрение систем обнаружения вторжений или обучение сотрудников основам кибербезопасности для предотвращения фишинга.

Управление сетевыми рисками – это не разовое мероприятие, а непрерывный процесс, включающий мониторинг сети и реагирование на инциденты. Такие инструменты, как SIEM (система управления информацией и событиями безопасности), позволяют анализировать сетевой трафик в режиме реального времени и выявлять подозрительную активность, например, попытки брутфорса или аномальные объемы трафика. Например, SIEM может обнаружить несанкционированные попытки доступа к серверу и инициировать автоматическую блокировку IP-адреса атакующего. Такой подход позволяет организациям определять приоритетность защитных мер, эффективно распределять ресурсы и минимизировать вероятность успешных атак. Вопрос о том, как управление рисками влияет на конфигурацию защитных систем, подчеркивает его роль в адаптации сетевой безопасности к конкретным угрозам и условиям, обеспечивая устойчивость инфраструктуры.

Многоуровневая защита, модель OSI, безопасность межсетевого взаимодействия и управление сетевыми рисками составляют основу для построения безопасных компьютерных сетей. Многоуровневая защита создает ряд барьеров, минимизирующих вероятность успешных атак, таких как DDoS. Модель OSI предоставляет структурированный подход к анализу уязвимостей и выбору защитных мер на каждом уровне сетевого взаимодействия. Безопасность межсетевого взаимодействия обеспечивает надежность и конфиденциальность передачи данных между сетями, защищая от таких угроз, как перехват BGP. Управление сетевыми рисками позволяет организациям систематически выявлять и устранять угрозы, адаптируя защитные меры к текущему ландшафту киберугроз. В совокупности эти элементы формируют целостную стратегию, которая защищает корпоративные сети от современных вызовов кибербезопасности, обеспечивая устойчивость и надежность в условиях постоянно развивающихся угроз.

Литература

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 1).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 1–4).

3. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 1).

4. Безопасность беспроводных локальных сетей: учеб. пособие / М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг, К. А. Ахрамеева. – Санкт-Петербург: СПбГУТ им. М. А. Бонч-Бруевича, 2021. – 71 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/279623 (дата обращения: 06.12.2024). – ISBN 978-5-89160-227-4. – Текст : электронный (гл. 1–4).

Контрольные вопросы

1. Основные положения для планирования безопасности сети.
2. Функции уровней защиты.
3. Происхождение угроз.
4. Основные причины утечки информации.
5. Виды утечек информации.

2.1.2 Политика безопасности. Структура политики безопасности

Перечень изучаемых вопросов

1. Роль политики безопасности в защите сетей
2. Компоненты сетевой политики безопасности
3. Разработка политики для сетевой инфраструктуры
4. Контроль и аудит сетевой политики

Методические указания к изучению

1. Роль политики безопасности в защите сетей

Политика безопасности играет центральную роль в обеспечении защиты компьютерных сетей, выступая в качестве руководства, которое стандартизирует подходы к управлению сетевыми ресурсами и данными. Этот документ определяет, как организация должна защищать свои сети от угроз, таких как хакерские атаки, вредоносное ПО или внутренние нарушения. Без четкой политики действия сотрудников и администраторов могут быть несогласованными, что увеличивает вероятность ошибок, таких как неправильная настройка сетевого оборудования или игнорирование угроз.

Например, политика может включать правила фильтрации трафика, которые требуют от межсетевых экранов блокировать подозрительные соединения, или политики удаленного доступа, которые определяют, как сотрудники подключаются к корпоративной сети через VPN. Эти правила помогают предотвратить инциденты, такие как DDoS-атаки или перехват данных, обеспечивая единый подход к защите.

Политика безопасности также способствует созданию культуры осведомленности о кибербезопасности в организации. Она устанавливает ожидания для пользователей, включая требования к использованию сложных паролей, ограничения на подключение личных устройств к сети и процедуры реагирования на инциденты. Например, политика может требовать от сотрудников немедленного уведомления ИТ-отдела о подозрительных электронных письмах, чтобы предотвратить фишинговые атаки, которые часто используются для получения доступа к сети. Стандартизация мер защиты через политику безопасности позволяет минимизировать риски, связанные с человеческим фактором, и обеспечивает согласованность действий в условиях сложных атак. Вопрос о том, почему политика безопасности критически важна для сетевой инфраструктуры, подчеркивает ее роль в создании структурированного подхода, который объединяет технические, организационные и человеческие аспекты защиты, обеспечивая устойчивость сети к внешним и внутренним угрозам.

2. Компоненты сетевой политики безопасности

Эффективная политика безопасности для компьютерных сетей включает набор ключевых компонентов, которые обеспечивают единые стандарты защиты и управления сетевыми ресурсами. Одним из центральных элементов является классификация сетевых данных, которая определяет, какие данные являются конфиденциальными, критически важными или общедоступными. Например, финансовая информация или персональные данные клиентов требуют строгой защиты, такой как шифрование и ограниченный доступ, в то время как публичные данные, такие как корпоративный веб-сайт, могут быть менее защищенными. Эта классификация позволяет администраторам приоритизировать ресурсы и применять соответствующие меры защиты, такие как настройка межсетевых экранов для фильтрации трафика, связанного с конфиденциальными данными.

Еще одним важным компонентом являются правила доступа, которые определяют, кто и как может взаимодействовать с сетевыми ресурсами. Например, политика может требовать, чтобы доступ к серверам баз данных был ограничен определенными IP-адресами или ролями, такими как администраторы баз данных, с использованием двухфакторной аутентификации (2FA). Правила доступа также могут включать настройку

VPN для удаленных сотрудников, обеспечивая безопасное подключение к сети. Мониторинг сетевого трафика является еще одним критическим элементом, который позволяет выявлять подозрительные активности, такие как необычно высокий объем данных или попытки несанкционированного доступа. Например, политика может предписывать использование систем управления безопасностью информации (SIEM) для анализа логов межсетевых экранов, что помогает обнаружить атаки в реальном времени.

Эти компоненты работают вместе, создавая единые стандарты защиты, которые обеспечивают согласованность и предсказуемость в управлении сетевой безопасностью. Без таких стандартов организация рискует столкнуться с хаотичным подходом, когда разные отделы применяют противоречивые меры защиты, что может привести к уязвимостям. Вопрос о том, какие компоненты политики наиболее важны для сетевой безопасности, подчеркивает необходимость баланса между классификацией данных, строгим контролем доступа и мониторингом, которые в совокупности создают надежную защиту от современных киберугроз.

3. Разработка политики для сетевой инфраструктуры

Разработка политики безопасности для сетевой инфраструктуры – это сложный процесс, который требует учета специфических угроз, архитектуры сети и потребностей организации. Этот процесс начинается с анализа сетевых угроз, который включает идентификацию потенциальных рисков, таких как перехват данных, DDoS-атаки или внутренние нарушения. Например, если организация использует беспроводные сети, анализ может выявить угрозы, связанные с атаками на Wi-Fi, такими как Evil Twin, что требует внедрения протоколов WPA3 и аутентификации пользователей. На основе анализа угроз определяются требования к политике, включая технические меры (например, настройка межсетевых экранов для DMZ) и организационные меры (например, обучение сотрудников).

Следующий этап – согласование политики с заинтересованными сторонами, включая ИТ-отдел, руководство и юридическую службу. Это гарантирует, что политика соответствует бизнес-целям и нормативным требованиям, таким как GDPR или локальные законы о защите данных. Например, политика для защиты демилитаризованной зоны (DMZ) может включать правила, ограничивающие доступ к публичным серверам, таким как веб-сайты, и требовать использования веб-файрволов (WAF) для защиты от атак на прикладном уровне. Важно, чтобы политика была адаптирована к архитектуре сети: для распределенных сетей с филиалами могут потребоваться правила для безопасного VPN-доступа, тогда как для локальной сети акцент может быть сделан на сегментацию с помощью VLAN.

Адаптация политики к сетевым рискам и архитектуре позволяет минимизировать уязвимости, такие как неправильная настройка оборудования или недостаточная защита критических систем. Например, политика для Wi-Fi-сетей может требовать регулярного обновления ключей шифрования и мониторинга подключенных устройств, чтобы предотвратить несанкционированный доступ. Вопрос о том, как разработать политику, минимизирующую сетевые уязвимости, подчеркивает важность системного подхода, который сочетает анализ угроз, техническую адаптацию и согласование с бизнес-процессами, обеспечивая защиту сети от текущих и будущих угроз.

4. Контроль и аудит сетевой политики

Контроль и аудит политики безопасности являются критически важными для обеспечения ее эффективности и актуальности в условиях постоянно меняющегося ландшафта киберугроз. Контроль предполагает мониторинг сетевого трафика и активности пользователей для выявления нарушений политики, таких как попытки несанкционированного доступа или неправильная настройка сетевых устройств. Например, системы управления безопасностью информации (SIEM) могут анализировать логи межсетевых экранов, обнаруживая аномалии, такие как необычно высокий объем исходящего трафика, который может указывать на утечку данных. Такой мониторинг позволяет в реальном времени реагировать на инциденты, минимизируя их последствия.

Аудит политики включает регулярную проверку ее соответствия текущим угрозам и требованиям организации. Это может включать тестирование безопасности, такое как пентестинг, для выявления уязвимостей в сетевой инфраструктуре, или анализ логов для проверки соблюдения правил доступа. Например, аудит может показать, что сотрудники используют слабые пароли, что требует ужесточения политики паролей. Аудит также помогает обновлять политику в ответ на новые угрозы, такие как появление новых видов вредоносного ПО или изменения в нормативных требованиях. Использование SIEM-систем для аудита позволяет автоматизировать сбор и анализ данных, упрощая выявление нарушений, таких как несанкционированные попытки подключения к VPN.

Контроль и аудит обеспечивают соблюдение политики и выявление инцидентов, что является ключевым элементом сетевой безопасности. Без регулярной проверки политика может устареть, оставляя сеть уязвимой для новых атак. Например, если политика не предусматривает мониторинг новых устройств в сети, злоумышленник может подключить компрометированное устройство, не будучи обнаруженным. Вопрос о том, как контроль и аудит

способствуют выявлению инцидентов, подчеркивает их роль в поддержании актуальности политики и обеспечении устойчивости сети к киберугрозам.

Политика безопасности является краеугольным камнем защиты компьютерных сетей, обеспечивая стандартизацию мер защиты, управление доступом и мониторинг сетевой активности. Ее роль заключается в создании единого руководства, которое минимизирует риски за счет согласованных действий сотрудников и администраторов. Компоненты политики, такие как классификация данных, правила доступа и мониторинг трафика, создают единые стандарты, необходимые для защиты сетевых ресурсов. Разработка политики требует тщательного анализа угроз и адаптации к архитектуре сети, чтобы минимизировать уязвимости. Контроль и аудит обеспечивают ее актуальность, позволяя выявлять инциденты и реагировать на них. В совокупности эти элементы формируют надежную стратегию сетевой безопасности, способную противостоять современным киберугрозам и обеспечивать устойчивость корпоративной инфраструктуры.

Литература

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст : электронный (гл. 1).

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL:

https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 2).

Контрольные вопросы

1. Почему политика безопасности считается критически важным элементом для защиты компьютерных сетей?
2. Как классификация сетевых данных влияет на разработку политики безопасности?
3. Какие компоненты политики безопасности наиболее важны для предотвращения несанкционированного доступа к сети?
4. Как процесс анализа сетевых угроз влияет на разработку политики безопасности?
5. Как адаптировать политику безопасности к архитектуре распределенной сети?
6. Какую роль играют SIEM-системы в контроле и аудите сетевой политики безопасности?
7. Как обеспечить актуальность политики безопасности в условиях эволюции киберугроз?

2.1.3 Тема 1.3 Симметричные и ассиметричные системы шифрования. Функции хеширования. Электронная подпись

Перечень изучаемых вопросов

1. Симметричное шифрование для сетевой безопасности.
2. Асимметричное шифрование в сетях.
3. Функции хеширования для обеспечения сетевой целостности.
4. Электронная подпись в сетевых взаимодействиях.

Методические указания к изучению

1. Симметричное шифрование для сетевой безопасности

Симметричное шифрование – это криптографический метод, при котором один и тот же ключ используется как для шифрования, так и для расшифровки данных. Этот подход, реализованный в таких алгоритмах, как AES (стандарт расширенного шифрования) и устаревший DES (стандарт шифрования данных), отличается высокой скоростью и эффективностью, что делает его идеальным для защиты больших объёмов сетевого трафика. В корпоративных сетях симметричное шифрование широко применяется для обеспечения конфиденциальности данных, передаваемых через виртуальные

частные сети (VPN) или локальные сети. Например, при использовании протокола IPSec для создания VPN-туннеля между филиалами компании данные шифруются с помощью AES, что предотвращает их перехват злоумышленниками, даже если трафик проходит через незащищенные каналы, такие как Интернет. В локальных сетях симметричное шифрование может защищать данные, хранящиеся на сетевых дисках, предотвращая доступ к ним в случае компрометации физического носителя.

Эффективность симметричного шифрования обусловлена его способностью быстро обрабатывать данные, что критически важно для приложений, требующих высокой пропускной способности, таких как потоковая передача данных или голосовая связь. Однако этот метод требует безопасного обмена ключами между сторонами, что может быть уязвимостью в сетевой среде, если ключи передаются по незащищённым каналам. Для решения этой проблемы симметричное шифрование часто комбинируется с асимметричными методами для безопасной передачи ключей. Роль симметричного шифрования в сетевой безопасности заключается в обеспечении конфиденциальности данных, передаваемых по сети, что предотвращает их компрометацию в случае перехвата. Например, в корпоративной сети, использующей Wi-Fi, шифрование трафика с помощью AES, реализованное в протоколе WPA3, защищает данные от атак, таких как перехват пакетов в беспроводной среде. Вопрос о том, как симметричное шифрование защищает сетевой трафик, подчеркивает его незаменимость в обеспечении быстрой и надежной защиты данных, что является основой для безопасной передачи информации в сетях.

2. Асимметричное шифрование в сетях

Асимметричное шифрование, в отличие от симметричного, использует пару ключей – открытый и закрытый, – что делает его мощным инструментом для обеспечения безопасности сетевых взаимодействий. Открытый ключ доступен всем и используется для шифрования данных, тогда как закрытый ключ, известный только владельцу, применяется для их расшифровки. Этот подход, реализованный в таких алгоритмах, как RSA и ECC (криптография на эллиптических кривых), позволяет безопасно обмениваться данными даже в незащищённых сетях, таких как Интернет. В сетевой безопасности асимметричное шифрование играет ключевую роль в двух аспектах: защита от перехвата ключей и аутентификация сторон. Например, в протоколе HTTPS, используемом для защиты веб-трафика, асимметричное шифрование применяется на этапе установления соединения, когда клиент и сервер обмениваются ключами для последующего симметричного шифрования TLS-сессии. Это гарантирует, что даже если злоумышленник перехватит трафик, он не сможет расшифровать данные без закрытого ключа.

Асимметричное шифрование также широко используется для аутентификации в сетевых протоколах, таких как SSH, где сервер и клиент используют ключи для подтверждения подлинности друг друга. Это предотвращает атаки, при которых злоумышленник пытается выдать себя за легитимную сторону. Например, в корпоративной сети администратор может подключиться к серверу через SSH, используя пару ключей для безопасного управления, что исключает риск перехвата учётных данных. Однако асимметричное шифрование менее эффективно по сравнению с симметричным из-за высокой вычислительной сложности, поэтому его часто применяют на начальных этапах соединения или для небольших объёмов данных. Роль асимметричного шифрования в сетевой безопасности заключается в обеспечении безопасного обмена ключами и аутентификации, что делает его незаменимым для защиты от атак типа «человек посередине» (MitM). Вопрос о том, как асимметричное шифрование повышает безопасность сетей, подчеркивает его способность создавать доверительные и защищенные соединения в условиях, когда стороны не имеют предварительно согласованных ключей.

3. Функции хеширования для обеспечения сетевой целостности

Функции хеширования представляют собой криптографический инструмент, который преобразует данные произвольной длины в строку фиксированной длины, называемую хешем, обеспечивая проверку целостности данных при сетевом взаимодействии. Такие алгоритмы, как SHA-256 и устаревший MD5, создают уникальный «отпечаток» данных, который изменяется при любом, даже минимальном, изменении исходного содержимого. В контексте сетевой безопасности функции хеширования играют ключевую роль в предотвращении подделки данных, обеспечивая уверенность в том, что передаваемая информация не была изменена злоумышленником. Например, в сетевых протоколах, таких как Kerberos, хеширование используется для проверки целостности сообщений аутентификации, гарантируя, что данные не были подделаны в процессе передачи. Аналогичным образом при передаче файлов по сети хеш-функции позволяют проверить, что загруженный файл идентичен оригиналу, защищая от внедрения вредоносного кода.

Одним из распространённых применений хеширования в сетях является защита паролей. Вместо хранения паролей в открытом виде сетевые системы, такие как серверы аутентификации, хранят их хеши, созданные с помощью SHA-256 или bcrypt. Это предотвращает компрометацию учётных данных в случае утечки базы данных. Однако хеширование не обеспечивает конфиденциальность, поскольку хеш-функции необратимы, но не защищают данные от перехвата. Уязвимости, такие как атаки на слабые алгоритмы (например, MD5), подчеркивают важность выбора надежных хеш-функций.

Роль хеш-функций в сетевой безопасности заключается в предотвращении подделки данных, что критически важно для защиты целостности сетевых транзакций и аутентификационных данных. Вопрос о том, как хеширование защищает от атак на сетевую целостность, подчеркивает его способность выявлять любые изменения в данных, обеспечивая доверие к сетевым взаимодействиям.

4. Электронная подпись в сетевых взаимодействиях

Электронная подпись – это криптографический механизм, который сочетает в себе асимметричное шифрование и хеширование для обеспечения подлинности и целостности сообщений в сетевых взаимодействиях. Она создается путем хеширования сообщения и шифрования хеша с использованием закрытого ключа отправителя. Получатель может проверить подпись, расшифровав хеш с помощью открытого ключа и сравнив его с хешем полученного сообщения. Этот процесс гарантирует, что сообщение не было изменено и действительно отправлено указанным лицом. В сетевой безопасности электронная подпись широко применяется в таких протоколах, как TLS, где цифровые сертификаты, содержащие подписи, подтверждают подлинность веб-серверов. Например, при подключении к сайту через HTTPS браузер проверяет подпись сертификата, чтобы убедиться в легитимности сервера, предотвращая атаки MitM.

Электронная подпись также используется для защиты сетевых транзакций, таких как электронные платежи или обмен конфиденциальными документами. Например, в корпоративной сети подпись может применяться для аутентификации сообщений, отправляемых между серверами, или для подтверждения легитимности обновлений программного обеспечения. Это обеспечивает доверие в сетевых взаимодействиях, особенно в распределённых системах, где стороны могут не иметь прямого контакта. Однако безопасность электронной подписи зависит от защиты закрытого ключа: его компрометация позволяет злоумышленнику подделывать подписи. Роль электронной подписи в сетевой безопасности заключается в создании доверительной среды, в которой участники могут быть уверены в подлинности и целостности данных. Вопрос о том, как электронная подпись предотвращает атаки MitM, подчеркивает ее способность аутентифицировать стороны и защищать сетевые взаимодействия от подделок.

Криптографические методы, такие как симметричное и асимметричное шифрование, функции хеширования и электронная подпись, составляют основу безопасности компьютерных сетей, обеспечивая конфиденциальность, целостность и подлинность данных. Симметричное шифрование защищает сетевой трафик, обеспечивая быструю и надежную конфиденциальность, как в случае с VPN или Wi-Fi. Асимметричное шифрование создает безопасные каналы для обмена ключами и аутентификации, поддерживая такие

протоколы, как HTTPS и SSH. Функции хеширования гарантируют целостность данных, предотвращая их подделку в сетевых протоколах. Электронная подпись обеспечивает доверие, защищая от атак MitM и подтверждая подлинность сообщений. В совокупности эти методы формируют комплексный подход к защите сетей, позволяя организациям противостоять современным киберугрозам и обеспечивать надежность сетевых взаимодействий.

Литература

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст : электронный (гл. 1).

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 2).

Контрольные вопросы

1. Функционирование сканирование карты сети.
2. Принципы SYN-бомбардировки.
3. Приведите порядок реализации спуфинга.

2.1.4 Тема 1.4 Идентификация, аутентификация и управление доступом

Перечень изучаемых вопросов

1. Идентификация в сетевой безопасности.
2. Аутентификация для защиты сетей.
3. Управление доступом в сетях.
4. Мониторинг сетевого доступа.

Методические указания к изучению

1. Идентификация в сетевой безопасности

Идентификация является первым шагом в обеспечении безопасного доступа к сетевым ресурсам, поскольку она позволяет установить, кто или что пытается получить доступ к сети. Этот процесс заключается в присвоении уникального идентификатора пользователю, устройству или процессу, чтобы сеть могла их распознать. В сетевой безопасности идентификаторы могут принимать различные формы, такие как имена пользователей, MAC-адреса устройств или цифровые сертификаты. Например, в корпоративной сети MAC-адреса используются для фильтрации устройств, разрешая подключение только зарегистрированным устройствам, что предотвращает подключение несанкционированных гаджетов к Wi-Fi или локальной сети. Аналогично, цифровые сертификаты применяются в VPN-соединениях для идентификации удаленных устройств, гарантируя, что только доверенные клиенты могут подключиться к корпоративной сети.

Идентификация играет ключевую роль в сетевой безопасности, поскольку она создает основу для последующей аутентификации и контроля доступа. Без четкого определения личности или устройства невозможно определить, кому следует предоставить доступ, а кому – отказать. Например, в сетях с сетевым контролем доступа (NAC) идентификация устройств по MAC-адресам или сертификатам позволяет автоматически изолировать неизвестные устройства, предотвращая потенциальные угрозы, такие как подключение скомпрометированного ноутбука. Этот процесс также помогает в отслеживании активности в сети, что важно для обнаружения аномалий. Однако идентификация сама по себе не обеспечивает защиты, так как злоумышленник может подделать идентификатор, например, через спуфинг MAC-адресов. Поэтому она должна сочетаться с надежной аутентификацией. Вопрос о том, как идентификация защищает сетевые ресурсы, подчеркивает ее роль как первого барьера, который предотвращает несанкционированный доступ и создает основу для дальнейших мер безопасности.

2. Аутентификация для защиты сетей

Аутентификация следует за идентификацией и направлена на подтверждение подлинности заявленного идентификатора, чтобы убедиться, что пользователь или устройство действительно являются теми, за кого себя выдают. В сетевой безопасности аутентификация может осуществляться различными методами, включая пароли, биометрические данные, такие как отпечатки пальцев, или аппаратные токены. Одним из наиболее эффективных подходов является двухфакторная аутентификация (2FA), которая сочетает два независимых фактора, например, пароль и одноразовый код, отправленный на мобильное устройство. Например, в корпоративных Wi-Fi-сетях протокол RADIUS (Remote Authentication Dial-In User Service) используется для централизованной аутентификации пользователей, требуя ввода учетных данных и дополнительного фактора, такого как код из приложения-аутентификатора. Это значительно повышает защиту от атак, таких как кража паролей через фишинг.

Аутентификация критически важна для сетевой безопасности, поскольку она предотвращает несанкционированный доступ к ресурсам, даже если злоумышленник знает идентификатор пользователя. Например, в случае компрометации пароля 2FA может остановить атакующего, требуя второй фактор, который сложнее получить. В сетевых системах, таких как VPN или SSH, аутентификация часто сочетает пароли с сертификатами или биометрией, чтобы обеспечить надежную защиту. Однако слабые методы аутентификации, такие как простые пароли, могут стать уязвимостью, особенно если они не обновляются регулярно или подвергаются брутфорс-атакам. Роль аутентификации в сетевой безопасности заключается в подтверждении подлинности пользователей и устройств, что предотвращает проникновение злоумышленников в сеть. Вопрос о том, почему двухфакторная аутентификация важна для сетевой безопасности, подчеркивает ее способность создавать дополнительный уровень защиты, снижая риски, связанные с человеческим фактором и кражей учетных данных.

3. Управление доступом в сетях

Управление доступом определяет, какие ресурсы сети доступны для идентифицированных и аутентифицированных пользователей или устройств, и в каком объеме. Этот процесс основывается на моделях, таких как ролевое управление доступом (RBAC), списки контроля доступа (ACL) и подход Zero Trust. RBAC назначает права доступа на основе ролей пользователей, например, администраторы сети могут настраивать маршрутизаторы, тогда как обычные сотрудники имеют доступ только к общим ресурсам. ACL, используемые на маршрутизаторах и межсетевых экранах, ограничивают трафик на основе IP-адресов, портов или протоколов, например, блокируя доступ к серверам в демилитаризованной зоне (DMZ) для внешних пользователей. Подход Zero Trust, набирающий популярность, требует

проверки каждого запроса на доступ, независимо от того, исходит ли он из внутренней или внешней сети, что минимизирует риски внутренних угроз.

Управление доступом играет ключевую роль в сетевой безопасности, ограничивая доступ к критическим сегментам сети и предотвращая несанкционированное использование ресурсов. Например, в корпоративной сети настройка ACL на маршрутизаторе может запретить доступ к серверам баз данных для всех, кроме определенных IP-адресов, снижая риск атак, таких как SQL-инъекции. RBAC, в свою очередь, упрощает управление доступом в больших сетях, позволяя администраторам назначать права на основе должностных обязанностей, что минимизирует вероятность человеческой ошибки, например, предоставления избыточных прав. Подход Zero Trust особенно эффективен в распределенных сетях, где границы между внутренней и внешней средой размыты, требуя постоянной проверки. Вопрос о том, как RBAC снижает риски сетевых атак, подчеркивает его способность ограничивать доступ по принципу минимальных привилегий, предотвращая компрометацию сети даже в случае взлома учетной записи.

4. Мониторинг сетевого доступа

Мониторинг сетевого доступа завершает процесс обеспечения безопасного доступа, позволяя выявлять и предотвращать угрозы в реальном времени. Этот процесс включает сбор и анализ данных о сетевых сессиях, используя журналы событий, системы управления безопасностью информации (SIEM) и другие инструменты мониторинга. Например, SIEM-системы собирают логи с маршрутизаторов, межсетевых экранов и серверов аутентификации, анализируя их на предмет аномалий, таких как многократные попытки входа с одного IP-адреса, что может указывать на брутфорс-атаку. Мониторинг также позволяет отслеживать действия пользователей, выявляя несанкционированный доступ или подозрительное поведение, например, попытки доступа к запрещенным сегментам сети.

В сетевой безопасности мониторинг играет ключевую роль, поскольку он не только выявляет инциденты, но и помогает в их предотвращении. Например, обнаружение брутфорс-атаки на сервер SSH через анализ логов может привести к автоматической блокировке атакующего IP-адреса. Кроме того, мониторинг позволяет проводить ретроспективный анализ инцидентов, чтобы улучшить политики безопасности. Например, если логи показывают, что сотрудники часто используют слабые пароли, это может стать основанием для ужесточения требований к аутентификации. Однако мониторинг требует интеграции с другими системами безопасности, такими как IDS/IPS, для эффективного реагирования на угрозы. Роль мониторинга в сетевой безопасности заключается в обеспечении видимости и контроля над сетевыми активностями, что позволяет своевременно выявлять и устранять угрозы. Вопрос о том, как мониторинг защищает от атак, подчеркивает его

способность обнаруживать инциденты в реальном времени, обеспечивая устойчивость сети.

Идентификация, аутентификация, управление доступом и мониторинг составляют комплексный подход к обеспечению безопасности компьютерных сетей. Идентификация создает основу для определения пользователей и устройств, предотвращая подключение несанкционированных участников. Аутентификация, особенно с использованием двухфакторных методов, подтверждает подлинность, защищая от кражи учетных данных. Управление доступом, основанное на моделях, таких как RBAC и Zero Trust, ограничивает права, минимизируя риски атак. Мониторинг обеспечивает видимость и контроль, позволяя выявлять и предотвращать инциденты. Вместе эти механизмы создают надежную систему защиты, которая противостоит современным киберугрозам, обеспечивая безопасность сетевых ресурсов и данных.

Литература

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст : электронный (гл. 1).

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 2).

Контрольные вопросы:

1. Охарактеризовать ложный ARP- сервер, IP Hijacking.
2. Привести методы распределенных атаки «отказ в обслуживании».
3. Привести классификацию распределенных атаки «отказ в обслуживании.

2.2 Защита от сетевых угроз

2.2.1 Тема 2.1 Доменные службы Active Directory. Структуры леса, доменных деревьев. Проектирование отношений и оптимизация аутентификации внутри леса

Перечень изучаемых вопросов

1. Active Directory для сетевой безопасности.
2. Сетевая структура леса и доменных деревьев.
3. Доверительные отношения и сетевая безопасность.
4. Оптимизация сетевой аутентификации.

Методические указания

1. Active Directory для сетевой безопасности

Active Directory представляет собой мощную платформу для централизованного управления пользователями, устройствами и ресурсами в корпоративных сетях, обеспечивая надежную основу для сетевой безопасности. Эта система позволяет администраторам контролировать доступ к сетевым ресурсам, устанавливать политики безопасности и отслеживать действия пользователей, что минимизирует риски компрометации. Одним из ключевых инструментов Active Directory является групповая политика, которая позволяет задавать единые стандарты безопасности для всей сети. Например, с помощью групповой политики можно настроить политики паролей, требующие использования сложных комбинаций символов и их регулярного обновления, что снижает вероятность успешных атак методом перебора. Кроме того, Active Directory поддерживает управление учетными записями, позволяя быстро блокировать доступ для уволенных сотрудников или скомпрометированных устройств, предотвращая несанкционированное использование сети.

Централизованное управление, предоставляемое Active Directory, упрощает администрирование безопасности в крупных организациях, где сотни или тысячи пользователей взаимодействуют с сетью. Без AD администраторам пришлось бы настраивать права доступа и политики на

каждом устройстве индивидуально, что увеличило бы риск ошибок, таких как предоставление избыточных привилегий. Например, в корпоративной сети AD можно настроить так, чтобы только сотрудники ИТ-отдела имели доступ к конфигурации маршрутизаторов, а остальные пользователи ограничивались доступом к общим ресурсам. Это снижает вероятность внутренних угроз, таких как случайное изменение критически важных настроек сети. Роль Active Directory в сетевой безопасности заключается в обеспечении централизованного контроля, который стандартизирует меры защиты и повышает устойчивость сети к внешним и внутренним угрозам. Вопрос о том, как AD повышает безопасность корпоративной сети, подчеркивает его способность объединять управление доступом, политиками и мониторингом в единую систему, минимизируя уязвимости и упрощая реагирование на инциденты.

2. Сетевая структура леса и доменных деревьев

Структура леса и доменных деревьев в Active Directory является основой для организации и сегментации сетевых ресурсов, что играет ключевую роль в обеспечении сетевой безопасности. Лес представляет собой совокупность доменов, объединенных общими схемами и доверительными отношениями, а доменные деревья формируют иерархическую структуру внутри леса, основанную на общем пространстве имен DNS. Эта структура позволяет организациям логически разделять ресурсы, изолируя различные сегменты сети для повышения безопасности. Например, в крупной компании с несколькими филиалами каждый филиал может быть представлен отдельным доменом в лесу, что позволяет изолировать ресурсы одного филиала от другого. Если злоумышленник скомпрометирует учетную запись в одном домене, структура леса ограничит его доступ к другим доменам, минимизируя масштаб атаки.

Сегментация, обеспечиваемая лесом и доменными деревьями, также упрощает управление политиками безопасности. Например, филиал, работающий с конфиденциальными данными, может иметь более строгие политики паролей или ограничения на удаленный доступ, в то время как центральный офис может использовать более гибкие настройки для повышения удобства. Такая гибкость позволяет адаптировать меры безопасности к специфическим рискам каждого сегмента сети. Кроме того, структура леса обеспечивает масштабируемость, позволяя добавлять новые домены по мере роста организации без значительных изменений в архитектуре. Однако неправильное проектирование леса, такое как избыточное количество доменов или слабые доверительные отношения, может создать уязвимости, позволяющие злоумышленникам перемещаться между сегментами сети. Роль структуры леса и доменных деревьев в сетевой

безопасности заключается в изоляции сетевых сегментов, что снижает риски распространения атак и упрощает управление. Вопрос о том, как структура леса снижает сетевые риски, подчеркивает ее способность ограничивать доступ и обеспечивать сегментацию, создавая барьеры для атакующих.

3. Доверительные отношения и сетевая безопасность

Доверительные отношения в Active Directory определяют, как домены в лесу или между лесами взаимодействуют друг с другом, позволяя пользователям одного домена получать доступ к ресурсам другого. Эти отношения являются критически важным элементом сетевой безопасности, поскольку они контролируют обмен данными и доступ между сегментами сети. Доверительные отношения могут быть односторонними, когда один домен доверяет другому, но не наоборот, или двусторонними, когда доверие взаимно. Например, в компании с филиалами центральный домен может иметь одностороннее доверие к домену филиала, что позволяет сотрудникам филиала получать доступ к общим ресурсам, но ограничивает их возможности влиять на центральную сеть. Это минимизирует риски, связанные с компрометацией менее защищенного филиала.

Настройка доверительных отношений требует тщательного подхода, чтобы предотвратить уязвимости. Неправильная конфигурация, например, автоматическое доверие ко всем доменам в лесу, может позволить злоумышленнику, получившему доступ к одному домену, перемещаться по всей сети, используя атаку типа «передай билет» с протоколом Kerberos. Чтобы свести к минимуму такие угрозы, доверительные отношения должны быть ограничены только необходимыми ресурсами, а доступ должен строго контролироваться с помощью политик и мониторинга. Например, доверие между доменами может быть настроено таким образом, чтобы предоставлять доступ к конкретной папке на сервере, а не ко всем ресурсам домена. Роль доверительных отношений в сетевой безопасности заключается в обеспечении безопасного обмена данными между доменами, что минимизирует риски атак, связанных с неправомерным использованием доверия. Вопрос о том, какие сетевые угрозы возникают при неправильной настройке доверия, подчеркивает необходимость строгого контроля и ограничения прав, чтобы предотвратить компрометацию всей сети из-за уязвимости в одном сегменте.

4. Оптимизация сетевой аутентификации

Оптимизация сетевой аутентификации в Active Directory направлена на повышение безопасности и эффективности процессов подтверждения подлинности пользователей и устройств. Основным протоколом аутентификации в AD является Kerberos, который обеспечивает безопасную передачу учетных данных в сети с помощью временных билетов и шифрования. Kerberos предотвращает перехват учетных данных, таких как

пароли, поскольку они передаются не в открытом виде, а заменяются зашифрованными билетами, которые действительны только в течение ограниченного времени. Это делает протокол устойчивым к атакам, таким как перехват трафика или повторное использование украденных данных. Например, когда пользователь входит в корпоративную сеть, Kerberos выдает ему билет, который позволяет ему получать доступ к ресурсам без повторной аутентификации, что повышает удобство и безопасность.

Для оптимизации аутентификации в распределённых сетях, где пользователи могут находиться в удалённых филиалах, Active Directory использует такие механизмы, как кэширование учётных данных. Это позволяет пользователям проходить аутентификацию локально, даже если связь с центральным контроллером домена временно недоступна, что особенно важно для сетей с нестабильным подключением. Однако кэширование требует строгой защиты, чтобы предотвратить кражу сохранённых данных. Кроме того, оптимизация включает размещение контроллеров домена вблизи пользователей для снижения задержек и настройку политик, таких как ограничение количества одновременных сеансов, чтобы минимизировать риски атак. Роль оптимизации аутентификации в сетевой безопасности заключается в защите учетных данных от перехвата и повышении надежности доступа, что критически важно для предотвращения несанкционированного проникновения. Вопрос о том, как Kerberos повышает безопасность сетевой аутентификации, подчеркивает его способность обеспечивать зашифрованную и временно ограниченную аутентификацию, защищая сеть от атак на учетные записи.

Active Directory с его структурой леса и доменных деревьев, доверительными отношениями и оптимизированной аутентификацией является мощным инструментом для обеспечения сетевой безопасности. AD предоставляет централизованное управление, стандартизируя защиту сетевых ресурсов с помощью групповой политики и управления учетными записями. Структура леса и доменных деревьев обеспечивает сегментацию, изолируя ресурсы и снижая риски распространения атак. Доверительные отношения контролируют доступ между доменами, минимизируя угрозы, связанные с их компрометацией. Оптимизация аутентификации, основанная на протоколе Kerberos, защищает учетные данные и повышает эффективность доступа. Вместе эти элементы создают комплексную систему, которая защищает корпоративные сети от современных киберугроз, обеспечивая надежность и устойчивость сетевой инфраструктуры.

Литература

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст : электронный (гл. 1).

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 2).

5. 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. 2).

Контрольные вопросы

1. Охарактеризуйте системы обнаружения вторжений.
2. Охарактеризуйте межсетевые экраны.
3. Охарактеризуйте системы шифрования трафика.

2.2.2 Тема 2.2 Корпоративная информационная система. Сети периметра и стратегии удаленного доступа

Перечень изучаемых вопросов

1. Сетевая архитектура корпоративных систем.
2. Сети периметра (DMZ) в сетевой защите.
3. Безопасный удаленный доступ к сети.
4. Мониторинг удаленного сетевого доступа.

Методические указания к изучению

1. Сетевая архитектура корпоративных систем

Сетевая архитектура корпоративной информационной системы формирует основу для обеспечения безопасности, определяя, как серверы, сетевые устройства и клиентские станции взаимодействуют в рамках сети. Корпоративные системы включают множество компонентов: серверы, на которых размещаются базы данных, приложения и сервисы; сетевые устройства, такие как маршрутизаторы и коммутаторы, управляющие трафиком; и клиентские устройства, используемые сотрудниками для доступа к ресурсам. Правильная организация этих компонентов позволяет минимизировать уязвимости, предотвращая атаки, такие как эксплуатация серверов или перехват данных. Например, защита серверов от внешних атак может включать размещение их в изолированных сегментах сети, доступных только через межсетевые экраны с настроенными правилами фильтрации. Это предотвращает прямое взаимодействие с внешними сетями, снижая риск атак, таких как DDoS или SQL-инъекции.

Архитектура сети напрямую влияет на безопасность, поскольку определяет, как данные передаются и где они наиболее уязвимы. Например, централизованная архитектура с единым серверным узлом может быть удобной для управления, но создает единую точку отказа, которую злоумышленники могут атаковать. В то же время децентрализованная архитектура с сегментацией сети, например, через VLAN, позволяет изолировать критические ресурсы, такие как финансовые базы данных, от менее защищенных зон, таких как гостевые Wi-Fi-сети. Такой подход минимизирует распространение атаки в случае компрометации одного сегмента. Кроме того, архитектура должна учитывать масштабируемость и интеграцию с системами безопасности, такими как IDS/IPS, которые отслеживают трафик для выявления угроз. Вопрос о том, как архитектура сети влияет на безопасность, подчеркивает необходимость продуманного проектирования, которое балансирует между функциональностью,

производительностью и защитой, минимизируя уязвимости и обеспечивая устойчивость системы.

2. Сети периметра (DMZ) в сетевой защите

Сети периметра, или демилитаризованные зоны (DMZ), являются важным элементом сетевой безопасности, обеспечивая изоляцию общедоступных сервисов от внутренней корпоративной сети. DMZ создается для размещения серверов, которые должны быть доступны из внешних сетей, таких как интернет, например, веб-серверов, почтовых серверов или серверов DNS. Эти сервисы часто становятся мишенью атак, поэтому их изоляция в DMZ предотвращает проникновение злоумышленников во внутреннюю сеть, где хранятся конфиденциальные данные. Например, веб-сервер, размещенный в DMZ, может быть защищен межсетевым экраном, который разрешает только HTTP/HTTPS-трафик, блокируя попытки доступа к другим портам или сервисам. Это снижает риск эксплуатации уязвимостей, таких как неправильно настроенные веб-приложения, которые могут быть использованы для атаки на внутренние ресурсы.

Организация DMZ требует тщательной настройки межсетевых экранов и правил фильтрации, чтобы ограничить взаимодействие между DMZ и внутренней сетью. Например, правила могут разрешать только исходящий трафик от веб-сервера к базе данных, находящейся во внутренней сети, но блокировать любые входящие соединения, инициированные из DMZ. Это предотвращает сценарии, при которых скомпрометированный сервер в DMZ становится точкой входа для атаки на внутреннюю сеть. Кроме того, DMZ может включать дополнительные меры безопасности, такие как веб-файрволы (WAF), которые защищают от атак на прикладном уровне, например, XSS или SQL-инъекций. Роль DMZ в сетевой безопасности заключается в создании буферной зоны, которая изолирует публичные сервисы и минимизирует риск проникновения во внутреннюю сеть. Вопрос о том, почему DMZ важна для сетевой безопасности, подчеркивает ее способность ограничивать воздействие атак, обеспечивая защиту критических ресурсов, даже если внешний сервис оказывается скомпрометированным.

3. Безопасный удаленный доступ к сети

С ростом числа удаленных сотрудников и распределенных рабочих сред обеспечение безопасного удаленного доступа к корпоративным сетям становится одной из ключевых задач сетевой безопасности. Технологии, такие как виртуальные частные сети (VPN) и подход Zero Trust, позволяют организациям защищать подключения пользователей, работающих из дома или других удаленных локаций. VPN, например, на основе протокола IPSec, создает зашифрованный туннель между устройством пользователя и корпоративной сетью, обеспечивая конфиденциальность данных даже при

использовании незащищенных каналов, таких как общественные Wi-Fi-сети. Для повышения безопасности VPN часто интегрируется с двухфакторной аутентификацией (MFA), требующей от пользователя ввода пароля и дополнительного фактора, например, одноразового кода, отправленного на мобильное устройство. Это снижает риск компрометации учетных данных через фишинг или перехват.

Подход Zero Trust, в отличие от традиционных методов, предполагает, что ни один пользователь или устройство не являются доверенными по умолчанию, независимо от их расположения. Этот подход требует постоянной проверки подлинности и прав доступа для каждого запроса, что особенно важно в условиях, когда границы между внутренней и внешней сетью размыты. Например, Zero Trust может требовать, чтобы удаленный сотрудник проходил аутентификацию через сертификат устройства и проверку состояния его безопасности перед доступом к корпоративным приложениям. Это предотвращает атаки, при которых злоумышленник использует украденные учетные данные для доступа к сети. Роль технологий удаленного доступа в сетевой безопасности заключается в защите подключений, минимизируя риски перехвата данных или несанкционированного доступа. Вопрос о том, как Zero Trust повышает безопасность сети, подчеркивает его способность устранять предположение о доверии, обеспечивая строгую проверку каждого соединения, что делает сеть устойчивой к современным угрозам.

4. Мониторинг удаленного сетевого доступа

Мониторинг удаленного сетевого доступа завершает стратегию защиты, позволяя организациям выявлять и предотвращать угрозы, связанные с удаленными подключениями. Этот процесс включает использование инструментов, таких как системы обнаружения и предотвращения вторжений (IDS/IPS) и анализаторы сетевого трафика, для отслеживания активности пользователей и устройств. Например, IDS/IPS могут обнаружить аномалии в VPN-соединениях, такие как необычно высокий объем исходящего трафика, который может указывать на утечку данных или действия вредоносного ПО. Анализ сетевого трафика, выполненный с помощью инструментов, таких как NetFlow или Wireshark, позволяет выявить подозрительные шаблоны, например, многократные попытки подключения с одного IP-адреса, что может сигнализировать о брутфорс-атаке.

Мониторинг также включает интеграцию с системами управления безопасностью информации (SIEM), которые собирают и анализируют логи с VPN-серверов, межсетевых экранов и других устройств. Это позволяет в реальном времени реагировать на инциденты, такие как несанкционированные попытки доступа, путем автоматической блокировки IP-адресов или уведомления администраторов. Кроме того, мониторинг помогает проводить

ретроспективный анализ, чтобы улучшить политики удаленного доступа. Например, если логи показывают, что пользователи часто подключаются через незащищенные сети без VPN, это может стать основанием для ужесточения требований к использованию шифрованных соединений. Роль мониторинга в сетевой безопасности заключается в обеспечении видимости и контроля над удаленными подключениями, что позволяет своевременно выявлять и предотвращать угрозы. Вопрос о том, как мониторинг предотвращает несанкционированный доступ, подчеркивает его способность обнаруживать аномалии и реагировать на них, защищая сеть от атак, связанных с удаленным доступом.

Защита корпоративных сетей требует комплексного подхода, который включает продуманную сетевую архитектуру, использование DMZ, безопасные технологии удаленного доступа и мониторинг. Сетевая архитектура минимизирует уязвимости, сегментируя ресурсы и интегрируя системы безопасности. DMZ изолирует публичные сервисы, предотвращая проникновение во внутреннюю сеть. Технологии удаленного доступа, такие как VPN и Zero Trust, защищают подключения, обеспечивая конфиденциальность и аутентификацию. Мониторинг выявляет и предотвращает угрозы, обеспечивая контроль над сетевой активностью. Вместе эти элементы создают надежную систему защиты, которая позволяет организациям противостоять киберугрозам, обеспечивая устойчивость и безопасность корпоративных информационных

Литература

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст :

электронный (гл. 1).

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 2).

5. 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).

Контрольные вопросы

1. Приведите специфику методы предотвращения вторжения.
2. Приведите общие методы отклонения вторжения, принципы обнаружение вторжений.

2.2.3 Тема 2.3. Обеспечение безопасности операционных систем. Локальные политики безопасности. Встроенные системы защиты операционных систем. Модель взаимодействия систем. Стек протоколов TCP/IP

Перечень изучаемых вопросов

1. Локальные политики для сетевой безопасности.
2. Встроенные сетевые механизмы защиты ОС.
3. Сетевое взаимодействие систем.
4. Безопасность стека TCP/IP.

Методические указания к изучению

1. Локальные политики для сетевой безопасности

Локальные политики безопасности представляют собой набор конфигураций, которые определяют правила поведения операционной системы и пользователей для защиты сетевых узлов. Эти политики включают настройку требований к паролям, ограничение запуска определенных служб и аудит сетевых событий, чтобы обеспечить контроль над действиями в системе. Например, в корпоративной сети на базе Windows групповая политика (Group Policy) позволяет администраторам устанавливать минимальную длину

паролей и требовать их регулярного обновления, что снижает риск атак брутфорса, направленных на компрометацию учетных записей. Кроме того, политики аудита могут настроить регистрацию всех попыток входа в систему, что помогает выявить подозрительные активности, такие как многократные неудачные попытки аутентификации, указывающие на потенциальную атаку.

Локальные политики также позволяют ограничивать сетевые службы, минимизируя точки входа для злоумышленников. Например, администратор может отключить устаревшие или ненужные службы, такие как Telnet, которые могут быть использованы для атак из-за слабых механизмов шифрования. В сетевой среде это особенно важно, поскольку каждый открытый порт или активная служба увеличивает поверхность атаки. Политики также могут ограничивать выполнение приложений, разрешая запуск только доверенного ПО, что предотвращает активацию вредоносных программ, распространяемых через сеть. Роль локальных политик в сетевой безопасности заключается в защите хостов от атак, обеспечивая минимальные привилегии и строгий контроль над сетевыми взаимодействиями. Вопрос о том, как локальные политики защищают сетевые узлы, подчеркивает их способность создавать барьеры на уровне ОС, снижая вероятность компрометации и упрощая управление безопасностью в распределенных сетях.

2. Встроенные сетевые механизмы защиты ОС

Встроенные механизмы защиты операционных систем представляют собой инструменты, интегрированные в ОС для предотвращения сетевых угроз на уровне хоста. Эти механизмы включают брандмауэры, системы контроля доступа и средства защиты от вредоносного ПО. Например, брандмауэр Windows Defender позволяет администраторам фильтровать входящий и исходящий сетевой трафик, разрешая соединения только с доверенными IP-адресами или портами. Это эффективно предотвращает атаки, такие как сканирование портов или попытки эксплуатации уязвимостей в сетевых службах. В Linux-системах SELinux (Security-Enhanced Linux) обеспечивает обязательный контроль доступа, ограничивая действия приложений и пользователей в соответствии с заданными политиками, что минимизирует риск эскалации привилегий в случае компрометации.

Эти инструменты играют ключевую роль в сетевой безопасности, поскольку защищают отдельные хосты, которые являются основными узлами сети. Например, настройка брандмауэра для блокировки всех входящих соединений, кроме необходимых для работы веб-сервера, снижает вероятность атак, таких как DDoS или эксплуатация уязвимостей. SELinux может предотвратить запуск вредоносного кода, даже если злоумышленник получает доступ к системе, ограничивая его действия строгими правилами. Однако

встроенные механизмы требуют регулярного обновления и правильной настройки, чтобы оставаться эффективными. Например, устаревший брандмауэр с некорректными правилами может пропустить вредоносный трафик, а неправильно настроенный SELinux может ограничить легитимные процессы, снижая производительность. Роль встроенных механизмов в сетевой безопасности заключается в создании защитного слоя на уровне хоста, предотвращающего сетевые угрозы и минимизирующего последствия атак. Вопрос о том, как встроенные механизмы ОС повышают сетевую безопасность, подчеркивает их способность изолировать уязвимости и обеспечивать защиту даже в случае компрометации других сетевых компонентов.

3. Сетевое взаимодействие систем

Модель взаимодействия систем определяет, как операционные системы обмениваются данными в сети, что напрямую влияет на их уязвимости и стратегии защиты. Наиболее распространенной является модель клиент-сервер, где клиентские устройства запрашивают услуги у серверов, таких как веб-серверы или базы данных. Эта модель, хотя и эффективна, создает уязвимости, такие как перехват данных или атаки «человек посередине» (MitM), при которых злоумышленник подменяет одну из сторон для получения доступа к трафику. Например, в корпоративной сети клиент, запрашивающий доступ к серверу электронной почты, может стать жертвой MitM-атаки, если соединение не защищено шифрованием TLS. Для защиты от таких угроз применяются протоколы, такие как HTTPS, которые обеспечивают шифрование и аутентификацию сторон, гарантируя целостность и конфиденциальность данных.

Альтернативные модели, такие как одноранговая (P2P), также имеют свои риски, поскольку каждый узел выступает одновременно клиентом и сервером, увеличивая поверхность атаки. В сетевой безопасности защита взаимодействия систем требует учета специфики модели и внедрения соответствующих мер. Например, в клиент-серверной модели важно использовать цифровые сертификаты для аутентификации серверов, чтобы предотвратить подмену, а также шифрование для защиты данных в пути. Кроме того, сегментация сети, например, через VLAN, может ограничить взаимодействие между системами, минимизируя распространение атак. Роль сетевого взаимодействия систем в сетевой безопасности заключается в обеспечении безопасного обмена данными, предотвращающего компрометацию информации. Вопрос о том, как модель взаимодействия влияет на сетевую защиту, подчеркивает необходимость адаптации защитных мер к архитектуре сети, чтобы минимизировать уязвимости, связанные с передачей данных.

4. Безопасность стека TCP/IP

Стек протоколов TCP/IP является основой для передачи данных в современных сетях, но его уязвимости создают значительные риски для сетевой безопасности. Этот стек включает несколько уровней – прикладной, транспортный, сетевой и канальный, – каждый из которых имеет свои угрозы. Например, на прикладном уровне атаки, такие как DNS-спуфинг, позволяют злоумышленникам перенаправлять трафик на поддельные серверы, обманывая пользователей. Для защиты от этого применяется DNSSEC, который использует цифровые подписи для подтверждения подлинности DNS-записей. На транспортном уровне атаки, такие как TCP SYN-флуд, перегружают серверы ложными запросами на соединение, что требует настройки брандмауэров для ограничения числа одновременных соединений.

На сетевом уровне угрозы, такие как IP-спуфинг, позволяют атакующим подделывать IP-адреса для обхода фильтров. Защита включает фильтрацию трафика на основе списков контроля доступа (ACL) и использование протоколов, устойчивых к подделке. На канальном уровне атаки, такие как ARP-спуфинг, угрожают локальным сетям, что требует внедрения динамической проверки ARP или сегментации сети. Безопасность стека TCP/IP требует комплексного подхода, включающего шифрование, аутентификацию и мониторинг трафика. Например, использование TLS для защиты HTTP-трафика или IPSec для шифрования сетевых пакетов минимизирует риск перехвата данных. Роль безопасности стека TCP/IP в сетевой безопасности заключается в защите протоколов, обеспечивающих передачу данных, от эксплуатации уязвимостей. Вопрос о том, как защита TCP/IP предотвращает сетевые атаки, подчеркивает необходимость многоуровневого подхода, который устраняет угрозы на каждом этапе передачи данных.

Защита операционных систем и стека TCP/IP формирует важную часть стратегии сетевой безопасности, обеспечивая устойчивость сети к киберугрозам. Локальные политики безопасности защищают хосты, стандартизируя требования к паролям, службам и аудиту. Встроенные механизмы ОС, такие как брандмауэры и SELinux, создают защитный слой на уровне хоста, предотвращая сетевые атаки. Модель взаимодействия систем определяет уязвимости и меры защиты, обеспечивая безопасный обмен данными. Безопасность стека TCP/IP минимизирует риски, связанные с протоколами передачи данных, через шифрование и фильтрацию. Вместе эти элементы создают надежную систему защиты, которая укрепляет сетевую инфраструктуру, противостоя современным угрозам, таким как MitM, DDoS или спуфинг.

Литература:

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст : электронный (гл. 1).

4. 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).

Контрольные вопросы

1. Охарактеризуйте идентификацию и аутентификацию пользователей с использованием технических устройств.

2. Охарактеризуйте идентификацию и аутентификацию с использованием индивидуальных биометрических характеристик пользователя.

2.2.4 Тема 2.4 Защита на канальном уровне – протоколы удаленного доступа

Перечень изучаемых вопросов

1. Канальный уровень и сетевая безопасность.
2. Протоколы удаленного доступа в сетях.
3. Безопасность Wi-Fi-сетей.

4. Мониторинг канального уровня сети.

Методические указания к изучению

1. Канальный уровень и сетевая безопасность

Канальный уровень модели OSI отвечает за передачу данных между устройствами в одной локальной сети, обеспечивая их доставку через физические каналы, такие как Ethernet или Wi-Fi. Несмотря на свою низкоуровневую природу, этот уровень является критически важным для сетевой безопасности, поскольку именно здесь возникают угрозы, способные подорвать целостность и конфиденциальность сетевых взаимодействий. Одной из наиболее распространенных атак является ARP-спуфинг, при которой злоумышленник подменяет ARP-таблицы, перенаправляя трафик через свое устройство для перехвата данных или проведения атак типа «человек посередине» (MitM). Еще одна угроза – MAC-флудинг, когда атакующий перегружает таблицу MAC-адресов коммутатора, заставляя его работать в режиме хаба и раскрывать весь сетевой трафик. Эти атаки демонстрируют, насколько уязвимым может быть канальный уровень без адекватной защиты.

Для противодействия таким угрозам широко используется сегментация сети с помощью виртуальных локальных сетей (VLAN). VLAN позволяют изолировать трафик различных групп устройств, например, отделяя пользовательские компьютеры от серверов или гостевые устройства от корпоративной сети. Это ограничивает распространение атак, таких как MAC-флудинг, и затрудняет злоумышленникам доступ к критическим ресурсам. Кроме того, технологии, такие как динамическая проверка ARP, помогают предотвратить подмену адресов, проверяя соответствие MAC- и IP-адресов. Роль канального уровня в сетевой безопасности заключается в создании фундамента для защиты локальных сетей, предотвращая атаки, которые могут скомпрометировать базовые механизмы передачи данных. Вопрос о том, почему канальный уровень важен для сетевой защиты, подчеркивает его позицию как первой линии обороны, где угрозы могут быть нейтрализованы до их проникновения на более высокие уровни сетевого стека.

2. Протоколы удаленного доступа в сетях

Протоколы удаленного доступа, работающие на канальном уровне, обеспечивают безопасное подключение удаленных пользователей или устройств к корпоративным сетям, что особенно важно в эпоху распределенных рабочих сред. Протоколы, такие как PPP (Point-to-Point Protocol) и L2TP (Layer 2 Tunneling Protocol), предоставляют механизмы для передачи данных через защищенные туннели, сочетая шифрование и

аутентификацию. PPP, например, используется для установления соединений между двумя узлами, обеспечивая аутентификацию через протоколы, такие как PAP или CHAP, и поддерживая базовое шифрование. Однако для повышения безопасности PPP часто комбинируется с L2TP, который создает туннель для передачи данных, защищенный шифрованием IPSec. Такой подход широко применяется в корпоративных VPN, где сотрудники подключаются к внутренней сети из удаленных локаций, например, из дома или в командировке, через зашифрованные каналы.

Настройка L2TP/IPSec для VPN в корпоративной сети демонстрирует, как протоколы удаленного доступа укрепляют сетевую безопасность. L2TP обеспечивает туннелирование, передавая данные через интернет, а IPSec добавляет шифрование и аутентификацию, защищая трафик от перехвата. Это предотвращает утечку конфиденциальной информации, даже если пользователь подключен через незащищенную общественную Wi-Fi-сеть. Однако безопасность этих протоколов зависит от правильной конфигурации, включая использование надежных алгоритмов шифрования, таких как AES-256, и строгих методов аутентификации, таких как сертификаты или двухфакторная аутентификация. Роль протоколов удаленного доступа в сетевой безопасности заключается в защите удаленных подключений, обеспечивая конфиденциальность и целостность данных. Вопрос о том, как протоколы повышают безопасность удаленного доступа, подчеркивает их способность создавать защищенные каналы связи, минимизируя риски, связанные с передачей данных через внешние сети.

3. Безопасность Wi-Fi-сетей

Wi-Fi-сети, работающие на канальном уровне, представляют собой одну из наиболее уязвимых точек в сетевой инфраструктуре из-за их беспроводной природы, которая облегчает перехват трафика. Для защиты Wi-Fi-сетей разработаны протоколы, такие как WPA3 (Wi-Fi Protected Access 3), которые обеспечивают шифрование и аутентификацию, предотвращая атаки, такие как Krack, направленные на уязвимости предыдущих стандартов, например, WPA2. WPA3 использует улучшенный алгоритм шифрования и устойчивый к перехвату процесс рукопожатия, что делает его более надежным для защиты сетевого трафика. В корпоративных Wi-Fi-сетях WPA3 часто комбинируется с двухфакторной аутентификацией (MFA), требующей от пользователей ввода учетных данных и дополнительного фактора, например, кода из мобильного приложения, для подключения к сети.

Настройка корпоративного Wi-Fi с использованием WPA3 и MFA демонстрирует, как можно минимизировать риски атак на беспроводные сети. Например, в офисе сотрудники могут подключаться к сети только после аутентификации через RADIUS-сервер, который проверяет их учетные данные

и сертификаты устройств. Это предотвращает подключение несанкционированных устройств, таких как скомпрометированные ноутбуки, и защищает трафик от перехвата. Кроме того, WPA3 поддерживает индивидуальное шифрование для каждого устройства, что ограничивает доступ злоумышленников к данным других пользователей, даже если сеть скомпрометирована. Однако безопасность Wi-Fi требует регулярного обновления ключей шифрования и мониторинга подключений, чтобы выявить подозрительные устройства. Роль безопасности Wi-Fi-сетей в сетевой безопасности заключается в предотвращении атак на беспроводные каналы, обеспечивая конфиденциальность и целостность данных. Вопрос о том, как WPA3 защищает сетевой трафик Wi-Fi, подчеркивает его способность устранять уязвимости и создавать надежную защиту в условиях, где физический контроль над средой передачи ограничен.

4. Мониторинг канального уровня сети

Мониторинг канального уровня сети завершает стратегию защиты, позволяя организациям выявлять и предотвращать угрозы в реальном времени. Этот процесс включает использование инструментов, таких как системы контроля доступа к сети (NAC) и анализаторы сетевого трафика, для отслеживания активности на канальном уровне. NAC-системы проверяют устройства, подключающиеся к сети, на соответствие политикам безопасности, например, наличие актуальных антивирусов или правильных MAC-адресов, блокируя несанкционированные подключения. Анализаторы трафика, такие как Wireshark, позволяют администраторам обнаруживать аномалии, например, ARP-атаки, при которых злоумышленник отправляет поддельные ARP-сообщения для перенаправления трафика. Выявление таких атак требует анализа ARP-таблиц и трафика, чтобы обнаружить несоответствия между MAC- и IP-адресами.

Мониторинг также включает интеграцию с системами управления безопасностью информации (SIEM), которые собирают логи с коммутаторов, точек доступа Wi-Fi и других устройств канального уровня. Это позволяет в реальном времени реагировать на инциденты, такие как MAC-флудинг, путем автоматической изоляции атакующего устройства. Кроме того, мониторинг помогает проводить ретроспективный анализ, выявляя слабые места в конфигурации сети, например, отсутствие сегментации VLAN, которое облегчает атаки. Роль мониторинга в сетевой безопасности заключается в обеспечении видимости и контроля над активностью на канальном уровне, предотвращая несанкционированный доступ и атаки. Вопрос о том, как мониторинг защищает канальный уровень сети, подчеркивает его способность обнаруживать угрозы на ранней стадии, минимизируя их воздействие на сетевую инфраструктуру.

Защита на канальном уровне, включая протоколы удаленного доступа, Wi-Fi-сети и мониторинг, формирует важный компонент сетевой безопасности, обеспечивая надежность локальных и удаленных соединений. Канальный уровень защищает сети от угроз, таких как ARP-спуфинг и MAC-флудинг, через сегментацию и динамическую проверку. Протоколы удаленного доступа, такие как L2TP/IPSec, создают безопасные туннели для удаленных пользователей, предотвращая перехват данных. Безопасность Wi-Fi-сетей, усиленная WPA3 и MFA, минимизирует риски атак на беспроводные каналы. Мониторинг, поддерживаемый NAC и SIEM, обеспечивает контроль и реагирование на угрозы. Вместе эти элементы создают комплексную защиту, которая укрепляет канальный уровень, противостоя современным киберугрозам и обеспечивая устойчивость сетевой инфраструктуры.

Литература:

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст : электронный (гл. 1).

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 2).

Контрольные вопросы

1. Охарактеризуйте IPSec протокол.
2. Охарактеризуйте концентратор доступа LAC.
3. Поясните принципы построения сервер LNS

2.2.5 Тема 2.5 Протоколы IPSec, SSL, TSL, SOCKS. Защита на сетевом и сеансовом уровнях

Перечень изучаемых вопросов

1. IPSec для сетевой безопасности.
2. SSL/TLS для защиты сетевых сеансов.
3. SOCKS в сетевой безопасности.
4. Интеграция протоколов для сетевой защиты.

Методические указания к изучению

1. IPSec для сетевой безопасности

IPSec (Internet Protocol Security) представляет собой набор протоколов, работающих на сетевом уровне модели OSI, которые обеспечивают защиту сетевых соединений через шифрование и аутентификацию данных. Этот протокол широко применяется для создания виртуальных частных сетей (VPN), позволяя организациям безопасно соединять географически распределённые филиалы или предоставлять удалённый доступ сотрудникам. IPSec поддерживает два режима работы: транспортный, защищающий только полезную нагрузку пакета, и туннельный, шифрующий весь пакет, включая заголовки. Туннельный режим особенно популярен для VPN, поскольку он скрывает топологию сети, делая её невидимой для злоумышленников. Например, компания с филиалами в разных городах может настроить IPSec VPN, чтобы обеспечить безопасный обмен данными между офисами через интернет, защищая трафик от перехвата.

IPSec использует такие механизмы, как AH (Authentication Header) для проверки целостности и ESP (Encapsulating Security Payload) для шифрования и аутентификации, что делает его устойчивым к атакам, направленным на подделку или модификацию данных. Например, при использовании ESP с алгоритмом AES-256 данные шифруются, а их целостность проверяется, что предотвращает вмешательство злоумышленников. Однако безопасность IPSec зависит от правильной настройки, включая выбор надежных алгоритмов шифрования и управления ключами через протокол IKE (Internet Key Exchange). Неправильная конфигурация, например, использование слабых ключей, может создать уязвимости. Роль IPSec в сетевой безопасности

заключается в обеспечении шифрования сетевого трафика, что гарантирует конфиденциальность и целостность данных на сетевом уровне. Вопрос о том, как IPSec защищает сетевые соединения, подчеркивает его способность создавать защищённые туннели, которые предотвращают перехват и подделку данных, обеспечивая надежную связь в небезопасных сетях.

2. SSL/TLS для защиты сетевых сеансов

SSL (Secure Sockets Layer) и его преемник TLS (Transport Layer Security) – это протоколы, работающие на сеансовом уровне, которые обеспечивают защиту данных, передаваемых между клиентом и сервером, через шифрование и аутентификацию. Эти протоколы наиболее известны своим применением в HTTPS, обеспечивающем безопасный доступ к веб-сайтам, а также в других протоколах, таких как FTPS для защищённой передачи файлов. TLS использует комбинацию асимметричного шифрования для безопасного обмена ключами и симметричного шифрования для защиты данных во время сеанса. Например, при подключении к веб-сайту через HTTPS браузер и сервер обмениваются цифровыми сертификатами, подтверждающими подлинность сервера, а затем устанавливают зашифрованное соединение с помощью алгоритмов, таких как AES.

Одной из ключевых особенностей TLS является его способность предотвращать атаки «человек посередине» (MitM), при которых злоумышленник пытается подменить одну из сторон для перехвата данных. Во время рукопожатия TLS сервер предоставляет сертификат, подписанный доверенным центром сертификации (CA), который клиент проверяет, чтобы убедиться в подлинности сервера. Если сертификат недействителен или подделан, соединение прерывается, защищая пользователя от подмены. Например, настройка TLS 1.3 на веб-сервере обеспечивает использование современных алгоритмов шифрования и устранение уязвимостей, присутствующих в более ранних версиях протокола. Однако безопасность TLS зависит от актуальности сертификатов и правильной конфигурации сервера, так как устаревшие версии протокола или слабые шифры могут быть уязвимы для атак, таких как POODLE. Роль SSL/TLS в сетевой безопасности заключается в защите от перехвата данных, обеспечивая конфиденциальность и аутентичность сеансов. Вопрос о том, как TLS предотвращает атаки MitM, подчеркивает его способность аутентифицировать стороны и шифровать данные, создавая доверительную среду для сетевых взаимодействий.

3. SOCKS в сетевой безопасности

SOCKS – это протокол, функционирующий на сеансовом уровне, который позволяет перенаправлять сетевой трафик через прокси-сервер, обеспечивая анонимизацию и обход сетевых ограничений. В отличие от IPSec или TLS, SOCKS не предоставляет шифрования, но его гибкость делает его

полезным для определённых сценариев сетевой безопасности. Например, SOCKS5, последняя версия протокола, поддерживает аутентификацию и может быть интегрирован с шифрующими протоколами, такими как SSH, для создания защищённых туннелей. В корпоративной среде SOCKS5 может использоваться для анонимизации трафика сотрудников, работающих с чувствительными данными, или для обхода географических ограничений при тестировании веб-приложений, скрывая истинные IP-адреса устройств.

Хотя SOCKS сам по себе не обеспечивает шифрования, его роль в сетевой безопасности заключается в предоставлении дополнительного уровня контроля над трафиком. Например, организация может настроить прокси-сервер SOCKS для фильтрации исходящего трафика, блокируя доступ к вредоносным сайтам или ограничивая использование определённых приложений. Это помогает предотвратить утечку данных или заражение сети через фишинговые ссылки. Однако использование SOCKS требует осторожности, так как неправильно настроенный прокси-сервер может стать точкой уязвимости, позволяя злоумышленникам перехватывать трафик или использовать сервер для анонимных атак. Роль SOCKS в сетевой безопасности заключается в перенаправлении трафика через контролируемые точки, обеспечивая анонимизацию и обход ограничений. Вопрос о том, как SOCKS влияет на сетевую безопасность, подчеркивает его способность повышать контроль над трафиком, но также указывает на необходимость интеграции с шифрующими протоколами для обеспечения конфиденциальности.

4. Интеграция протоколов для сетевой защиты

Интеграция протоколов, таких как IPSec, TLS и SOCKS, позволяет создавать многоуровневую защиту сетевого трафика, комбинируя их сильные стороны для противодействия разнообразным угрозам. Например, организация может одновременно использовать IPSec для создания VPN, обеспечивающего шифрование на сетевом уровне, и TLS для защиты веб-трафика, передаваемого через HTTPS. Такой подход защищает данные как на уровне сетевых соединений, так и на уровне приложений, минимизируя риски перехвата или подделки. В сценарии, где филиал компании подключается к центральному офису через IPSec VPN, сотрудники могут безопасно получать доступ к корпоративным веб-приложениям, защищённым TLS, что создаёт двойной слой защиты от атак MitM или перехвата данных.

Интеграция также может включать использование SOCKS в сочетании с IPSec или TLS для дополнительной анонимизации. Например, трафик, направленный через SOCKS5-прокси, может быть дополнительно зашифрован с помощью IPSec, чтобы скрыть как содержимое данных, так и их источник. Это особенно полезно для организаций, работающих в регионах с высокой цензурой или угрозами слежки. Однако интеграция протоколов требует

тщательного управления, чтобы избежать конфликтов или снижения производительности. Например, избыточное шифрование может увеличить задержки, что критично для приложений реального времени, таких как видеоконференции. Роль интеграции протоколов в сетевой безопасности заключается в создании многоуровневой защиты, которая повышает устойчивость сети к атакам. Вопрос о том, как интеграция протоколов повышает сетевую безопасность, подчеркивает её способность комбинировать шифрование, аутентификацию и анонимизацию для комплексной защиты данных.

Протоколы IPSec, SSL/TLS, SOCKS и их интеграция формируют мощный арсенал для защиты сетевого и сеансового уровней, обеспечивая безопасную передачу данных в компьютерных сетях. IPSec защищает сетевые соединения, создавая шифрованные туннели для VPN, что предотвращает перехват трафика. SSL/TLS обеспечивает безопасность сеансов, защищая веб- и файловый трафик от атак MitM через шифрование и аутентификацию. SOCKS предоставляет гибкость в перенаправлении трафика, повышая контроль и анонимизацию. Интеграция этих протоколов создаёт многоуровневую защиту, комбинируя их возможности для противодействия сложным угрозам. Вместе эти механизмы укрепляют сетевую инфраструктуру, обеспечивая конфиденциальность, целостность и устойчивость к кибератакам в условиях постоянно меняющегося ландшафта угроз.

Литература

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст :

электронный (гл. 1).

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 2).

5. 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. 2).

Контрольные вопросы

1. Функции программ-посредников.
2. Общая схема установления соединения по протоколу SOCKS.
3. Типы аутентификации в протоколе SSL.

2.2.6 Тема 2.6 Функционирование межсетевых экранов на различных уровнях модели OSI

Перечень изучаемых вопросов

1. Типы файрволов для сетевой защиты.
2. Брандмауэры на сетевом уровне.
3. Брандмауэры на прикладном уровне.
4. Мониторинг файрволов в сетях.

Методические указания к изучению

1. Типы файрволов для сетевой защиты

Межсетевые экраны различаются по своим возможностям и уровням работы в модели OSI, что определяет их эффективность в различных сценариях сетевой защиты. Основные типы включают пакетные фильтры, файрволы с отслеживанием состояния и межсетевые экраны следующего поколения (NGFW). Пакетные фильтры, работающие на сетевом уровне, анализируют заголовки пакетов, принимая решения о пропуске или блокировке на основе IP-адресов, портов и протоколов. Их простота обеспечивает высокую производительность, но ограниченные возможности

анализа делают их уязвимыми для сложных атак. Файрволы с отслеживанием состояния добавляют динамический контроль, отслеживая активные соединения и блокируя пакеты, не соответствующие установленным сессиям, что эффективно против атак, таких как TCP SYN-флуд. NGFW, в свою очередь, объединяют функции традиционных файрволов с глубоким анализом пакетов (DPI), обнаружением вторжений и фильтрацией приложений, позволяя защищать сеть от современных угроз, таких как вредоносное ПО, скрытое в зашифрованном трафике.

Примером практического применения является настройка Cisco ASA, универсального файрвола, который может работать в разных режимах. В корпоративной сети Cisco ASA может быть настроен как NGFW, фильтруя трафик по IP-адресам и портам, анализируя содержимое HTTPS-соединений и блокируя попытки эксплуатации уязвимостей веб-приложений. Выбор типа файрвола зависит от потребностей сети: для высокоскоростных соединений предпочтительны пакетные фильтры, тогда как для защиты сложных приложений лучше подходят NGFW. Роль файрволов в сетевой безопасности заключается в фильтрации трафика, предотвращающей проникновение вредоносных данных в сеть. Вопрос о том, как тип файрвола влияет на сетевую защиту, подчеркивает необходимость выбора подходящего решения, которое балансирует между производительностью, глубиной анализа и уровнем защиты, адаптируясь к конкретным угрозам и архитектуре сети.

2. Брандмауэры на сетевом уровне

Брандмауэры, функционирующие на сетевом уровне (уровень 3 модели OSI), обеспечивают базовую защиту сети, фильтруя трафик на основе информации в заголовках пакетов, таких как IP-адреса, порты и протоколы. Эти устройства, часто реализованные в виде списков контроля доступа (ACL) на маршрутизаторах, проверяют каждый пакет независимо, пропуская или блокируя его в соответствии с заданными правилами. Например, ACL на маршрутизаторе может быть настроен для блокировки входящего трафика с определённых IP-адресов, связанных с известными источниками атак, или для разрешения только SSH-соединений (порт 22) с доверенных устройств. Такая фильтрация эффективно предотвращает несанкционированный доступ и атаки, такие как сканирование портов, при котором злоумышленники ищут открытые уязвимости.

Брандмауэры сетевого уровня особенно полезны для защиты периметра сети, где они служат первой линией обороны против внешних угроз. Например, в корпоративной сети маршрутизатор с ACL может блокировать весь входящий трафик, кроме необходимого для работы веб-сервера, снижая риск DDoS-атак или эксплуатации уязвимостей. Однако их ограничением является отсутствие анализа содержимого пакетов или контекста соединений, что делает их менее эффективными против атак, использующих легитимные

порты или поддельные IP-адреса (IP-спуфинг). Для повышения защиты сетевые файрволы часто дополняются механизмами отслеживания состояния, которые учитывают активные сессии. Роль брандмауэров на сетевом уровне в сетевой безопасности заключается в блокировке вредоносного трафика, создавая барьер против базовых атак. Вопрос о том, как сетевые файрволы защищают от атак, подчеркивает их способность быстро фильтровать трафик на основе простых правил, минимизируя нагрузку на внутренние ресурсы сети.

3. Брандмауэры на прикладном уровне

Брандмауэры, работающие на прикладном уровне (уровень 7 модели OSI), обеспечивают более глубокую защиту, анализируя содержимое трафика и поведение приложений. Эти устройства, такие как веб-файрволы (WAF), используют глубокий анализ пакетов (DPI), чтобы проверять данные, передаваемые через протоколы, такие как HTTP или FTP, выявляя подозрительные шаблоны, например, попытки SQL-инъекций или XSS-атак (межсайтовый скриптинг). WAF, установленный перед веб-сервером, может анализировать входящие запросы, блокируя вредоносные скрипты или запросы, нарушающие нормальные шаблоны использования приложения. Например, в интернет-магазине WAF может предотвратить атаку, направленную на ввод вредоносного SQL-кода в форму поиска, защищая базу данных от компрометации.

Брандмауэры прикладного уровня особенно важны для защиты веб-приложений, которые становятся основной мишенью современных атак. В отличие от сетевых файрволов, они способны распознавать контекст трафика, например, различая легитимные HTTP-запросы от попыток эксплуатации уязвимостей. Однако их работа требует значительных вычислительных ресурсов, что может замедлить обработку трафика, особенно в сетях с высокой нагрузкой. Для повышения эффективности WAF часто интегрируются с другими системами, такими как системы предотвращения вторжений (IPS), для автоматического реагирования на угрозы. Роль брандмауэров на прикладном уровне в сетевой безопасности заключается в защите от атак, нацеленных на приложения, дополняя фильтрацию сетевого уровня. Вопрос о том, как WAF дополняет сетевую защиту, подчеркивает его способность предотвращать сложные атаки, которые проходят через базовые фильтры, обеспечивая безопасность критических сервисов.

4. Мониторинг файрволов в сетях

Мониторинг межсетевых экранов является неотъемлемой частью их эффективного функционирования, позволяя организациям выявлять и реагировать на сетевые инциденты в реальном времени. Этот процесс включает анализ логов файрволов, которые содержат информацию о заблокированном или разрешённом трафике, а также интеграцию с системами

управления безопасностью информации (SIEM) для централизованного сбора и анализа данных. Например, анализ логов файрвола может выявить многократные попытки подключения к закрытым портам, что указывает на попытку сканирования сети, или резкий рост трафика, характерный для DDoS-атаки. SIEM-системы усиливают мониторинг, коррелируя данные от файрволов с другими источниками, такими как IDS/IPS, для выявления сложных атак, которые могут остаться незамеченными при анализе одного устройства.

Мониторинг также помогает в оптимизации правил файрволов, выявляя устаревшие или избыточные настройки, которые могут снизить производительность или создать уязвимости. Например, если логи показывают, что определённое правило ACL редко используется, его можно удалить, упрощая конфигурацию и ускоряя обработку трафика. Кроме того, мониторинг позволяет проводить ретроспективный анализ инцидентов, чтобы улучшить защиту. Например, обнаружение DDoS-атаки через анализ логов файрвола может привести к добавлению новых правил для ограничения трафика с подозрительных IP-адресов. Роль мониторинга файрволов в сетевой безопасности заключается в обнаружении инцидентов и поддержании актуальности защитных мер. Вопрос о том, как мониторинг файрволов предотвращает сетевые атаки, подчеркивает его способность обеспечивать видимость и контроль, позволяя своевременно реагировать на угрозы и укреплять сетевую защиту.

Межсетевые экраны, функционирующие на различных уровнях модели OSI, являются неотъемлемой частью сетевой безопасности, обеспечивая фильтрацию трафика, защиту приложений и мониторинг активности. Разнообразие типов файрволов — от пакетных фильтров до NGFW — позволяет адаптировать защиту к специфическим потребностям сети, балансируя между производительностью и глубиной анализа. Сетевые файрволы блокируют вредоносный трафик, создавая барьер на уровне IP-адресов и портов. Прикладные файрволы, такие как WAF, защищают от атак на приложения, анализируя содержимое трафика. Мониторинг обеспечивает видимость и контроль, выявляя инциденты и оптимизируя настройки. Вместе эти элементы создают многоуровневую систему защиты, которая укрепляет сетевую инфраструктуру, противостоя современным киберугрозам, таким как DDoS, MitM или эксплуатация уязвимостей приложений.

Литература:

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL:

https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 2, 4).

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный (гл. 12, 13).

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст : электронный (гл. 1).

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный (гл. 2).

Контрольные вопросы

1. Фильтрация пакетов.
2. Межсетевые экраны прикладного уровня.
3. Межсетевые экраны с динамической фильтрацией пакетов.
4. Межсетевые экраны инспекции состояний.
5. Межсетевые экраны уровня ядра.

2.2.7 Тема 2.7 Виртуальные частные сети

Перечень изучаемых вопросов

1. Туннелирование.
2. Протоколы VPN транспортного уровня
3. Протокол L2TP

Методические указания к изучению

1. Туннелирование

Туннелирование является фундаментальным механизмом работы виртуальных частных сетей, позволяя передавать данные через виртуальный защищённый канал, созданный внутри незащищённой сети, такой как интернет. Этот процесс заключается в инкапсуляции пакетов данных одного протокола в пакеты другого, что скрывает содержимое и, при необходимости, источник трафика от внешних наблюдателей. В контексте сетевой безопасности туннелирование обеспечивает конфиденциальность и целостность данных, защищая их от перехвата или модификации. Например, в корпоративной сети туннелирование позволяет филиалу компании безопасно обмениваться данными с центральным офисом, передавая конфиденциальную информацию, такую как финансовые отчёты или клиентские данные, через зашифрованный канал, недоступный для злоумышленников.

Для повышения безопасности туннелирование часто сочетается с шифрованием и аутентификацией. Протоколы, такие как IPSec, могут шифровать данные внутри туннеля, используя алгоритмы, такие как AES, чтобы предотвратить их чтение в случае перехвата. Аутентификация, реализованная через сертификаты или предварительно разделённые ключи, подтверждает подлинность участников соединения, защищая от атак MitM. Например, в сценарии удалённого доступа сотрудник может использовать VPN для подключения к корпоративной сети, где туннелирование скрывает структуру сети и защищает данные от анализа трафика. Однако безопасность туннелирования зависит от правильной настройки: слабые алгоритмы шифрования или компрометация ключей могут сделать туннель уязвимым. Роль туннелирования в сетевой безопасности заключается в создании изолированного канала для передачи данных, минимизируя риски компрометации и обеспечивая безопасное соединение между узлами. Вопрос о том, как туннелирование повышает сетевую безопасность, подчеркивает его способность скрывать данные и защищать их от внешних угроз, создавая основу для работы других VPN-протоколов.

2. Протоколы VPN транспортного уровня

Протоколы VPN, функционирующие на транспортном уровне модели OSI (уровень 4), обеспечивают безопасную передачу данных, управляя соединениями между устройствами и защищая их с помощью шифрования и аутентификации. Эти протоколы, такие как PPTP (Point-to-Point Tunneling Protocol), SSTP (Secure Socket Tunneling Protocol) и OpenVPN, работают поверх туннелей, созданных на канальном или сетевом уровне, добавляя дополнительный слой защиты. Например, SSTP использует SSL/TLS для шифрования данных, что делает его устойчивым к атакам, направленным на перехват трафика, и позволяет интегрироваться с инфраструктурой HTTPS, упрощая настройку в корпоративных сетях. В таких сетях SSTP может обеспечивать безопасный доступ удалённых сотрудников к внутренним

ресурсам, таким как CRM-системы или файловые серверы, даже при использовании общественных Wi-Fi-сетей.

Ключевой особенностью протоколов транспортного уровня является их способность обеспечивать надёжную доставку данных, сочетая туннелирование с криптографическими механизмами. Например, OpenVPN поддерживает гибкую настройку шифрования, используя библиотеки OpenSSL, что позволяет применять современные алгоритмы, такие как AES-256, и защищать данные от перехвата. PPTP, хотя и менее безопасен из-за устаревших алгоритмов, таких как MS-CHAP, исторически использовался для простых VPN-соединений, но его использование сейчас ограничено из-за уязвимостей. Выбор протокола требует учёта баланса между безопасностью и производительностью: сложные алгоритмы шифрования увеличивают задержки, что может быть критично для приложений, требующих низкой латентности, таких как видеоконференции. Роль протоколов транспортного уровня в сетевой безопасности заключается в обеспечении защищённых соединений, предотвращающих компрометацию данных. Вопрос о том, как протоколы транспортного уровня повышают безопасность VPN, подчеркивает их способность сочетать шифрование и аутентификацию для защиты данных, передаваемых через небезопасные сети.

3. Протокол L2TP

Протокол L2TP (Layer 2 Tunneling Protocol) является одним из наиболее популярных протоколов для создания VPN, работающим на канальном уровне, но часто используемым в сочетании с протоколами транспортного уровня, такими как IPSec, для обеспечения безопасности. L2TP создаёт туннель, инкапсулируя данные канального уровня, что позволяет передавать их через интернет, сохраняя структуру локальной сети. Поскольку L2TP сам по себе не предоставляет шифрования, он обычно комбинируется с IPSec, который добавляет шифрование и аутентификацию, используя алгоритмы, такие как AES, и механизмы, такие как сертификаты или предварительно разделённые ключи. Например, в корпоративной сети L2TP/IPSec используется для создания VPN, позволяя сотрудникам безопасно подключаться к внутренним серверам из удалённых локаций, таких как кафе или аэропорты, защищая данные от перехвата в общественных сетях.

Настройка L2TP/IPSec демонстрирует его преимущества для сетевой безопасности. L2TP обеспечивает туннелирование, позволяя передавать данные, такие как PPP-пакеты, через интернет, а IPSec добавляет шифрование и аутентификацию, предотвращая атаки, такие как MitM или подделка данных. Например, сотрудник, использующий L2TP/IPSec VPN, может безопасно работать с корпоративными приложениями, передавая конфиденциальные данные через зашифрованный канал. Однако L2TP/IPSec требует тщательной настройки: слабые ключи или устаревшие алгоритмы

шифрования могут снизить его эффективность. Кроме того, L2TP может быть заблокирован в сетях с жёсткими ограничениями NAT или файрволами, что требует использования альтернатив, таких как SSTP или OpenVPN. Роль L2TP в сетевой безопасности заключается в создании надёжных туннелей для удалённого доступа, интегрированных с мощными механизмами шифрования. Вопрос о том, как L2TP повышает безопасность VPN, подчеркивает его способность обеспечивать туннелирование в сочетании с шифрованием, создавая защищённый канал для передачи данных.

Виртуальные частные сети являются важным элементом сетевой безопасности, обеспечивая защищённую передачу данных в условиях небезопасных сетей. Туннелирование создаёт виртуальные каналы, скрывая данные и защищая их от перехвата, что делает его основой VPN. Протоколы транспортного уровня, такие как SSTP и OpenVPN, обеспечивают надёжную доставку данных, сочетая туннелирование с шифрованием и аутентификацией, что предотвращает компрометацию. L2TP, особенно в комбинации с IPSec, предоставляет гибкое решение для создания безопасных VPN, защищая удалённые подключения от атак. Вместе эти механизмы формируют комплексную систему защиты, которая обеспечивает конфиденциальность, целостность и аутентичность данных, позволяя организациям поддерживать безопасные соединения в условиях современных киберугроз.

Литература

1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва : НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный (гл. 5).

Контрольные вопросы

1. Привести особенности порядка реагирования на вторжения в интернет-сети и организационно-правовые вопросы.
2. Указать и охарактеризовать сохранение доказательств вторжения.
3. Протоколы VPN транспортного уровня.

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. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО КУРСОВОМУ ПРОЕКТУ

Подробные указания приведены в учебно-методическом пособии по выполнению курсовых проектов для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» по дисциплине «Безопасность вычислительных систем»

Цели каждой отдельной курсового проекта должны раскрывать выбранную студентом тему. Курсовой проект предназначена для углубления студентами теоретических и практических навыков в области обеспечения информационной безопасности операционных систем. Современные требования к специалистам предполагают не только глубокое знание теоретических основ и принципов использования информационных технологий. Будущие специалисты должны иметь четкое представление обо всех этапах создания и эксплуатации информационных технологий, уметь осуществлять выбор из широкого арсенала современных средств и методов защиты информации в операционных системах наиболее адекватные поставленной задаче. Курсовой проект – это одна из форм учебной (творческой и научно-исследовательской) работы, ее выполнение является обязательным для всех студентов очной и заочной форм обучения. Выполнение проекта представляет собой самостоятельное решение студентом под руководством преподавателя частной задачи или проведение исследования по одному из вопросов, изучаемых в цикле специальных дисциплин (по ГОС ВПО) или в дисциплинах профессионального цикла (по ФГОС ВПО). Основной целью выполнения курсовых работ (проектов) является закрепление, углубление и обобщение знаний, полученных студентом за время теоретического и практического обучения, расширение объема профессионально значимых умений и навыков. Содержание курсовых работ (проектов) должно отвечать учебным задачам дисциплины, увязываться с последующей работой выпускников по специальности /направлению подготовки.

Поэтому в цели и задачи проекта входят:

1) закрепление практических навыков настройки политик безопасности операционных систем, полученных на лабораторных занятиях по дисциплине «Безопасность операционных систем»;

2) углубление теоретических и практических знаний в области методологии отладки политик безопасности операционных систем;

3) развитие навыков самостоятельного планирования задач защиты операций и ключевой информации операционных систем;

4) получение опыта сбора регистрируемых событий, и обработки регистрируемых событий в операционной системе;

5) приобретение навыков создания резервных копий операционных систем.

Выполнение проекта позволяет расширить и закрепить приобретенные студентом в ходе обучения в вузе теоретические знания и продемонстрировать полученные навыки по самостоятельной постановке и решению конкретной задачи, а также продемонстрировать владение профессиональными навыкам в области защиты информации.

При выполнении проекта обучающимся рекомендуется использование элементов дистанционных образовательных технологий с использованием информационных и учебно-методических ресурсов. При этом график проекта должен определяться количеством часов, указанным в учебном плане.

Важнейшими требованиями при выполнении курсового проекта для студента являются ее самостоятельность и актуальность, связанная с решением вопросов по заданиям или по тематике работ промышленных, коммерческих или научно-исследовательских организаций; использованием современной программной и аппаратной базы; справочных материалов; новейших методов организации расчетов, проектирования и исследований.

Обучающийся выбирает тему курсового проекта из числа предложенных тем. При выборе темы курсового проекта (КР) необходимо учесть возможность дальнейшего ее развития, углубления и конкретизации, а также использования в курсовой работе.

Обучающийся может предложить свою тему с обоснованием целесообразности ее разработки и при согласовании с заведующим кафедрой и/или научным руководителем.

Выбранная тема курсового проекта должна быть согласована с научным руководителем. Изменения темы курсового проекта могут быть внесены только после согласования с научным руководителем.

При выборе темы курсового проекта необходимо учитывать следующие условия:

– соответствие темы курсового проекта содержанию дисциплины, по которой выполняется работа; актуальность проблемы;

– наличие специальной литературы и возможность получения фактических данных, необходимых для анализа;

– собственные научные интересы и способности обучающегося; преемственность исследований, начатых в предыдущих курсовых работах (проектах) и в период учебных практик;

– исключение по возможности дублирования (дословного совпадения формулировок) тем курсовых работ (проектов), выполняемых обучающимися (группой обучающихся).

Также при самостоятельном определении темы студенту требуется учесть свой опыт в выбранной сфере, наличие соответствующих знаний и навыков, а также имеющихся наработок по предполагаемой тематике. Это, прежде всего, относится к тем, кто долго собирал и обрабатывал материал по той или иной проблематике, участвовал в НИРС, научных конференциях, имеет публикации в научных журналах, сборниках и т. д. Научный руководитель может быть преподаватель выпускающей кафедры

Студенту следует периодически информировать научного руководителя о ходе выполнения курсового проекта, консультироваться по вызывающим затруднения или сомнения теоретическим и практическим вопросам, обязательно ставить в известность о возможных проблемах в выполнении работы и её содержания. Изменение выбранной ранее темы курсового проекта возможно при согласовании с научным руководителем.

работа выполняется студентом в период семестра, когда по учебному плану изучается соответствующая дисциплина.

работа представляет собой решение практической, научно-исследовательской задачи одной из актуальных проблем в области защиты операционных систем,

Объектами курсового проекта могут быть методы поиска уязвимостей операционных систем, методы анализа уязвимости операционных, способы повышения защищенности операционных систем, специфика комплектования системного обеспечения в целях повышения информационной безопасности.

При выполнении курсового проекта должно быть предусмотрено:

– обоснование актуальности и важности решаемой задачи обеспечения информационной безопасности выбранного объекта;

– анализ проблемной области защиты операционных систем;

– определение, анализ возможных путей и способов исследования и описание выбранных методов и средств решения поставленных задач;

– методы и способы решения проблем безопасности операционных систем.

При определении темы и соответственно порядка разработки курсового проекта можно придерживаться следующего плана:

– точная формулировка темы, целей и задач выполнения курсового проекта;

– изучение специфики проблемной области;

– выявление уже существующих решений и определение их эффективности

– обоснование предложений по решению проблем в области информационной защиты операционных систем;

– реализация предложенных средств и методов защиты, исследования меры защищенности операционных систем и их компонентов;

– проверка работоспособности предложенных мер защиты.

Работа предусматривает **следующие этапы:**

1. **Подготовка** к выполнению курсового проекта заключается в изучении литературы по выбранной проблеме, сборе исходных данных по рассматриваемым проблемам. На этом этапе изучаются цели функционирования и развития объекта, его обеспеченность средствами защиты, каналы уязвимости, Студент собирает, обобщает и систематизирует материалы, необходимые для разработки предложений Полученные материалы используются во введении и аналитической части работы.

2. Разработка темы. На основе собранных и обобщенных материалов, формулируются способы решения задач и разрабатываются алгоритмы решения задач, определяется специфика и порядок их реализации, реализуются предложенные решения, обосновывается эффективность разработки, исследований, решений.

3. Этап включает оформление курсового проекта. При этом выполняется:

– систематизация и обработка материалов курсового проекта;

– отбор материала для оформления содержательной части работы и составление структуры ее изложения, подготовка необходимого иллюстративного материала и т. д.;

– определение направлений и основного содержания предложений, выявление необходимости дополнительного сбора материалов; формирование чернового варианта разработки в целом;

– сбор дополнительных материалов, детальная разработка и обоснование выдвинутых предложений;

– уточнение аналитической и исследовательской части работы;

– редактирование и окончательное оформление отобранного материала;

– оформление иллюстративного материала.

4. Заключительным этапом подготовки курсового проекта к защите является предъявление ее преподавателю ИБ. К этому моменту работа должна быть подписана студентом.

Список типовых (примерных) тем

Темы курсовых проектов

1. IPSec протокол.
2. Протокол L2TP.
3. Концентратор доступа LAC.

4. Сервер LNS.

5. протоколом PPP.

6. Протокол Internet Protocol Security (IPSec).

7. Протокол SSL.

8. Протокол TSL.

9. Протокол SOCKS.

10. Схемы применения IPSec.

11. Система правил избирательное разграничение доступа.

12. Протокол LDAP.

13. Протокол Kerberos.

14. Протокол DNS.

15. VPN-серверы.

16. Протоколы VPN транспортного уровня.

17. ISA-серверы.

18. Протокол SOCKS. SOCKS-сервер.

19. Дополнительные возможности МЭ. Реагирование на задаваемые события.

20. Разработка схемы сетевой защиты на базе межсетевых экранов.

21. Фильтрация пакетов.

22. Межсетевые экраны прикладного уровня.

23. Межсетевые экраны с динамической фильтрацией пакетов.

24. Межсетевые экраны инспекции состояний.

25. Межсетевые экраны уровня ядра.

26. Протокол L2F.

Методические указания по выполнению расчетно-графической работы – нет.

6. 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, курсовой проект.

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 %**
	«неудовлетво-рительно»	**«удовлетво-рительно»**	**«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, либо в состоянии находить отдельные фрагменты информации в рамках	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпрети-ровать и систематизи-ровать необходимую информацию в рамках поставленной	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в

Система оценок / Критерий				
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетво-рительно»	**«удовлетво-рительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
	поставленной задачи		задачи	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 предостав-ленной информации	В состоянии осуществлять систематичес-кий и научно-корректный анализ предоставлен-ной 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 профессиональ ных 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. Обобщённые категории атак и их краткая характеристика.
2. Охарактеризуйте распространенные приемы хакеров и методы защиты от их реализаций.
3. Сетевые атаки. Общая классификация по технологиям.
4. Кратко охарактеризуйте известные атаки на канальном уровне OSI
5. Раскройте специфику атаки «Переполнение CAM-таблицы». Приведите способы защиты от нее.
6. Раскройте специфику атаки «VLAN Hoping». Приведите способы защиты от нее.
7. Раскройте специфику атаки на STP. Приведите способы защиты от нее.
8. Раскройте специфику атак на PVLAN, на DHCP. Приведите способы защиты от них.
9. Раскройте специфику атаки ARP-spoofing. Приведите способы защиты от нее.
10. Кратко охарактеризуйте известные атаки на сетевом уровне OSI.
11. Раскройте специфику атак на маршрутизаторы.
12. Раскройте специфику атак на среды с протоколом RIP с использованием ложных маршрутов. Приведите способы защиты.
13. Раскройте специфику атак на среды с протоколом RIP с использованием взлома хеша MD5 и понижением версий. Приведите способы защиты.
14. Раскройте специфику атак на среды с протоколом OSPF с использованием ложных маршрутов. Приведите способы защиты.
15. Раскройте специфику атак на среды с протоколом BGP с использованием router masquerading, взлома хеша MD5. Приведите способы защиты.
16. Раскройте специфику атак на среды с протоколом BGP с «слепого DOS» и других способов (кроме использования router masquerading, взлома хеша MD5). Приведите способы защиты.
17. Раскройте специфику атак на среды с протоколом IS-IS. Приведите способы защиты.

18. Раскройте специфику атак на среды с протоколом MPLS. Приведите способы защиты.

19. Раскройте специфику протокола IPSec.

20. Раскройте специфику защиты с сетей с учетом масштабов и конфигураций.

Вопросы к экзамену

1. Обобщённые категории атак и х краткая характеристика.

2. Охарактеризуйте распространенные приемы хакеров и методы защиты от их реализаций.

3. Сетевые атаки. Общая классификация по технологиям.

4. Кратко охарактеризуйте известные атаки на канальном уровне OSI.

5. Раскройте специфику атаки «Переполнение CAM-таблицы». Приведите способы защиты от нее.

6. Раскройте специфику атаки «VLAN Hoping». Приведите способы защиты от нее.

7. Раскройте специфику атаки на STP. Приведите способы защиты от нее.

8. Раскройте специфику атак на PVLAN, на DHCP. Приведите способы защиты от них.

9. Раскройте специфику атаки ARP-spoofing. Приведите способы защиты от нее.

10. Кратко охарактеризуйте известные атаки на сетевом уровне OSI.

11. Раскройте специфику атак на маршрутизаторы.

12. Раскройте специфику атак на среды с протоколом RIP с использованием ложных маршрутов. Приведите способы защиты.

13. Раскройте специфику атак на среды с протоколом RIP с использованием взлома хеша MD5 и понижением версий. Приведите способы защиты.

14. Раскройте специфику атак на среды с протоколом OSPF с использованием ложных маршрутов. Приведите способы защиты.

15. Раскройте специфику атак на среды с протоколом BGP с использованием router masquerading, взлома хеша MD5. Приведите способы защиты.

16. Раскройте специфику атак на среды с протоколом BGP с «слепого DOS» и других способов (кроме использования router masquerading, взлома хеша MD5). Приведите способы защиты.

17. Раскройте специфику атак на среды с протоколом IS-IS. Приведите способы защиты.

18. Раскройте специфику атак на среды с протоколом MPLS. Приведите способы защиты.

19. Раскройте специфику протокола IPSec.

20. Раскройте специфику защиты с сетей с учетом масштабов и конфигураций.

21. Приведите классификацию МЭ. Раскройте специфику защиты с использованием МЭ пакетного типа.

22. Приведите классификацию МЭ. Раскройте специфику защиты с использованием МЭ сеансового типа.

23. Приведите классификацию МЭ. Раскройте специфику защиты с использованием МЭ сеансового типа.

24. Раскройте специфику функционирования МЭ.

25. Протоколы SSL и TLS.

26. Протокол SOCKS.

27. Протокол PPTP, L2TP.

28. Защиты трафика в WiFi-сетях.

29. Опишите способы защиты сетей с использование распределения доступа и настроек протокольных сред в сетях домен в Windows Server (по лаб. раб.).

30. Опишите способы защиты сетей с использование распределения доступа и настроек протокольных сред в сетях Cisco (по лаб. раб.)

31. Опишите способы защиты сетей с использование распределения доступа и настроек протокольных сред в сетях Cisco (по лаб. раб.)

32. Опишите способы защиты сетей с использование технологий VPN (OpenVPN) (по лаб. раб. и лек.)

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. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. – Москва: НИЯУ МИФИ, 2023. – 224 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/355511 (дата обращения: 06.12.2024). – ISBN 978-5-7262-2949-2. – Текст : электронный.

2. Воробьев, С. П. Компьютерные сети и сетевая безопасность: учеб. пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. – Новочеркасск: ЮРГПУ (НПИ), 2022. – 216 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/292247 (дата обращения: 06.12.2024). – ISBN 978-5-9997-0805-2. – Текст : электронный.

3. Магомедов, Ш. Г. Интеллектуальные методы защиты вычислительных комплексов от сетевых атак: учеб. пособие / Ш. Г. Магомедов, В. П. Фраленко, В. М. Хачумов. – Москва: РТУ МИРЭА, 2022. – 120 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/311249 (дата обращения: 06.12.2024). – Текст : электронный.

4. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба; ред. О. В. Маер; Омский государственный технический университет. – Омск: Омский государственный технический университет (ОмГТУ), 2021. – 119 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700833 (дата обращения: 06.12.2024). – ISBN 978-5-8149-3250-1. – Текст : электронный.

5. 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.

6. Безопасность беспроводных локальных сетей: учеб. пособие / М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг, К. А. Ахрамеева. – Санкт-Петербург: СПбГУТ им. М. А. Бонч-Бруевича, 2021. – 71 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/279623 (дата обращения: 06.12.2024). – ISBN 978-5-89160-227-4. – Текст : электронный.

Дополнительные источники

1. Национальная безопасность: учебник / В. И. Абрамов, М. А. Газимагомедов, К. К. Гасанов [и др.]; под ред. К. К. Гасанова, Н. Д. Эриашвили, О. А. Мироновой. – 3-е изд., перераб. и доп. – Москва: Юнити-Дана, 2023. – 288 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=700171 (дата обращения: 05.11.2024). – ISBN 978-5-238-03639-7. – Текст : электронный.

2. 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.

3. Мэйволд, Э. Безопасность сетей: учеб. пособие / Э. Мэйволд. – 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 09.11.2024). – Текст : электронный.

4. Бурлаков, М. Е. Контроль защищенности локальных вычислительных сетей от несанкционированного доступа. Лабораторный практикум: учеб. пособие / М. Е. Бурлаков, М. Н. Осипов. – Самара: Самарский университет, 2022. – 116 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/336473 (дата обращения: 06.12.2024). – ISBN 978-5-7883-1749-6. – Текст : электронный.

5. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учеб. пособие / А. Г. Киренберг. – Кемерово: КузГТУ имени 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.

6. Введение в информационную безопасность и защиту информации: учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск: НГТУ, 2017. – 132 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/118219 (дата обращения: 06.12.2024). – ISBN 978-5-7782-3233-4. – Текст : электронный.

Учебно-методические пособия, нормативная литература

1. Подтопельный, В. В. Безопасность вычислительных сетей: учеб.-метод. 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», 2022. – 130 с. – URL: https://www.klgtu.ru/vikon/sveden/files/ain/UMP_Bezopasnosty_vychis litelynyx_setei.pdf (дата обращения: 08.12.2024). – Текст : электронный.

2. Подтопельный, В. В. Безопасность вычислительных сетей: учеб.-метод. пособие по выполнению лабораторных работ по дисциплине для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / В. В. Подтопельный – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 42 с. – URL: https://www.klgtu.ru/vikon/sveden/files/zie/UMP_Bezopasnosty_vychis litelynyx_setei_(laboratornye_raboty).pdf (дата обращения: 08.12.2024). – Текст : электронный.

3. Подтопельный, В. В. Безопасность вычислительных сетей: учеб.-метод. пособие по выполнению курсовых проектов для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых вычислительных сетей». – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 56 с. – URL: https://www.klgtu.ru/vikon/sveden/files/ril/UMP_Bezopasnosty_vychisl itelynyx_setei_(kursovoi_proekt).pdf (дата обращения: 08.12.2024). – Текст : электронный.

4. «Доктрина информационной безопасности Российской Федерации» (утв. Указом Президентом РФ 05.12.2016 № 646 (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

5. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

6. Федеральный закон от 28.12.2010 N 390-ФЗ О безопасности» (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

7. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

8. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

9. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

10. Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера» (в действующей редакции). – Режим доступа: для авториз. пользователей из справ. – правовой системы КонсультантПлюс. – Текст: электронный.

11. «ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят и введен в действие Постановлением Госстандарта РФ от 09.02.1995 N 49) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

12. «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 373-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

13. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. Решением Гостехкомиссии России от 30.03.1992) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

14. «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Решением Гостехкомиссии России 30.03.1992) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

Локальный электронный методический материал

Владислав Владимирович Подтопельный

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 5,4. Печ. л. 4,9.

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