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

В. В. Подтопельный

ТЕОРИЯ АНАЛИЗА КОМПЬЮТЕРНЫХ АТАК

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.
Теория анализа компьютерных атак: 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. – 59 с.

Учебно-методическое пособие включает в себя рассмотрение теоретических вопросов в области защиты информации по дисциплине «Теория анализа компьютерных атак». 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 дисциплины. Пособие предназначено для студентов 3-го курса специальности 10.05.03 «Информационная безопасность автоматизированных систем».
Табл. 2, список лит. – 25 наименований

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» от 26 мая 2025 г., протокол № 4

УДК 004.056(076)

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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

Цель освоения дисциплины: обеспечение целостности (физической и логической) информации, а также предупреждение несанкционированной ее модификации, несанкционированного получения и размножения

Компетенции:

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

знать:

– способы поиска и анализа уязвимостей;

– методы учета уязвимостей, метрические спецификации уязвимостей и угроз;

– методы моделирования компьютерных атак и их исследование, и методы анализа компьютерных атак;

уметь:

– осуществлять поиск уязвимостей;

– использовать методы определения метрических характеристик уязвимостей;

– моделировать компьютерные атаки и анализировать, и прогнозировать с учетом специфики информационных систем и нарушителей;

владеть:

– владеть навыком поиска и анализа уязвимостей, угроз;

– определения специфических характеристик атак с учетом особенностей информационных систем;

– владеть навыкам анализа компьютерных атак различными методами.

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествует «Безопасность операционных систем.

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

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

иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Требования к аттестации» 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 УМПД, 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

1.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):

– OSSEC (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом);

– Ethereal (Программы перехвата и анализа сетевых пакетов);

Типовое ПО на всех ПК:

1. Операционная система Windows 7 (получаемая по программе Microsoft «Open Value Subscription»).

2. Офисное приложение MS Office Standard 2016 (получаемое по программе Microsoft «Open Value Subscription»).

3. Kaspersky Endpoint Security

4. Google Chrome (GNU).

5. Учебный комплект программного обеспечения КОМПАС-3D v21.

6. MathCAD 15 M020.

7. Python (GNU/Linux,macOS и Windows).

8. PascalABC.Net.

9. 1C:Enterprise 8.

10. Blender.

11. GPSS World Student Version.

12. Microsoft Visual Studio Code (получаемоепопрограмме Microsoft «Open Value Subscription»).

13. Oracle VM VirtualBox (GNU/Linux, macOS и Windows) 14. QGIS

1. ТЕМАТИЧЕСКИЙ ПЛАН

Таблица 1 – Тематический план

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
Лекции (5-й семестр –16 ч ауд., 54,85 ч – сам. р.)				
1.1	Методы обнаружения атак и анализа компьютерных атак	Классификации методов обнаружения атак и анализа компьютерных атак	4	10
1.2	Методы обнаружения атак и анализа компьютерных атак	Методы обнаружения на основе поведенческого анализа, машинного обучения, методы вычислительного интеллекта	4	10
1.3	Методы обнаружения атак и анализа компьютерных атак	Специфика анализа атак как процессов реализации угроз	4	10
1.4	Методы обнаружения атак и анализа компьютерных атак	Аналитическое моделирование процессов реализации угроз	4	24,85
Лекции (6-й семестр – 32 ч ауд., 34 ч – сам. р.)				
2.1	Методы моделирования компьютерных атак	Методика анализа и регулирования рисков при реализации нескольких угроз удаленного доступа к элементам ИТКС	8	10
2.2	Методы моделирования компьютерных атак	Метод натурного и имитационного моделирования процессов противодействия компьютерным атакам на критически важные информационные системы	8	10
2.3	Методы моделирования компьютерных атак	Метод экспериментальной оценки эффективности компьютерных атак	8	10
2.4	Методы моделирования компьютерных атак	Метод оценки эффективности активного противодействия компьютерным атакам на критически важные информационные системы	8	4
			48	**88,85**

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Практические занятия (5-й семестр)		
1.	Методы обнаружения атак и анализа компьютерных атак	Специфика применения методов обнаружения атак и анализа компьютерных атак	8	-
2.	Методы обнаружения атак и анализа компьютерных атак	Использование методов вычислительного интеллекта для анализа компьютерных атак	8	-
3.	Методы обнаружения атак и анализа компьютерных атак	Специфика анализа атак как процессов реализации угроз	8	-
4.	Методы обнаружения атак и анализа компьютерных атак	Аналитическое моделирование процессов реализации угроз	8	-
		Всего за семестр:	32	
		Практические занятия (6-й семестр)		
1.	Методы моделирования компьютерных атак	Методика анализа и регулирования рисков при реализации нескольких угроз	8	-
2.	Методы моделирования компьютерных атак	Метод натурного и имитационного моделирования процессов компьютерных атак и противодействия им	8	-
3.	Методы моделирования компьютерных атак	Метод экспериментальной оценки эффективности компьютерных атак	8	-
4.	Методы моделирования компьютерных атак	Метод оценки эффективности активного противодействия компьютерным атакам на критически важные информационные системы	8	-
		Всего за семестр:	32	-

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
		Курсовая работа (проект)		
1.1	Название раздела	Контрольная точка 1. Раздел 1	-	-
2.1	Название раздела	Контрольная точка 2. Раздел 2	-	-
		Оформление проекта. Защита	34,75	-
			34,75	**0**
		РЭ	11	
		КА	5,4	
		Рубежный (текущий) и итоговый контроль		
2.1	Название второго раздела	Контроль 1 (не предусмотрен)	-	-
3.1	Название третьего раздела	Контроль 2 (не предусмотрен)	-	-
		Итоговый контроль (зачет)		
		Итоговый контроль (экзамен)		
		Всего		**252**

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

Раздел 1. Методы обнаружения атак и анализа компьютерных атак

Тема 1.1 Введение. Классификации методов обнаружения атак и анализа компьютерных атак.

Перечень изучаемых вопросов

1. Сигнатурные методы
2. Аномальные методы
3. Гибридные системы
4. Классификация по уровню абстракции

Методические указания к изучению

1. Сигнатурные методы обнаружения атак

Сигнатурные методы обнаружения атак основаны на использовании заранее определённых шаблонов (сигнатур), которые соответствуют известным угрозам. Эти шаблоны представляют собой уникальные характеристики вредоносного кода или сетевой активности, такие как последовательности байтов, специфические заголовки пакетов или команды, характерные для эксплойтов. Принцип работы заключается в сравнении анализируемого трафика или данных с базой сигнатур: при совпадении система фиксирует атаку и инициирует защитные меры, такие как блокировка соединения или уведомление администратора.

Примерами инструментов, использующих сигнатурный подход, являются системы обнаружения вторжений (IDS) и антивирусные программы, такие как Snort и ClamAV. Snort, например, анализирует сетевой трафик в реальном времени, используя правила, описывающие сигнатуры атак, такие как попытки эксплуатации уязвимостей в протоколах. ClamAV, в свою очередь, ориентирован на сканирование файловой системы и выявление вредоносных программ по их сигнатурам. Эти инструменты эффективны для обнаружения известных угроз, однако их основное ограничение заключается в неспособности выявлять новые или модифицированные атаки, для которых сигнатуры отсутствуют. Кроме того, постоянное обновление баз сигнатур требует значительных ресурсов, а задержки в обновлении могут привести к уязвимостям.

Методические рекомендации. Для глубокого освоения сигнатурных методов рекомендуется начинать с изучения архитектуры систем обнаружения вторжений, таких как Snort. Студентам следует разобрать синтаксис правил Snort, чтобы понять, как создаются сигнатуры для конкретных атак. Практические занятия должны включать настройку Snort на виртуальной машине и анализ тестового трафика, содержащего известные атаки, такие как SQL-инъекции или эксплойты протокола SMB. Для закрепления теоретических знаний полезно изучить процесс обновления баз сигнатур, включая использование сообществ, таких как Snort VRT. Важно также рассмотреть ограничения метода через анализ реальных кейсов, где сигнатурный подход не позволил выявить угрозу, например, атаки нулевого дня.

2. Методы обнаружения атак на основе аномалий

Эти методы обнаружения атак ориентированы на выявление отклонений от нормального поведения системы, сети или пользователя. В отличие от сигнатурного подхода, эти методы не требуют предварительного знания характеристик атаки, что делает их эффективными для обнаружения новых угроз. Основой аномального подхода является создание базового профиля нормальной активности, который может включать параметры сетевого трафика, системные вызовы или поведение пользователей. Отклонения от этого профиля интерпретируются как потенциальные атаки.

Современные аномальные системы широко используют методы машинного обучения, такие как кластеризация, классификация и нейронные сети. Например, алгоритмы машинного обучения могут анализировать временные ряды сетевого трафика и выявлять аномалии, такие как резкое увеличение числа запросов, характерное для DDoS-атак. Однако аномальные методы сталкиваются с проблемой ложных срабатываний, поскольку не все отклонения от нормы являются атаками. Например, внезапное увеличение активности пользователя может быть связано с легитимной задачей, такой как обработка больших данных. Кроме того, создание точного базового профиля требует значительных вычислительных ресурсов и времени.

Методические рекомендации. Изучение аномальных методов следует начинать с основ статистики и машинного обучения, чтобы студенты могли понять принципы построения моделей нормального поведения. Рекомендуется использовать открытые наборы данных, такие как KDD Cup 1999 или NSL-KDD, для обучения алгоритмов обнаружения аномалий. Практические занятия должны включать настройку инструментов, таких как Zeek (ранее Bro), для мониторинга сети и выявления аномалий. Важно уделить внимание анализу ложных срабатываний: студенты должны научиться интерпретировать результаты и настраивать пороговые значения для минимизации ошибок. Для углубленного изучения можно рассмотреть применение глубоких нейронных сетей в задачах обнаружения аномалий, используя фреймворки, такие как TensorFlow или PyTorch.

3. Гибридные системы обнаружения атак

Гибридные системы объединяют преимущества сигнатурных и аномальных методов, компенсируя их недостатки. Такие системы используют сигнатурный анализ для быстрого и точного обнаружения известных угроз, а аномальный подход — для выявления неизвестных атак. Например, гибридная система может сначала проверить трафик на соответствие базе сигнатур, а затем передать подозрительные, но не идентифицированные пакеты на анализ аномалий. Это позволяет повысить точность обнаружения и снизить количество ложных срабатываний.

Примерами гибридных систем являются Suricata и Cisco Firepower. Suricata поддерживает как сигнатурные правила, так и механизмы поведенческого анализа, что делает её универсальным инструментом для защиты сетей. Cisco Firepower интегрирует сигнатурный анализ с продвинутыми методами машинного обучения, позволяя выявлять сложные атаки, такие как целевые

атаки (APT). Однако гибридные системы требуют сложной настройки и значительных вычислительных ресурсов, что может быть ограничением для небольших организаций.

Методические рекомендации. Для изучения гибридных систем рекомендуется начать с сравнительного анализа сигнатурных и аномальных методов, чтобы студенты понимали, как их комбинация улучшает обнаружение атак. Практические занятия должны включать установку и настройку Suricata в лабораторной среде с последующим анализом смешанного трафика, содержащего как известные, так и неизвестные угрозы. Студентам следует изучить, как Suricata обрабатывает правила и применяет поведенческий анализ, а также провести эксперименты с настройкой чувствительности аномального модуля. Для углубленного изучения можно рассмотреть архитектуру Cisco Firepower, изучив её документацию и кейсы применения в реальных условиях.

4. Классификация методов по уровню абстракции

Методы обнаружения атак классифицируются по уровню абстракции, который определяет, на каком уровне информационной системы осуществляется анализ: сетевом, хостовом или прикладном. Каждый уровень играет уникальную роль в многоуровневой защите, обеспечивая комплексный подход к обнаружению угроз.

На сетевом уровне анализ сосредоточен на мониторинге трафика, проходящего через сетевые устройства. Системы сетевого уровня, такие как Snort или Suricata, анализируют заголовки пакетов, протоколы и содержимое, выявляя атаки, такие как сканирование портов или DDoS. Сетевой уровень эффективен для обнаружения атак, происходящих до достижения целевой системы, но может быть ограничен при анализе зашифрованного трафика.

Хостовый уровень предполагает мониторинг активности на отдельной системе, включая системные вызовы, доступ к файлам и поведение процессов. Инструменты, такие как OSSEC или Sysmon, анализируют журналы событий и системные метрики, выявляя атаки, такие как внедрение вредоносного кода или несанкционированный доступ. Хостовый уровень особенно важен для обнаружения атак, которые обходят сетевые средства защиты.

Прикладной уровень фокусируется на анализе поведения приложений и их взаимодействия с пользователями. Например, системы защиты веб-приложений (WAF), такие как ModSecurity, анализируют HTTP-запросы, выявляя атаки, такие как SQL-инъекции или XSS. Прикладной уровень критически важен для защиты веб-приложений, но требует глубокого понимания их логики.

Многоуровневая защита предполагает интеграцию всех трёх уровней, чтобы обеспечить максимальную устойчивость к атакам. Например, сетевая IDS может выявить попытку сканирования, хостовая система – внедрение вредоносного кода, а WAF – эксплуатацию уязвимости веб-приложения.

Методические рекомендации. Изучение классификации по уровню абстракции следует начинать с анализа архитектуры информационных систем, чтобы студенты понимали, как данные проходят через сетевой, хостовый и прикладной уровни. Практические занятия должны включать настройку ин-

струментов для каждого уровня: Snort для сетевого, OSSEC для хостового и ModSecurity для прикладного. Студентам рекомендуется создать лабораторную среду, имитирующую атаку, например, SQL-инъекцию, и проанализировать, как каждый уровень защиты реагирует на угрозу. Для закрепления знаний полезно изучить концепцию многоуровневой защиты через кейсы, такие как защита корпоративной сети от APT.

Для эффективного изучения темы важно сочетать теоретические лекции, практические занятия и самостоятельную работу. Лекции должны быть структурированы так, чтобы сначала давать обзор каждого метода, а затем углубляться в его технические детали. Практические занятия следует проводить в виртуальной среде, такой как VMware или VirtualBox, где студенты могут безопасно экспериментировать с настройкой инструментов и анализом атак. Самостоятельная работа должна включать изучение документации инструментов, таких как Snort, Suricata или OSSEC, а также анализ реальных кейсов из открытых источников, таких как отчеты MITRE ATT&CK.

Особое внимание следует уделить развитию критического мышления. Студентам нужно задавать вопросы, требующие сравнения методов, например, почему аномальный подход может быть предпочтительнее сигнатурного в определённых сценариях. Также важно включать междисциплинарные элементы, такие как основы статистики для аномальных методов или сетевые протоколы для анализа трафика.

Литература

1. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с. — Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/385979 (дата обращения: 08.10. 2024). – ISBN 978-5-507- 48601-4. – Текст : электронный (гл. 1, 2).

2. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный (гл. 2, 3).

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. Систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный. Ч. 1. – 171 с. (гл. 1.4).

4. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст : электронный (гл. 10).

Контрольные вопросы

1. Каковы основные принципы работы сигнатурных методов обнаружения атак, и какие факторы ограничивают их эффективность при выявлении новых угроз?
2. Каким образом аномальные методы используют машинное обучение для обнаружения атак, и как можно минимизировать проблему ложных срабатываний?
3. В чём заключается преимущество гибридных систем обнаружения атак по сравнению с использованием только сигнатурных или аномальных методов?
4. Как классификация методов обнаружения атак по уровню абстракции способствует реализации многоуровневой защиты информационных систем?
5. Какие инструменты сигнатурного анализа наиболее широко применяются в современных системах обнаружения вторжений, и каковы их основные функции?
6. Каковы основные этапы создания базового профиля нормального поведения в аномальных методах, и какие вызовы возникают на этом этапе?
7. Как сетевой, хостовый и прикладной уровни обнаружения атак взаимодействуют в рамках многоуровневой защиты, и какие угрозы они способны выявить?
8. Какие практические шаги можно предпринять для настройки гибридной системы, такой как Suricata, чтобы оптимизировать её производительность в условиях ограниченных ресурсов?

Тема 1.2 Методы обнаружения на основе поведенческого анализа, машинного обучения, методы вычислительного интеллекта

Перечень изучаемых вопросов

1. Поведенческий анализ
2. Машинное обучение в обнаружении атак
3. Методы вычислительного интеллекта
4. Сравнение эффективности методов

Методические указания

Тема «Методы обнаружения на основе поведенческого анализа, машинного обучения и вычислительного интеллекта» занимает особое место, поскольку она охватывает современные подходы к обнаружению атак, основанные на анализе поведения систем, применении алгоритмов машинного обучения и методов вычислительного интеллекта. Эти подходы позволяют эффективно противостоять сложным и ранее неизвестным угрозам, которые не поддаются выявлению традиционными методами. В данной статье подробно раскрываются вопросы, связанные с поведенческим анализом, применением машинного обучения, методами вычислительного интеллекта и сравнением их эффективности. Особое внимание уделяется методическим рекомендациям, направленным на глубокое освоение материала и развитие практических навыков анализа киберугроз.

1. Поведенческий анализ в обнаружении атак

Поведенческий анализ представляет собой подход к обнаружению компьютерных атак, основанный на мониторинге и интерпретации поведения систем, пользователей или сетевых процессов. В отличие от сигнатурных методов, которые полагаются на заранее известные шаблоны угроз, поведенческий анализ фокусируется на выявлении аномалий, отклоняющихся от нормального поведения. Нормальное поведение определяется через создание базового профиля, который может включать такие параметры, как типичные паттерны сетевого трафика, последовательности системных вызовов, активность пользователей или использование ресурсов системы. Например, резкое увеличение числа исходящих соединений с хоста может указывать на участие в ботнете, а необычные системные вызовы – на выполнение вредоносного кода.

Поведенческий анализ особенно эффективен для обнаружения атак нулевого дня, целевых атак (APT) и инсайдерских угроз, которые не имеют явных сигнатур. Инструменты, реализующие этот подход, такие как Zeek или Splunk с модулями поведенческого анализа, собирают данные из логов, сетевого трафика и системных метрик, после чего применяют алгоритмы для выявления аномалий. Однако поведенческий анализ сталкивается с рядом вызовов. Во-первых, создание точного базового профиля требует длительного наблюдения и может быть затруднено в динамичных системах, где нормальное поведение часто меняется. Во-вторых, высокая чувствительность метода может приводить к ложным срабатываниям, когда легитимные действия ошибочно классифицируются как атаки.

Методические рекомендации. Для освоения поведенческого анализа студентам следует начать с изучения концепции нормального и аномального поведения в информационных системах. Теоретические занятия должны включать разбор структуры базовых профилей и методов их построения, таких как статистический анализ или кластеризация. Практические занятия рекомендуется проводить в лабораторной среде с использованием инструментов, таких как Zeek, для мониторинга сетевого трафика. Студентам полезно настроить систему для анализа тестового трафика, содержащего как нормальную активность, так и имитацию атак, например, сканирование портов или попытки эксплуатации уязвимостей. Для углубленного понимания важно изучить методы снижения ложных срабатываний, включая настройку пороговых значений и использование контекстного анализа. Самостоятельная работа должна включать анализ реальных кейсов, таких как обнаружение APT, с использованием открытых наборов данных, например, Los Alamos National Laboratory dataset.

2. Машинное обучение в обнаружении атак

Машинное обучение (ML) занимает центральное место в современных системах обнаружения атак благодаря способности алгоритмов анализировать большие объемы данных и выявлять сложные закономерности. ML применяется как в аномальном, так и в классификационном подходах. В аномальном подходе алгоритмы, такие как изоляционный лес или автоэнкодеры, обучаются на данных нормального поведения и выявляют отклонения, которые могут указывать на атаку. В классификационном подходе алгоритмы, такие как логистиче-

ская регрессия, деревья решений или нейронные сети, обучаются на маркированных данных, содержащих примеры атак и нормальной активности, чтобы предсказывать класс события (атака или норма).

Применение машинного обучения в обнаружении атак включает несколько этапов: сбор и предварительная обработка данных, выбор и обучение модели, а также тестирование и настройка. Например, для обнаружения DDoS-атак модель может быть обучена на характеристиках сетевого трафика, таких как объем пакетов, частота запросов и распределение портов. Инструменты, такие как TensorFlow, PyTorch или специализированные платформы, например, Darktrace, позволяют реализовать ML-модели для реального времени. Основное преимущество машинного обучения заключается в его способности адаптироваться к новым угрозам и обрабатывать сложные, многомерные данные. Однако ML-модели требуют качественных данных для обучения, а их интерпретируемость может быть ограничена, особенно в случае глубоких нейронных сетей. Кроме того, противники могут использовать атаки на ML-модели, такие как отравление данных, чтобы обойти обнаружение.

Методические рекомендации. Изучение машинного обучения в контексте обнаружения атак следует начинать с основ статистики и теории вероятностей, чтобы студенты понимали принципы работы алгоритмов. Теоретические занятия должны охватывать основные типы ML-алгоритмов (обучение с учителем, без учителя, с подкреплением) и их применение в задачах кибербезопасности. Практические занятия рекомендуется проводить с использованием Python и библиотек, таких как scikit-learn или TensorFlow, для реализации простых моделей, например, классификатора на основе логистической регрессии для обнаружения фишинговых атак. Студентам полезно работать с открытыми наборами данных, такими как NSL-KDD или CICIDS2017, чтобы изучить этапы подготовки данных и обучения моделей. Для углубленного изучения можно рассмотреть атаки на ML-модели, такие как adversarial examples, и методы защиты, включая робастное обучение. Самостоятельная работа должна включать разработку и тестирование ML-модели для конкретной задачи, например, обнаружения вредоносного кода.

3. Методы вычислительного интеллекта

Методы вычислительного интеллекта (CI) представляют собой набор подходов, вдохновлённых природными процессами, которые используются для решения сложных задач обнаружения атак. К ним относятся генетические алгоритмы, искусственные нейронные сети, нечёткая логика, роевой интеллект и их комбинации. Эти методы особенно полезны в ситуациях, где традиционные алгоритмы оказываются неэффективными из-за высокой сложности или неопределённости данных.

Генетические алгоритмы, например, используются для оптимизации правил обнаружения атак, моделируя процесс естественного отбора. Они могут автоматически генерировать новые сигнатуры или настраивать параметры аномальных моделей. Нечёткая логика применяется для обработки неопределённости, позволяя классифицировать события, которые не являются явно нормальными или аномальными. Роевой интеллект, такой как алгоритмы муравьиной

колонии или роя частиц, эффективен для анализа сетевого трафика и поиска оптимальных путей обнаружения атак. Искусственные нейронные сети, входящие в состав вычислительного интеллекта, часто применяются для глубокого анализа данных, например, в системах обнаружения вредоносного кода.

Методы вычислительного интеллекта обладают высокой гибкостью и способностью к адаптации, но их реализация требует значительных вычислительных ресурсов и глубокого понимания их внутренней логики. Кроме того, такие методы могут быть чувствительны к выбору начальных параметров, что влияет на их производительность.

Методические рекомендации. Для освоения методов вычислительного интеллекта студентам следует начать с изучения их биологических и математических основ, таких как принципы эволюции в генетических алгоритмах или нечёткие множества в нечёткой логике. Теоретические занятия должны включать разбор архитектуры каждого метода и примеры их применения в кибербезопасности. Практические занятия рекомендуется проводить с использованием инструментов, таких как MATLAB или Python-библиотеки DEAP (для генетических алгоритмов) и scikit-fuzzy (для нечёткой логики). Студентам полезно реализовать простой генетический алгоритм для оптимизации правил IDS или модель нечёткой логики для классификации сетевых событий. Для углубленного изучения можно рассмотреть гибридные подходы, такие как комбинация нейронных сетей и роевого интеллекта. Самостоятельная работа должна включать анализ научных статей, описывающих применение CI в обнаружении атак, и разработку небольшой модели для решения практической задачи.

4. Сравнение эффективности методов

Сравнение эффективности методов поведенческого анализа, машинного обучения и вычислительного интеллекта является важным аспектом, поскольку позволяет выбрать оптимальный подход для конкретной задачи обнаружения атак. Эффективность методов оценивается по таким критериям, как точность обнаружения, уровень ложных срабатываний, вычислительная сложность, адаптивность к новым угрозам и простота реализации.

Поведенческий анализ отличается высокой чувствительностью к аномалиям, что делает его подходящим для обнаружения неизвестных атак, но его эффективность сильно зависит от качества базового профиля и может быть снижена в динамичных системах. Машинное обучение обеспечивает высокую точность при наличии качественных данных, но требует длительного обучения и может быть уязвимо к атакам на модели. Методы вычислительного интеллекта предлагают гибкость и способность решать нестандартные задачи, но их сложность и ресурсоёмкость ограничивают применение в реальном времени.

Сравнительный анализ показывает, что выбор метода зависит от контекста. Например, в системах с высоким уровнем шума и неопределённости предпочтительны методы вычислительного интеллекта, такие как нечёткая логика. В системах с большим количеством маркированных данных лучше использовать машинное обучение с алгоритмами классификации. Поведенческий анализ оптимален для мониторинга критически важных систем, где важна ранняя детекция аномалий.

Методические рекомендации. Изучение сравнения эффективности методов следует начинать с анализа критериев оценки, таких как точность, полнота и F1-меры. Теоретические занятия должны включать разбор методологий сравнения, таких как кросс-валидация и тестирование на независимых наборах данных. Практические занятия рекомендуется проводить с использованием открытых наборов данных, таких как CICIDS2017, для сравнения производительности разных методов, например, поведенческой модели на основе Zeek, ML-модели на основе scikit-learn и генетического алгоритма на основе DEAP. Студентам полезно разработать сравнительную таблицу, отражающую сильные и слабые стороны каждого метода. Для углубленного изучения можно провести эксперимент, моделирующий реальную атаку, и сравнить время реакции и точность методов. Самостоятельная работа должна включать изучение научных публикаций, посвящённых бенчмаркингу методов обнаружения атак.

Эффективное изучение темы требует интеграции теоретических, практических и самостоятельных форм работы. Теоретические лекции должны быть структурированы так, чтобы сначала давать обзор каждого метода, а затем углубляться в его технические аспекты, включая математические основы и примеры применения. Практические занятия следует проводить в виртуальной среде, такой как Docker или VirtualBox, где студенты могут безопасно экспериментировать с настройкой инструментов и анализом данных. Самостоятельная работа должна включать изучение документации инструментов, таких как Zeek, TensorFlow или DEAP, а также анализ реальных кейсов из открытых источников, таких как MITRE ATT&CK или научные статьи.

Для развития критического мышления студентам следует задавать вопросы, требующие сравнения методов, например, почему машинное обучение может быть предпочтительнее вычислительного интеллекта в определённых сценариях. Междисциплинарный подход, включающий основы статистики, теории алгоритмов и сетевых технологий, способствует более глубокому пониманию материала. Преподавателям рекомендуется использовать интерактивные методы, такие как обсуждение кейсов или соревнования по анализу данных, чтобы повысить вовлечённость студентов.

Тема «Методы обнаружения на основе поведенческого анализа, машинного обучения и вычислительного интеллекта» предоставляет комплексный инструментарий для анализа и противодействия современным киберугрозам. Поведенческий анализ обеспечивает раннее обнаружение аномалий, машинное обучение предлагает мощные средства для обработки больших данных, а методы вычислительного интеллекта открывают возможности для решения сложных задач с высокой неопределённостью. Сравнение эффективности этих методов позволяет выбрать оптимальный подход в зависимости от контекста и ресурсов. Методические рекомендации, предложенные в статье, направлены на обеспечение глубокого освоения материала через сочетание теории, практики и самостоятельной работы. Такой подход формирует у студентов навыки, необходимые для эффективного анализа компьютерных атак и разработки устойчивых систем защиты в условиях динамично развивающегося ландшафта киберугроз.

Литература

1. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/385979 (дата обращения: 08.10. 2024). – ISBN 978-5-507- 48601-4. – Текст : электронный (гл. 2).

2. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный (гл. 3, 13).

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный. Ч. 1. – 171 с. (гл. 1.6).

4. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст: электронный (гл. 4, 11, 20).

Контрольные вопросы

1. Как поведенческий анализ позволяет выявлять неизвестные атаки, и какие факторы влияют на точность создания базового профиля нормального поведения?
2. Какие типы алгоритмов машинного обучения наиболее эффективны для обнаружения атак, и каковы их преимущества и ограничения?
3. Как методы вычислительного интеллекта, такие как генетические алгоритмы или нечёткая логика, применяются для оптимизации систем обнаружения атак?
4. Какие критерии следует использовать при сравнении эффективности методов поведенческого анализа, машинного обучения и вычислительного интеллекта?
5. Как можно минимизировать ложные срабатывания в системах поведенческого анализа, и какие инструменты наиболее подходят для этой задачи?
6. Какие этапы подготовки данных и обучения модели критически важны для успешного применения машинного обучения в обнаружении атак?
7. В каких сценариях методы вычислительного интеллекта предпочтительнее традиционных алгоритмов машинного обучения для обнаружения киберугроз?
8. Как выбор метода обнаружения атак зависит от характеристик защищаемой системы, и какие практические шаги можно предпринять для проведения сравнительного анализа?

Тема 1.3 Специфика анализа атак как процессов реализации угроз
Перечень изучаемых вопросов

1. Жизненный цикл атаки.
2. Моделирование атак.
3. Контекст угроз.
4. Анализ многоэтапных атак.

Методические указания к изучению

1. Жизненный цикл атаки

Анализ атак как процессов реализации угроз начинается с изучения их жизненного цикла, который представляет собой последовательность этапов, через которые проходит атака от подготовки до завершения. Этот процесс обычно включает разведку, проникновение, закрепление, выполнение вредоносных действий и, в некоторых случаях, сокрытие следов. На этапе разведки злоумышленники собирают информацию о цели, используя такие методы, как сканирование портов, социальная инженерия или анализ открытых источников (OSINT). Проникновение предполагает эксплуатацию уязвимостей, например, через фишинг или внедрение вредоносного кода. Закрепление включает установку устойчивого доступа, такого как создание бэкдоров или внедрение в системные процессы. Выполнение вредоносных действий может варьироваться от кражи данных до шифрования файлов в атаках-вымогателях. Сокрытие следов, например, удаление логов или использование прокси, направлено на затруднение обнаружения.

Понимание жизненного цикла атаки позволяет специалистам по безопасности предугадывать действия злоумышленников и разрабатывать меры защиты на каждом этапе. Например, усиление аутентификации может затруднить проникновение, а мониторинг системных процессов — выявить закрепление. Однако сложность анализа заключается в вариативности атак: разные угрозы могут включать дополнительные этапы или пропускать некоторые из них, что требует гибкого подхода к их изучению.

Методические рекомендации. Для освоения концепции жизненного цикла атаки студентам следует начать с изучения стандартных моделей, таких как Cyber Kill Chain от Lockheed Martin или MITRE ATT&CK. Теоретические занятия должны включать разбор каждого этапа с примерами реальных атак, таких как атака WannaCry, чтобы показать, как этапы реализуются на практике. Практические занятия рекомендуется проводить в лабораторной среде, используя инструменты, такие как Metasploit, для моделирования этапов атаки, например, разведки и проникновения. Студентам полезно настроить систему мониторинга, например, с помощью Zeek, чтобы отслеживать действия «злоумышленника» и анализировать их на каждом этапе. Самостоятельная работа должна включать изучение отчетов об инцидентах, таких как публикации FireEye или CrowdStrike, чтобы понять, как жизненный цикл атаки проявляется в реальных сценариях. Для углубленного изучения можно рассмотреть адаптацию моделей жизненного цикла к специфическим типам атак, таким как атаки на IoT-устройства.

2. Моделирование атак

Моделирование атак представляет собой процесс создания формализованных описаний или симуляций киберугроз для анализа их поведения, последствий и методов противодействия. Этот подход позволяет предсказывать действия злоумышленников, тестировать защитные механизмы и разрабатывать стратегии реагирования. Моделирование может быть выполнено на разных уровнях: от теоретических моделей, таких как деревья атак или графы угроз, до практических симуляций в контролируемой среде. Теоретические модели, например, деревья атак, представляют возможные пути реализации угрозы, начиная с исходной точки (например, уязвимости) и заканчивая достижением цели (например, компрометацией данных). Графы угроз учитывают взаимосвязи между компонентами системы, позволяя оценить вероятность и последствия атаки.

Практическое моделирование часто проводится в виртуальных средах, таких как киберполигоны, где имитируются реальные атаки, включая фишинг, эксплуатацию уязвимостей или DDoS. Инструменты, такие как CALDERA или Red Team Automation, позволяют автоматизировать моделирование сложных сценариев. Основное преимущество моделирования заключается в возможности тестировать защитные системы без риска для реальной инфраструктуры. Однако создание точных моделей требует глубокого понимания системы, а также актуальных данных об уязвимостях и тактиках злоумышленников.

Методические рекомендации. Изучение моделирования атак следует начинать с анализа теоретических подходов, таких как построение деревьев атак и графов угроз. Теоретические занятия должны включать разбор методологий, таких как STRIDE или DREAD, для оценки угроз. Практические занятия рекомендуется проводить в виртуальной среде, используя инструменты, такие как Metasploit или CALDERA, для моделирования атак, например, эксплуатации уязвимости в веб-приложении. Студентам полезно разработать модель атаки для конкретной системы, например, корпоративной сети, и протестировать её в симуляции. Для углубленного изучения можно рассмотреть автоматизированные платформы, такие как MITRE ATT&CK Navigator, для создания сценариев атак. Самостоятельная работа должна включать анализ кейсов, где моделирование помогло предотвратить инциденты, а также изучение стандартов, таких как NIST SP 800-53, для интеграции моделирования в процессы управления рисками.

3. Контекст угроз

Контекст угроз представляет собой совокупность факторов, которые определяют вероятность, характер и последствия атаки. Эти факторы включают тип защищаемой системы, её критические активы, профиль злоумышленников, их мотивацию, доступные ресурсы и внешние условия, такие как геополитическая обстановка. Например, атака на банковскую систему может быть мотивирована финансовой выгодой и использовать сложные методы, такие как APT, тогда как атака на образовательное учреждение может быть результатом хактивизма и ограничиться DDoS. Понимание контекста позволяет приоритизировать защитные меры и адаптировать их к конкретным угрозам.

Анализ контекста угроз включает сбор данных из различных источников, таких как отчеты об угрозах (Threat Intelligence), анализ уязвимостей и мониторинг активности в даркнете. Инструменты, такие как MISP или ThreatConnect, помогают собирать и анализировать данные, чтобы создать профиль угрозы. Однако сложность анализа заключается в динамичности контекста: новые уязвимости, изменение мотивации злоумышленников или появление новых технологий могут резко изменить ландшафт угроз.

Методические рекомендации. Для освоения анализа контекста угроз студентам следует начать с изучения концепции Threat Intelligence и её источников, таких как открытые платформы (OTX) или коммерческие сервисы (Recorded Future). Теоретические занятия должны включать разбор структуры отчетов об угрозах и методов их интерпретации. Практические занятия рекомендуется проводить с использованием MISP для интеграции данных об угрозах и построения профиля для гипотетической системы, например, веб-приложения. Студентам полезно проанализировать реальный отчет об угрозах, например, от Verizon DBIR, и определить, как контекст влияет на выбор защитных мер. Для углубленного изучения можно рассмотреть влияние геополитических факторов на киберугрозы, используя кейсы, такие как атаки на критическую инфраструктуру. Самостоятельная работа должна включать мониторинг актуальных угроз через открытые источники и разработку рекомендаций по защите для конкретного сценария.

4. Анализ многоэтапных атак

Многоэтапные атаки, такие как целевые атаки (APT), представляют собой сложные процессы, включающие последовательное выполнение нескольких действий для достижения конечной цели. Эти атаки характеризуются длительным жизненным циклом, скрытностью и высокой степенью координации. Например, APT может начинаться с фишингового письма, затем включать эксплуатацию уязвимости, установку бэкдора, горизонтальное перемещение по сети и, наконец, эксфильтрацию данных. Анализ таких атак требует понимания их структуры, а также способности коррелировать события на разных этапах.

Основным инструментом анализа многоэтапных атак является корреляция логов и событий, собранных с помощью систем SIEM, таких как Splunk или ELK Stack. Эти системы позволяют выявить связи между, казалось бы, несвязанными инцидентами, например, между подозрительным входом в систему и необычным сетевым трафиком. Кроме того, анализ многоэтапных атак опирается на фреймворки, такие как MITRE ATT&CK, которые классифицируют тактики и техники, используемые злоумышленниками. Сложность анализа заключается в необходимости обработки больших объемов данных и выявления слабых сигналов, которые могут быть замаскированы под легитимную активность.

Методические рекомендации. Изучение анализа многоэтапных атак следует начинать с изучения фреймворков, таких как MITRE ATT&CK, чтобы понять тактики и техники, используемые в APT. Теоретические занятия должны включать разбор реальных кейсов, таких как атака SolarWinds, чтобы показать, как этапы атаки связаны между собой. Практические занятия рекомендуется проводить с использованием SIEM-систем, таких как Splunk, для анализа логов,

содержащих следы многоэтапной атаки. Студентам полезно создать сценарий атаки в лабораторной среде, используя инструменты, такие как Cobalt Strike, и попытаться выявить его с помощью корреляции событий. Для углубленного изучения можно рассмотреть методы attribution, направленные на определение источника атаки. Самостоятельная работа должна включать анализ отчетов об APT, таких как публикации Mandiant, и разработку плана реагирования на подобную атаку.

Для эффективного изучения темы важно сочетать теоретические лекции, практические занятия и самостоятельную работу. Лекции должны быть структурированы так, чтобы сначала давать обзор концепций, таких как жизненный цикл атаки, а затем углубляться в их технические детали, включая примеры инструментов и кейсов. Практические занятия следует проводить в виртуальной среде, такой как VMware или киберполигон, где студенты могут безопасно моделировать атаки и анализировать их следы. Самостоятельная работа должна включать изучение документации фреймворков, таких как MITRE ATT&CK, и анализ отчетов об инцидентах из открытых источников, таких как Krebs on Security или ThreatPost.

Для развития критического мышления студентам следует задавать вопросы, требующие анализа, например, как контекст угроз влияет на выбор защитных мер или как корреляция событий помогает выявить APT. Междисциплинарный подход, включающий основы сетевых технологий, анализа данных и психологии (для социальной инженерии), способствует более глубокому пониманию материала. Преподавателям рекомендуется использовать интерактивные методы, такие как разбор кейсов в группах или симуляции атак, чтобы повысить вовлечённость студентов и развить их практические навыки.

Тема «Специфика анализа атак как процессов реализации угроз» предоставляет фундамент для понимания киберугроз как сложных, многоэтапных процессов, требующих системного подхода к их анализу. Жизненный цикл атаки раскрывает этапы реализации угроз, моделирование атак позволяет тестировать защитные механизмы, контекст угроз обеспечивает приоритизацию мер, а анализ многоэтапных атак помогает выявлять скрытые угрозы, такие как APT. Методические рекомендации, предложенные в статье, направлены на обеспечение глубокого освоения материала через сочетание теории, практики и самостоятельной работы. Такой подход формирует у студентов навыки, необходимые для эффективного анализа компьютерных атак и разработки устойчивых систем защиты, способных противостоять сложным и динамичным киберугрозам.

Литература

1. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с. — Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/385979 (дата обращения: 08.10. 2024). – ISBN 978-5-507- 48601-4. – Текст : электронный (гл. 1, параграф 1.3).

2. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный (гл. 2, 10, 15).

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный. Ч. 1. – 171 с. (гл. 1, параграф 1.1).

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=70 0833 (дата обращения: 08.10.2024). – ISBN 978- 5-8149-3250-1. – Текст : электронный (л.р. 1, 2).

5. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст : электронный (гл. 20).

Контрольные вопросы

1. Как структура жизненного цикла атаки помогает специалистам по безопасности разрабатывать меры противодействия на каждом этапе?
2. Какие методы и инструменты наиболее эффективны для моделирования атак, и как они способствуют тестированию защитных систем?
3. Как анализ контекста угроз влияет на приоритизацию защитных мер, и какие источники данных наиболее ценны для этого процесса?
4. Какие особенности многоэтапных атак затрудняют их обнаружение, и как корреляция событий помогает преодолеть эти сложности?
5. Как фреймворки, такие как MITRE ATT&CK, используются для анализа жизненного цикла и тактик многоэтапных атак?
6. Какие шаги необходимо предпринять для создания точной модели атаки, и каковы ограничения теоретических и практических подходов к моделированию?
7. Как геополитические и организационные факторы формируют контекст угроз, и как это учитывается при разработке защитных стратегий?
8. Какие практические инструменты и методы анализа логов наиболее эффективны для выявления следов многоэтапных атак в корпоративной сети?

Тема 1.4 Аналитическое моделирование процессов реализации угроз
Перечень изучаемых вопросов

1. Детерминированные модели.
2. Стохастические модели.
3. Агент-ориентированное моделирование.
4. Верификация моделей.

Методические указания к изучению

Аналитическое моделирование процессов реализации угроз является ключевым инструментом в современной кибербезопасности, позволяющим не только прогнозировать сценарии атак, но и разрабатывать стратегии их нейтрализации. Эта дисциплина объединяет математические методы, компьютерные симуляции и эмпирический анализ, чтобы создать целостное представление о динамике угроз. В рамках изучения данной темы рассматриваются четыре фундаментальных направления, каждое из которых требует детального погружения в теоретические основы и практические аспекты применения моделей.

1. Детерминированные модели

Детерминированные модели основаны на строгих математических зависимостях, где каждое действие злоумышленника или реакция системы описывается однозначными уравнениями. Например, деревья атак (attack trees) структурируют возможные пути достижения цели атаки, разбивая их на иерархию подцелей и методов. Каждый узел дерева представляет этап атаки, а ветви — альтернативные сценарии. Такой подход эффективен для анализа сложных многошаговых атак, таких как проникновение в корпоративную сеть через цепочку уязвимостей. Однако детерминированные модели имеют ограничения: они не учитывают вероятностные факторы (например, случайные ошибки злоумышленника) и динамику изменения среды. Для преодоления этих недостатков их часто комбинируют с другими методами.

Методические рекомендации. Студентам рекомендуется начать с изучения базовых работ Брюса Шнайера, а затем перейти к анализу реальных инцидентов, таких как атака на Colonial Pipeline (2021). Практические задания должны включать построение деревьев атак для конкретных сценариев (например, фишинговой кампании) с использованием инструментов вроде SecurITree. Важно обсуждать, как изменения в топологии сети или обновления ПО влияют на структуру модели.

2. Стохастические модели

Стохастические модели опираются на теорию вероятностей, что позволяет учитывать случайные события и неопределенности. Например, цепи Маркова моделируют переходы между состояниями системы (например, «нормальная работа», «обнаружена уязвимость», «произошла утечка данных»), где каждое изменение состояния имеет определенную вероятность. Эти модели особенно полезны для оценки долгосрочных рисков, таких как APT-атаки, где злоумышленники действуют скрытно и адаптивно. Математически цепь Маркова может быть представлена матрицей переходных вероятностей $P=[p_{ij}]$, где p_{ij} – вероятность перехода из состояния i в состояние

j. Анализ таких моделей позволяет прогнозировать, например, вероятность успешного внедрения вредоносного ПО в систему с учетом частоты обновлений антивируса.

Методические рекомендации. Для освоения стохастических моделей необходимо углубиться в основы теории вероятностей и статистики. Практические задания могут включать расчеты в MATLAB или Python с использованием библиотек NumPy и Pandas. Пример: моделирование атаки на банковскую систему с учетом вероятности обнаружения аномалий SIEM-системой. Студентам стоит изучить отчеты ENISA о трендах киберугроз для корректного задания вероятностных параметров.

3. Агент-ориентированное моделирование

Агент-ориентированное моделирование (АОМ) фокусируется на автономных агентах (злоумышленниках, администраторах, пользователях), которые взаимодействуют в виртуальной среде по заданным правилам. Например, можно смоделировать распространение червя в IoT-сети, где каждый устройство-агент имеет параметры уязвимости и скорость передачи данных. АОМ выявляет эмерджентные свойства системы, которые невозможно предсказать аналитически, такие как внезапные каскадные сбои.

Методические рекомендации. Рекомендуется использовать платформы NetLogo или GAMA для создания симуляций. Студенты должны разрабатывать сценарии, учитывающие стратегии агентов: например, злоумышленник, меняющий тактику при обнаружении. Для углубления понимания можно сравнить результаты моделирования с реальными кейсами, такими как атака Mirai на DNS-провайдер Dyn (2016), и обсудить, почему модель могла не учесть человеческий фактор.

4. Верификация моделей: от теории к практике

Верификация моделей – критический этап, обеспечивающий их соответствие реальным процессам. Это включает в себя:

1. **Валидацию на исторических данных** – сравнение прогнозов модели с известными инцидентами (например, тактиками APT-группы Lazarus).

2. **Эксперименты в контролируемой среде** – тестирование моделей в лабораторных условиях, имитирующих реальную инфраструктуру. Например, модель, предсказывающая скорость распространения ransomware, должна быть проверена на данных о WannaCry или NotPetya.

3. *Методические рекомендации.* Студентам следует освоить методы кросс-валидации и A/B-тестирования. Практикум может включать работу с базами данных MITRE ATT&CK и CVE. Важно анализировать случаи, когда модель дала ложный прогноз: например, не учла социальную инженерию в сценарии атаки.

Литература

1. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с. — Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная

система. – URL: https://e.lanbook.com/book/385979 (дата обращения: 08.10. 2024). – ISBN 978-5-507- 48601-4. – Текст : электронный (гл. 2, параграф 2.2).

2. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный (гл. 13).

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный. Ч. 1. – 171 с. (параграф 1.7).

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=70 0833 (дата обращения: 08.10.2024). – ISBN 978- 5-8149-3250-1. – Текст : электронный (гл. 3).

5. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст : электронный (гл. 10, 11, 20).

Контрольные вопросы

1. Какие математические методы лежат в основе построения деревьев атак, и как они учитывают альтернативные сценарии реализации угроз?
2. Как определить матрицу переходных вероятностей в цепи Маркова для моделирования атаки на облачную инфраструктуру, и какие факторы могут повлиять на её элементы?
3. Какие преимущества агент-ориентированного моделирования перед детерминированным подходом проявляются при анализе целевых атак на промышленные системы?
4. Как исторические данные об эксплуатации уязвимости Log4j могут быть использованы для верификации модели распространения эксплойтов в корпоративной сети?
5. Почему детерминированные модели неэффективны для прогнозирования атак, основанных на социальной инженерии, и какие методы могли бы дополнить анализ?
6. Какие этические дилеммы возникают при использовании агент-ориентированных моделей, имитирующих поведение хакерских группировок?
7. Как оценить точность стохастической модели, предсказывающей вероятность успеха фишинговой кампании, и какие метрики для этого необходимы?

8. Какие ограничения исторических данных из MITRE ATT&CK могут снизить качество верификации модели, и как их можно компенсировать?

Раздел 2. Методы моделирования компьютерных атак

Тема 2.1 Методика анализа и регулирования рисков при реализации нескольких угроз удаленного доступа к элементам ИТКС.

Перечень изучаемых вопросов

1. Идентификация угроз удаленного доступа.
2. Оценка рисков.
3. Регулирование рисков.
4. Управление инцидентами.

Методические указания к изучению

Современные информационно-телекоммуникационные системы (ИТКС) сталкиваются с растущим числом угроз удаленного доступа, требующих системного подхода к анализу и управлению рисками. Тема 2.1 фокусируется на комплексной методике, объединяющей идентификацию угроз, оценку рисков, их регулирование и управление инцидентами. Эти элементы формируют цикл безопасности, обеспечивающий устойчивость ИТКС к атакам. Методические рекомендации включают сочетание теоретических знаний с практическими кейсами, моделированием и критическим анализом.

1. Идентификация угроз удаленного доступа

Идентификация угроз является первым этапом построения системы защиты. Она предполагает систематический поиск и классификацию потенциальных уязвимостей, эксплуатируемых через удаленный доступ. К числу распространенных угроз относятся: эксплуатация слабых мест в сетевых протоколах, атаки на аутентификационные механизмы (например, брутфорс), фишинг, внедрение вредоносного ПО через удаленные подключения. Для идентификации применяются методы анализа сетевого трафика, аудита конфигураций, pentesting и моделирования атак (Red Teaming).

Методические рекомендации:

a. Рекомендуется изучать реальные инциденты (например, утечки данных через VPN) для понимания тактик злоумышленников.

b. Использовать инструменты сканирования уязвимостей (Nessus, OpenVAS) в лабораторных работах.

c. Анализировать отчеты CERT и базы данных уязвимостей (CVE) для актуализации знаний.

2. Оценка рисков

Оценка рисков направлена на определение критичности угроз и их потенциального воздействия на ИТКС. Качественные методы (например, матрицы рисков) позволяют ранжировать угрозы по уровню опасности, а количественные (FAIR-модель) – рассчитывать финансовые потери. Важно учитывать контекст системы: критичность данных, доступность ресурсов, нормативные тре-

бования. Например, риск утечки конфиденциальной информации через незащищенный RDP-порт будет иметь высокий приоритет в банковской сфере.

Методические рекомендации:

a. Проводить workshops по составлению матриц рисков для конкретных сценариев (например, облачная инфраструктура).

b. Использовать симуляторы рисков (Cybersecurity Risk Assessment Tool) для визуализации последствий.

c. Изучать стандарты ISO 27005 и NIST SP 800-30 как основу для методологии.

3. Регулирование рисков

Регулирование предполагает выбор стратегий минимизации рисков: снижение (внедрение MFA, сегментация сети), передача (страхование киберрисков), принятие (для низкоприоритетных угроз) или избегание (отказ от рискованных технологий). Ключевой аспект – баланс между затратами и эффективностью мер. Например, внедрение SIEM-системы снижает риск несвоевременного обнаружения атак, но требует значительных ресурсов.

Методические рекомендации:

a. Анализировать кейсы успешного внедрения мер (например, переход на Zero Trust Architecture).

b. Проводить сравнительный анализ инструментов (Firewall vs. IDS) для выбора оптимальных решений.

c. Моделировать сценарии, где регулирование приводит к непредвиденным последствиям (например, избыточная сегментация сети).

4. Управление инцидентами

Управление инцидентами охватывает процессы обнаружения, реагирования, восстановления и пост-анализа. Эффективный план реагирования включает создание CSIRT-команд, использование playbook для типовых атак (DDoS, ransomware) и регулярные учения. Пост-анализ (Lessons Learned) помогает выявить слабые места в защите и скорректировать стратегии. Например, расследование инцидента с утечкой данных может выявить необходимость усиления мониторинга API.

Методические рекомендации:

a. Организовывать ролевые игры (CTF-соревнования) для отработки навыков реагирования.

b. Изучать фреймворки (NIST SP 800-61) для структурирования процессов.

c. Разрабатывать чек-листы для аудита планов восстановления.

Изучение темы требует междисциплинарного подхода, объединяющего технические знания, аналитическое мышление и понимание бизнес-контекста. Важно подчеркивать взаимосвязь этапов: идентификация угроз влияет на оценку рисков, а управление инцидентами завершает цикл, обеспечивая обратную связь для системы защиты. Практические задания должны имитировать реальные условия, формируя навыки быстрого принятия решений в условиях неопределенности.

Литература

1. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/385979 (дата обращения: 08.10. 2024). – ISBN 978-5-507- 48601-4. – Текст : электронный.

2. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный.

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный. Ч. 1. – 171 с.

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=70 0833 (дата обращения: 08.10.2024). – ISBN 978- 5-8149-3250-1. – Текст : электронный (л.р. 10).

5. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст : электронный.

Контрольные вопросы

Какие критерии следует учитывать при классификации угроз удаленного доступа в контексте критичности элементов ИТКС?

1. Объясните, как количественные методы оценки рисков (например, FAIR) позволяют прогнозировать финансовые последствия кибератак.
2. Почему передача рисков через страхование не может полностью заменить технические меры защиты? Приведите пример.
3. Опишите сценарий, в котором принятие риска становится оптимальной стратегией для организации.
4. Какие этапы управления инцидентами наиболее критичны для минимизации downtime системы? Аргументируйте.
5. Как пост-анализ инцидента способствует улучшению процессов идентификации угроз?
6. Сравните эффективность сегментации сети и многофакторной аутентификации как методов регулирования рисков удаленного доступа.

7. Какие этические аспекты необходимо учитывать при моделировании атак (Red Teaming) в учебных целях?

Тема 2.2 Метод натурного и имитационного моделирования процессов противодействия компьютерным атакам

Перечень изучаемых вопросов

1. Натурное моделирование.
2. Имитационное моделирование.
3. Сравнение подходов.
4. Оптимизация защиты.

Методические указания к изучению

В условиях динамично развивающегося ландшафта киберугроз моделирование процессов противодействия атакам становится ключевым инструментом для подготовки специалистов в области кибербезопасности. Натурное и имитационное моделирование позволяют не только выявлять уязвимости, но и формировать стратегии адаптивной защиты. Методология тестирования на реальных системах и симуляции атак в контролируемых средах дополняют друг друга, обеспечивая баланс между реализмом и безопасностью. Изучение этих подходов требует интеграции технических навыков, понимания этико-правовых норм и умения интерпретировать данные для оптимизации защиты.

1. Натурное моделирование

Натурное моделирование предполагает проведение атак на реальные инфраструктуры с целью оценки их устойчивости. Ключевые методы включают пентесты (тестирование на проникновение) и деятельность «красных команд» – групп этичных хакеров, имитирующих действия злоумышленников. Например, пентестинг веб-приложения может выявить уязвимости SQLi или XSS, а «красные команды» способны смоделировать многоэтапную атаку, включающую социальную инженерию. Преимущество натурного подхода – высокая точность результатов, так как тестирование отражает реальное поведение системы под нагрузкой. Однако такие методы требуют строгого соблюдения юридических рамок (например, согласования с владельцем инфраструктуры) и могут привести к непреднамеренному downtime.

Методические указания:

a. Организовывать лабораторные работы с использованием платформ вроде Hack The Box или TryHackMe для безопасного проведения пентестов.

b. Разбирать кейсы из отчетов Bug Bounty (например, HackerOne) для понимания типовых уязвимостей.

c. Моделировать сценарии, где студенты получают роль «красной команды» и защитников («синей команды»), чтобы отработать взаимодействие.

2. Имитационное моделирование: использование специализированных сред

Имитационное моделирование проводится в изолированных средах, таких как CyberRange, или с помощью инструментов эмуляции сетей (GNS3, CORE). Эти платформы позволяют создавать виртуальные копии корпоративных сетей,

IoT-устройств или промышленных систем, где можно безопасно воспроизводить сложные атаки, включая APT (Advanced Persistent Threats). Например, в CyberRange можно смоделировать атаку на энергосистему, оценив последствия и скорость реакции SOC (Security Operations Center). Преимущество имитации – масштабируемость и отсутствие риска для реальных активов. Однако точность результатов может снижаться из-за упрощения моделируемых процессов.

Методические указания:

a. Использовать GNS3 для построения виртуальных сетей с маршрутизаторами и межсетевыми экранами, изучая атаки типа MITM (Man-in-the-Middle).

b. Внедрять сценарии на базе MITRE ATT&CK Framework для обучения тактикам противодействия.

c. Анализировать ограничения имитационных моделей (например, невозможность учесть человеческий фактор).

3. Сравнение подходов: точность vs стоимость, этические и юридические аспекты

Натурное моделирование обеспечивает высокую достоверность, но связано с существенными затратами на подготовку и рисками для инфраструктуры. Имитационное моделирование экономичнее и безопаснее, но может упускать нюансы, связанные с аппаратными ограничениями или поведением пользователей. Этические дилеммы возникают в обоих случаях: пентесты требуют четких соглашений NDA (Non-Disclosure Agreement), а симуляции – защиты данных, используемых в виртуальных средах. Юридические аспекты включают соответствие стандартам GDPR, HIPAA или PCI DSS при работе с конфиденциальной информацией.

Методические указания:

a. Проводить дебаты на тему «Этика хакинга: где границы допустимого?» с анализом реальных инцидентов (например, утечка данных при пентесте).

b. Изучать законодательные акты страны, регулирующие кибербезопасность, для формирования правовой грамотности.

c. Сравнивать бюджет типового проекта натурного и имитационного тестирования на примере малого предприятия.

4. Оптимизация защиты

Данные, полученные в ходе моделирования, служат основой для корректировки политик безопасности. Например, выявление частых атак на RDP-порты может привести к внедрению сегментации сети или MFA (многофакторной аутентификации). Анализ логов из CyberRange помогает оптимизировать правила SIEM-систем (Security Information and Event Management), сокращая число ложных срабатываний. Важно не только фиксировать уязвимости, но и оценивать эффективность примененных контрмер.

Методические указания:

a. Разрабатывать циклы PDCA (Plan-Do-Check-Act) на основе результатов тестов.

b. Использовать метрики вроде MTTD (Mean Time to Detect) и MTTR (Mean Time to Respond) для количественной оценки улучшений.

с. Изучать кейсы компаний, которые смогли снизить число инцидентов после редизайна архитектуры.

Синтез натурного и имитационного моделирования формирует у студентов комплексное понимание процессов киберзащиты. Практические навыки работы с инструментами дополняются критическим мышлением, необходимым для принятия решений в условиях ограниченных ресурсов и юридических барьеров. Акцент должен делаться на итеративность: моделирование – анализ – оптимизация — повторное тестирование. Это позволяет создать адаптивную систему безопасности, способную противостоять эволюционирующим угрозам.

Литература

1. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/385979 (дата обращения: 08.10. 2024). – ISBN 978-5-507- 48601-4. – Текст : электронный (гл. 2).

2. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный (гл. 3, параграф 3.3).

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный. Ч. 1. – 171 с. (гл. 1, параграф 1.3).

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=70 0833 (дата обращения: 08.10.2024). – ISBN 978- 5-8149-3250-1. – Текст : электронный.

5. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст : электронный (гл. 4, 27).

Контрольные вопросы

1. Какие этические принципы должны соблюдаться при проведении пентестов на реальной инфраструктуре заказчика?

2. Объясните, почему имитационное моделирование не может полностью заменить тестирование на реальных системах. Приведите пример ограничения.

3. Как использование MITRE ATT&CK Framework повышает эффективность тренировок в CyberRange?

4. Опишите сценарий, в котором результаты натурного моделирования привели к изменению корпоративных политик безопасности.

5. Какие метрики следует использовать для оценки успешности оптимизации защиты после серии имитационных тестов?

6. Сравните затраты на развертывание CyberRange и организацию деятельности «красной команды» для средней компании.

7. Почему при имитации атак на IoT-устройства важно учитывать специфику их аппаратного обеспечения?

8. Как законодательные требования (например, GDPR) влияют на выбор между натурным и имитационным моделированием?

Тема 2.3 Метод экспериментальной оценки эффективности компьютерных атак

Перечень изучаемых вопросов

1. Планирование экспериментов.
2. Инструменты для оценки.
3. Анализ результатов.
4. Этические ограничения.

Методические указания к изучению

Экспериментальная оценка эффективности компьютерных атак – это систематический подход к изучению уязвимостей информационных систем через контролируемое моделирование атакующих сценариев. Такой метод позволяет не только выявлять слабые места в защите, но и измерять эффективность контрмер, что критически важно для формирования адаптивных стратегий кибербезопасности. Изучение данной темы требует понимания принципов планирования экспериментов, владения специализированными инструментами, навыков анализа данных и строгого соблюдения этико-правовых норм. Интеграция теории и практики обеспечивает подготовку специалистов, способных прогнозировать и нейтрализовать угрозы в реальном времени.

1. Планирование экспериментов

Планирование эксперимента начинается с четкого формулирования целей. Например, оценка устойчивости веб-приложения к SQL-инъекциям или проверка способности SOC (Security Operations Center) обнаруживать многоэтапные атаки. Ключевым этапом является выбор метрик, которые количественно отражают результаты тестирования. Метрики включают время до обнаружения атаки (MTTD — Mean Time to Detect), процент успешных проникновений, количество ложных срабатываний системы защиты и скорость восстановления (MTTR – Mean Time to Respond).

Важно учитывать контекст системы: для финансовых учреждений критична метрика предотвращения утечек данных, а для промышленных систем — устойчивость к атакам на доступность (DDoS). Эксперимент должен быть вос-

производимым, чтобы результаты можно было верифицировать и использовать для сравнения разных сценариев защиты.

Методические указания:

a. Рекомендуется разрабатывать чек-листы для постановки целей эксперимента, учитывающие специфику отрасли (например, здравоохранение vs IoT).

b. Проводить мастер-классы по выбору метрик на основе анализа реальных инцидентов, таких как атака на Colonial Pipeline.

c. Использовать шаблоны документов (например, TTPs – Tactics, Techniques, Procedures) для структурирования планов тестирования.

2. Инструменты для оценки

Экспериментальная оценка эффективности атак невозможна без специализированных инструментов. Фреймворки вроде Metasploit предоставляют готовые эксплойты для тестирования уязвимостей, а платформы типа Cobalt Strike позволяют моделировать сложные атаки, включая фишинг и lateral movement. Инструменты автоматизации, такие как AutoSploit, ускоряют процесс сканирования и эксплуатации слабых мест.

Особое внимание стоит уделять эмуляции Tactics, Techniques and Procedures (TTPs) злоумышленников. Например, с помощью MITRE Caldera можно воспроизводить сценарии APT-групп, имитируя их методы работы. Для оценки защиты облачных сред применяются инструменты вроде Pacu, ориентированные на AWS.

Методические указания

a. Организовывать лабораторные работы с пошаговым развертыванием Metasploit для эксплуатации уязвимостей в виртуальных машинах (например, Metasploitable).

b. Анализировать отчеты об атаках Advanced Persistent Threats (APT) для настройки реалистичных сценариев в Cobalt Strike.

c. Изучать документацию инструментов (например, BloodHound для анализа Active Directory) для углубления технических навыков.

3. Анализ результатов.

Полученные данные требуют тщательной обработки. Статистические методы, такие как корреляционный анализ, помогают выявить взаимосвязь между конфигурацией системы и успешностью атак. Визуализация данных через инструменты вроде Kibana или Grafana упрощает интерпретацию метрик. Например, heatmap-анализ может показать, какие узлы сети наиболее часто подвергаются атакам.

Ключевой задачей является идентификация узких мест в защите. Если эксперимент выявил, что 80 % успешных проникновений происходят через устаревшее ПО, это указывает на необходимость срочного обновления систем. Анализ логов SIEM-систем позволяет оценить эффективность правил обнаружения и минимизировать задержки реагирования.

Методические указания

a. Использовать Python-библиотеки (Pandas, Matplotlib) для обработки и визуализации данных экспериментов.

b. Проводить воркшопы по составлению отчетов, включающих рекомендации по устранению уязвимостей.

c. Моделировать ситуации, где статистические аномалии (например, резкий рост ложных срабатываний) требуют пересмотра политик мониторинга.

4. Этические ограничения: баланс между исследованиями и законностью Эксперименты с компьютерными атаками должны строго соответствовать правовым нормам. Тестирование без письменного согласия владельца системы является киберпреступлением, даже если проводится в исследовательских целях. Соглашения NDA (Non-Disclosure Agreement) и Rules of Engagement (RoE) обязательны для формализации границ экспериментов. Например, пентестеры обязаны немедленно прекратить атаку при обнаружении критической уязвимости, способной вызвать коллапс системы.

Этические дилеммы возникают при работе с публичными системами. Так, сканирование портов государственного учреждения без разрешения может привести к юридическим последствиям, даже если цель – академическое исследование.

Методические указания

a. Разбирать кейсы судебных разбирательств (например, дело США против Романа Селезнева) для понимания правовых рисков.

b. Включать в учебный процесс ролевые игры, где студенты готовят RoE и получают «разрешение» от условного заказчика.

c. Изучать международные стандарты, такие как PCI DSS и ISO 27001, для формирования культуры compliance.

Метод экспериментальной оценки эффективности атак формирует у студентов навыки, необходимые для борьбы с современными киберугрозами. Важно подчеркивать цикличность процесса: планирование — проведение — анализ — корректировка защиты. Практические задания должны имитировать работу SOC, red и blue teams, развивая способность действовать в условиях неопределенности. Особое внимание уделяется этической ответственности: даже самая совершенная техническая подготовка теряет ценность без соблюдения законов и профессиональной этики.

Литература

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный (гл. 2).

2. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст : электронный (л. 16, 18).

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный. Ч. 1. – 171 с. (гл. 2).

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=70 0833 (дата обращения: 08.10.2024). – ISBN 978- 5-8149-3250-1. – Текст : электронный (гл. 5).

5. 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: 05.10.2024). – ISBN 978-5-238-03639-7. – Текст : электронный.

6. Программно-аппаратные средства обеспечения информационной безопасности: лаб. практикум для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» / Федер. агентство по рыболовству, Калининингр. гос. техн. ун-т, Балт. гос. акад. рыбопромыслового флота; сост.: А. Г. Жестовский, В. В. Подтопельный. – 2-е изд., перераб. и доп. – Калининград: БГАРФ, 2019. – Режим доступа: для авториз. пользователей. – URL: https://lib.klgtu.ru/web/index.php (дата обращения: 05.11.2024). – ISBN 978-5-238-03639-7. – Текст : электронный. – 2019. – Текст : непосредственный. Ч. 1.: Защита компьютерной информации и компьютерных систем от вредоносных программ (гл. 1).

Контрольные вопросы

1. Какие метрики следует выбрать для оценки устойчивости банковской системы к атакам на конфиденциальность данных? Обоснуйте выбор.
2. Объясните, как использование MITRE ATT&CK Framework повышает реалистичность экспериментов с Cobalt Strike.
3. Почему корреляционный анализ данных эффективен для выявления скрытых зависимостей между уязвимостями и успешностью атак?
4. Опишите сценарий, при котором несогласованное тестирование на реальной системе может привести к уголовной ответственности.
5. Какие инструменты визуализации данных наиболее эффективны для интерпретации результатов пентеста? Приведите примеры.
6. Сравните возможности Metasploit и Cobalt Strike в контексте моделирования фишинговых атак.
7. Как стандарт PCI DSS влияет на планирование экспериментов для e-commerce платформ?

8. Почему анализ ложных срабатываний SIEM-системы важен для оптимизации правил обнаружения атак?

Тема 2.4 Метод оценки эффективности активного противодействия компьютерным атакам

Перечень изучаемых вопросов

1. Критерии эффективности.
2. Технологии активного противодействия.
3. Оценка в условиях реального времени.
4. Устойчивость к адаптивным атакам.

Методические указания к изучению

Активное противодействие компьютерным атакам требует не только внедрения защитных технологий, но и постоянной оценки их эффективности в динамично меняющихся условиях. Современные киберугрозы, такие как APT (Advanced Persistent Threats) или атаки с использованием искусственного интеллекта, вынуждают специалистов разрабатывать адаптивные методы защиты, способные нейтрализовать угрозы в реальном времени. В рамках данной темы рассматриваются критерии эффективности, технологии активного противодействия, методы оценки в режиме реального времени и устойчивость к эволюционирующим атакам. Изучение этих аспектов формирует у студентов навыки проектирования и оптимизации систем кибербезопасности, основанные на анализе данных и понимании тактик противника.

1. Критерии эффективности: скорость нейтрализации угрозы и минимизация ложных срабатываний

Эффективность активного противодействия измеряется способностью системы быстро обнаруживать и блокировать атаки, а также минимизировать ложные срабатывания, которые приводят к неоправданным затратам ресурсов. Скорость нейтрализации угрозы определяется метриками вроде MTTD (Mean Time to Detect) и MTTR (Mean Time to Respond). Например, система, которая обнаруживает фишинговую атаку за 5 минут и блокирует её за 2 минуты, считается высокоэффективной. Однако избыточная агрессивность защиты, например, частое блокирование легитимного трафика из-за ошибочных правил IPS (Intrusion Prevention System), снижает доверие к системе и увеличивает нагрузку на аналитиков.

Методические рекомендации:

a. Рекомендуется проводить практикумы по расчету MTTD и MTTR на основе данных реальных инцидентов (например, атак на критическую инфраструктуру).

b. Анализировать кейсы, где высокая частота ложных срабатываний привела к игнорированию реальных угроз (эффект «усталости оповещений»).

c. Использовать симуляторы вроде Breach and Attack Simulation (BAS) для оценки баланса между скоростью реакции и точностью.

2. Технологии активного противодействия: от автоматических систем до тактик дезинформации

Современные технологии активной защиты включают автоматизированные системы (IPS, Next-Gen Firewalls), honeypots (ловушки для хакеров) и методы дезинформации злоумышленников. IPS-системы анализируют сетевой трафик в режиме реального времени, блокируя подозрительные действия на основе сигнатур и поведенческих паттернов. Honeypots имитируют уязвимые сервисы, собирая данные о тактиках атакующих, что позволяет улучшать защиту. Дезинформация, такая как поддельные учетные данные или фальшивые файлы, замедляет продвижение злоумышленников и увеличивает их затраты на атаку. Например, внедрение honeypot в корпоративную сеть может выявить сканирование портов и попытки эксплуатации уязвимостей.

Методические рекомендации:

a. Организовывать лабораторные работы с развертыванием honeypots (например, используя инструмент Cowrie для эмуляции SSH-серверов).

b. Моделировать сценарии, где студенты настраивают правила IPS для блокировки конкретных типов атак (SQLi, XSS).

c. Изучать примеры операций дезинформации, такие как Project Honey Pot в борьбе со спамом.

3. Оценка в условиях реального времени: роль SIEM-систем и анализа журналов

SIEM-системы (Security Information and Event Management), такие как Splunk или IBM QRadar, агрегируют данные с различных источников (сетевые устройства, серверы, приложения) и коррелируют события для выявления аномалий. Например, одновременное возникновение множества failed login attempts с разных IP-адресов и последующая попытка доступа к базе данных может сигнализировать о скоординированной атаке. Анализ журналов (лог-файлов) позволяет реконструировать цепочку событий и определить точки компрометации. Ключевая задача – обеспечить минимальную задержку между сбором данных и их интерпретацией, чтобы реагирование происходило до эскалации угрозы.

Методические рекомендации:

a. Настраивать SIEM-системы в учебных средах для мониторинга искусственно сгенерированных атак.

b. Проводить тренировки по анализу логов с использованием запросов на языке SPL (Search Processing Language) в Splunk.

c. Изучать инциденты, такие как атака на SolarWinds, чтобы понять роль логов в расследовании.

4. Устойчивость к адаптивным атакам

Адаптивные атаки меняют тактику в ответ на внедренные защитные меры. Например, злоумышленники могут использовать полиморфные вредоносы, изменяющие свой код для обхода сигнатурных анализаторов, или применять методы обфускации трафика. Для противодействия таким угрозам используются технологии машинного обучения, анализирующие поведенческие аномалии, и системы, реализующие принцип Zero Trust. Тестирование устойчивости включает стресс-тесты, где защита подвергается атакам, имитирующим адапта-

цию (например, изменение векторов атак после блокировки первоначальных методов).

Методические рекомендации. Использовать фреймворки вроде MITRE Shield для моделирования адаптивных атак и разработки контрмер.

a. Проводить анализ кейсов, таких как Emotet, который постоянно эволюционировал для обхода детектирования.

b. Внедрять в учебный процесс задачи по настройке поведенческих анализаторов (например, Darktrace).

Методы оценки эффективности активного противодействия требуют комплексного подхода, сочетающего технические навыки, аналитическое мышление и понимание тактик противника. Практические занятия должны фокусироваться на работе с реальными инструментами и данными, чтобы студенты могли оценивать компромиссы между скоростью, точностью и ресурсозатратностью защитных мер. Особое внимание следует уделять этическим аспектам: даже агрессивные методы дезинформации должны соответствовать правовым нормам и не нарушать границы допустимого.

Литература

1. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/385979 (дата обращения: 08.10. 2024). – ISBN 978-5-507- 48601-4. – Текст : электронный (гл. 3–5).

2. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный (гл. 4–8, 17, 18).

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный Ч. 1. – 171 с. (гл. 1, параграф 1.5).

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=70 0833 (дата обращения: 08.10.2024). – ISBN 978- 5-8149-3250-1. – Текст : электронный (гл. 4).

5. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL:

https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст : электронный (гл. 6–8, 21).

6. Подтопельный, В. В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный. – Калининград: БГАРФ, 2020. – Текст : непосредственный. – Ч. 3. Поиск и извлечение вредоносных программ в программной среде. – 2020. – 99 с.

7. Подтопельный, В. В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2020. – Текст : непосредственный. – Ч. 4. Настройка подсистем СЗИ. – 2021. – 97 с.

Контрольные вопросы

1. Какие метрики, кроме MTTD и MTTR, можно использовать для оценки скорости нейтрализации угроз? Обоснуйте их relevance.
2. Объясните, как honeypots способствуют сбору разведданных о тактиках злоумышленников. Приведите пример использования в корпоративной сети.
3. Почему высокая частота ложных срабатываний IPS может снизить общую эффективность защиты?
4. Опишите сценарий, в котором SIEM-система помогла предотвратить многоэтапную атаку за счет корреляции событий из разных источников.
5. Какие ограничения имеют сигнатурные методы анализа при противодействии адаптивным атакам?
6. Сравните эффективность дезинформации и автоматической блокировки трафика как методов активного противодействия.
7. Как принцип Zero Trust Architecture повышает устойчивость к атакам, эволюционирующим в ответ на традиционные меры защиты?
8. Какие этические проблемы возникают при внедрении методов дезинформации в рамках активной защиты?

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Практические 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 практическими занятиями необходимо проработать соответствующие разделы лекционного материала;

– рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом практического 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 практическом 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 практических занятий приводится в разделе «Тематический план».

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 «Теория анализа компьютерных атак»

Цели каждой отдельной курсового проекта должны раскрывать выбранную студентом тему. Курсовой проект предназначен для углубления студентами теоретических и практических навыков в области обеспечения информационной безопасности связанного с анализом компьютерных атак. 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 системах с учетом результатов анализа компьютерных атак. 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 курсового 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 проектов является закрепление, углубление и обобщение знаний, полученных студентом за время теоретического и практического обучения, расширение объема профессионально значимых умений и навыков.

Различия курсовой работы и курсового проекта в следующем: курсовой проект в обязательной практической части предполагает работу над сложной расчетной и (или) проектной задачей, содержит описание хода решения задач и отчетные данные. Как правило, курсовой проект характерен для информационных или инженерных направлений, или специальностей.

Содержание курсовых проектов должно отвечать учебным задачам дисциплины, увязываться с последующей работой выпускников по специальности /направлению подготовки.

Поэтому в цели и задачи курсового 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 курсового 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 курсового проекта обучающимся рекомендуется использование элементов дистанционных образовательных технологий с использованием информационных и учебно-методических ресурсов. При этом график курсового 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 курсовой проект, 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 проектах и в период учебных практик;

– исключение по возможности дублирования (дословного совпадения формулировок) тем курсовых 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.

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

Курсовой проект 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.

Курсовой проект 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 курсовой проект должна быть подписана студентом.

Примерные темы курсовых проектов

1. Вероятностная оценка риска APT-атак с использованием байесовских сетей (на примере атаки SolarWinds).
2. Моделирование распространения сетевых червей на основе уравнений диффузии.
3. Анализ эффективности алгоритмов машинного обучения для детектирования аномалий в сетевом трафике: сравнение ROC-кривых.
4. Статистический анализ временных рядов логов для прогнозирования DDoS-атак.
5. Применение теории игр для моделирования взаимодействия атакующего и системы защиты.
6. Оценка вероятности успеха фишинговой атаки с использованием логистической регрессии.
7. Анализ метрик False Positive Rate в системах IDS: методы минимизации на основе распределения Пуассона.
8. Моделирование цепочек кибератак с помощью марковских процессов (на примере Kill Chain).
9. Статистическая кластеризация вредоносных доменов на основе DNS-запросов.
10. Вероятностные методы идентификации ботнетов в трафике IoT-устройств.
11. Математический анализ полиморфизма в коде вредоносов: метрики энтропии и их интерпретация.

12. Оценка времени жизни эксплойта в системе с обновлениями: модель на основе процессов восстановления.

13. Анализ поведения ransomware через стохастические автоматы (на примере WannaCry).

14. Моделирование жизненного цикла вредоносного ПО с использованием цепей Маркова.

15. Количественная оценка ущерба от атак на SCADA-системы: методы Монте-Карло.

16. Алгоритмы обнаружения скрытых каналов связи в сетевом трафике на основе анализа энтропии.

17. Оптимизация правил сигнатурного анализа с использованием генетических алгоритмов.

18. Анализ эффективности методов PCA (Principal Component Analysis) для снижения размерности данных в IDS.

19. Вероятностное обнаружение DNS-туннелирования через анализ распределения запросов.

20. Моделирование латентных периодов атак на основе временных рядов (ARIMA/SARIMA).

21. Вероятностный анализ устойчивости хеш-функций к коллизиям: сравнение SHA-256 и BLAKE3.

22. Оценка сложности brute-force-атак на алгоритмы шифрования с использованием распределения Больцмана.

23. Математические методы анализа side-channel атак на RSA (на примере атак по времени).

24. Моделирование атак на гомоморфное шифрование: оценка ошибок декодирования.

25. Разработка математической модели для оценки эффективности песочницы Cuckoo Sandbox против zero-day угроз.

26. Анализ эффективности Suricata vs Snort: сравнение метрик точности и производительности.

27. Прогнозирование векторов атак на основе анализа уязвимостей CVE: регрессионные модели.

28. Вероятностная оценка времени до компрометации системы (Time-to-Compromise) на основе данных MITRE ATT&CK.

29. Анализ корреляции между активностью в Dark Web и реальными кибератаками: методы кросс-энтропии.

30. Оптимизация honeypot-сетей через теорию массового обслуживания (модели M/M/1 и M/G/1).

6. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

Текущая аттестация

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации:

Преподаватель вправе выбрать методику оценивания знаний студентов: традиционная зачетно-экзаменационная, либо балльно-рейтинговая.

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.

Выбрана традиционная зачетно-экзаменационная методика оценивания знаний

Предусматривается: зачет, экзамен, курсовой проект

Текущая аттестация

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

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

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**	**2**	**3**	**4**	**5**
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между	Обладает минимальным набором знаний, необходимым для системного	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект

Система оценок / Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
	собой (только некоторые из которых может связывать между собой)	взгляда на изучаемый объект		
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно-корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

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

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

Завершающим этапом изучения дисциплины является итоговая аттестация, представляющая собой зачет (5 семестр), экзамен (6 семестр)

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. Назовите основные категории методов обнаружения атак. В чем ключевое отличие сигнатурного и аномального анализа?
2. Приведите примеры гибридных систем обнаружения атак и объясните их преимущества.
3. Какие критерии используются для классификации методов обнаружения атак по типу обрабатываемых данных (сетевые, хостовые, гибридные)?
4. Опишите принцип работы поведенческого анализа в контексте обнаружения APT-атак. Какие метрики поведения чаще всего анализируются?
5. Какие ограничения имеет поведенческий анализ при работе с зашифрованным трафиком?
6. Как методы анализа аномалий (например, кластеризация) применяются для выявления подозрительной активности пользователей?
7. Перечислите алгоритмы машинного обучения, наиболее эффективные для обнаружения DDoS-атак. Обоснуйте их выбор.
8. В чем заключается проблема «ложных срабатываний» (False Positives) в системах на основе ML? Какие методы позволяют её минимизировать?
9. Как генетические алгоритмы могут быть использованы для оптимизации правил в IDS/IPS? Приведите пример.
10. Какие особенности данных требуют применения методов глубокого обучения (DL) для анализа сетевых атак?
11. Опишите модель Cyber Kill Chain. Как её этапы связаны с анализом процессов реализации угроз?
12. Какие методы используются для анализа временных характеристик атак (например, латентный период, скорость распространения)?
13. Как анализ логов помогает восстановить цепочку событий при многоэтапной атаке? Приведите пример из реального кейса.
14. Какие математические модели (например, марковские цепи, Petri-сети) применяются для моделирования этапов атаки?
15. Как теория игр используется для анализа взаимодействия злоумышленника и системы защиты?

16. Объясните, как метод Монте-Карло помогает оценивать риски реализации угроз в корпоративной сети.

17. На примере атаки WannaCry опишите, как методы сигнатурного и поведенческого анализа могут быть совмещены для её обнаружения.

18. Какие вероятностные метрики (например, F1-score, AUC-ROC) наиболее релевантны для оценки эффективности ML-моделей в обнаружении атак?

19. Как моделирование на основе временных рядов (ARIMA, LSTM) применяется для прогнозирования кибератак?

20. Предложите метод аналитического моделирования для оценки устойчивости системы к атаке типа «человек посередине» (MITM).

Вопросы к экзамену

1. Дайте определение понятию «риск удаленного доступа» в контексте ИТКС. Какие факторы его формируют?

2. Опишите этапы методики анализа рисков при множественных угрозах удаленного доступа (на примере стандарта NIST SP 800-30).

3. Как матрица вероятности/ущерба используется для приоритизации рисков? Приведите пример.

4. Какие методы количественной оценки рисков (например, FAIR, OCTAVE) подходят для анализа угроз к критически важным системам?

5. Объясните, как регулируются риски при одновременной реализации нескольких угроз (на примере атак на цепочку поставок).

6. Как учитывается человеческий фактор при оценке рисков удаленного доступа к ИТКС?

7. Какие инструменты (например, MITRE ATT&CK) используются для моделирования сценариев комбинированных атак?

8. Опишите методологию оценки остаточного риска после внедрения защитных мер.

9. Как стандарт ISO 27005 применяется для управления рисками в распределенных ИТКС?

10. Приведите пример регуляторных требований (например, ФЗ-187) к защите критических информационных систем.

11. В чем разница между натурным и имитационным моделированием? Какие ограничения есть у каждого метода?

12. Опишите процесс создания цифрового двойника критической системы для имитации атак (на примере SCADA).

13. Какие инструменты (например, NS-3, GNS3) используются для моделирования сетевых атак на ИТКС?

14. Как валидируются результаты имитационного моделирования? Приведите метрики достоверности.

15. Смоделируйте сценарий атаки на энергетическую инфраструктуру с использованием фреймворка CORE.

16. Какие данные необходимы для натурного моделирования атаки типа «отказ в обслуживании» (DoS) на промышленный контроллер?

17. Как учитываются скрытые угрозы (zero-day) при проектировании имитационных моделей?

18. Опишите метод «красных команд» (Red Teaming) в контексте натурного тестирования защиты ИТКС.

19. Какие этические и юридические ограничения существуют при натурном моделировании атак?

20. Как результаты моделирования интегрируются в политики безопасности организации?

21. Дайте определение «эффективности атаки». Какие метрики используются для её оценки (например, время до компрометации)?

22. Опишите методику проведения контролируемого эксперимента по оценке фишинговой атаки.

23. Как измеряется успешность атаки на систему с многофакторной аутентификацией?

24. Какие статистические методы (например, A/B-тестирование) применяются для сравнения эффективности разных векторов атак?

25. Приведите пример экспериментальной оценки атаки на шифровальный модуль (например, криптоанализ AES).

26. Как учитываются ложные срабатывания при оценке эффективности атак на системы обнаружения вторжений (IDS)?

27. Опишите процесс оценки устойчивости системы к атакам типа «человек посередине» (MITM) в лабораторных условиях.

28. Какие инструменты (например, Metasploit, Cobalt Strike) используются для автоматизации экспериментов?

29. Как результаты экспериментов по оценке атак влияют на обновление Threat Intelligence?

30. На примере атаки Stuxnet объясните, как экспериментальные данные помогли выявить уязвимости в промышленных системах.

31. Перечислите критерии оценки эффективности активного противодействия (например, время реакции, точность блокировки).

32. Опишите методологию тестирования системы IPS на устойчивость к APT-атакам.

33. Как оценивается эффективность динамического изменения правил фаервола в режиме реального времени?

34. Какие метрики (например, MTTD – Mean Time to Detect) используются для анализа работы SOC?

35. Сравните эффективность сигнатурного и поведенческого анализа в контексте противодействия файловым вирусам.

36. Как метод «обратного инжиниринга» помогает оценить устойчивость защиты к атакам на ПО?

37. Опишите процесс оценки эффективности honeypot-сетей для сбора данных об атакующих.

38. Какие методы машинного обучения применяются для адаптации систем защиты к новым угрозам?

39. Приведите пример оценки экономической эффективности внедрения системы SIEM.

40. На примере атаки на Colonial Pipeline объясните, как анализ логов помог улучшить активное противодействие.

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

Основная литература

1. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/385979 (дата обращения: 08.10. 2024). – ISBN 978-5-507- 48601-4. – Текст : электронный.

2. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/438971 (дата обращения: 04.12.2024). – ISBN 978-5-507- 50467-1. – Текст : электронный.

3. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2023. – Текст : непосредственный. Ч. 1. – 171 с.

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=70 0833 (дата обращения: 08.10.2024). – ISBN 978- 5-8149-3250-1. – Текст : электронный.

5. Баланов, А. Н. Кибербезопасность: учеб. пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с. – Режим доступа: для авториз. пользователей. – Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/422558 (дата обращения: 04.12.2024). – ISBN 978-5-507-49562-7. – Текст : электронный.

Дополнительная литература

6. 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: 05.10.2024). – ISBN 978-5-238-03639-7. – Текст: электронный.

7. Программно-аппаратные средства обеспечения информационной безопасности: лаб. практикум для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» / Федер. агентство по рыболовству, Калининигр. гос. техн. ун-т, Балт. гос. акад. рыбопромыслового флота; сост.: А. Г. Жестовский, В. В. Подтопельный. – 2-е изд., перераб. и доп. – Калининград: БГАРФ, 2019. – Режим доступа: для авториз. пользователей. – URL: https://lib.klgtu.ru/web/index.php (дата обращения: 05.11.2024). – ISBN 978-5-238-03639-7. – Текст : электронный. – 2019. – Текст : непосредственный. – Ч. 1. Защита компьютерной информации и компьютерных систем от вредоносных программ.

8. Жестовский, А. Г. Программно-аппаратные средства обеспечения информационной безопасности: учеб. пособие для студентов высш. учеб. заведений, обучающихся по направлению «Информ. Безопасность», по прогр. подгот. бакалавров, магистров, специалистов / А. Г. Жестовский, В. В. Подтопельный ; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2018. – Текст : непосредственный. – Ч. 2. Настройка систем защиты информации от несанкционированного доступа. – 2018. – 100 с.

9. Подтопельный, В. В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный. – Калининград: БГАРФ, 2020. – Текст : непосредственный. – Ч. 3. Поиск и извлечение вредоносных программ в программной среде. – 2020. - 99 с.

10. Подтопельный, В. В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. пособие для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2020. – Текст : непосредственный. – Ч. 4. Настройка подсистем СЗИ. – 2021. – 97 с.

11. Аверченков, В. И. Аудит информационной безопасности: учеб. пособие / В. И. Аверченков. – 4-е изд., стер. – Москва: ФЛИНТА, 2021. – 269 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 05.11.2024). – ISBN 978-5-9765-1256-6. – Текст : электронный.

Учебно-методические пособия, нормативная литература

12. Информационная безопасность распределенных информационных систем: метод. указания по выполнению лабораторных работ для студентов спе-

циальности 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения / Федер. агентство по рыболовству [и др.]; сост. В. В. Подтопельный. – Калининград: БГАРФ, 2020. – Текст : непосредственный. Ч. 1 / сост. В. В. Подтопельный. – 2020. – 61 с.

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

14. Комплексное обеспечение информационной безопасности автоматизированных систем: метод. указания по выполнению лаб. работ для студентов специальности 10.05.03 «Информ. безопасность автоматизир. систем» всех форм обучения / Федер. агентство по рыболовству [и др.]; авт.-сост.: В. В. Подтопельный, А. А. Бабаева. – Калининград: БГАРФ, 2021. – Текст : непосредственный. Ч. 1. – 2021. – 53 с.

15. «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.

16. «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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. «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.

23. «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.

24. «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.

25. «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

ТЕОРИЯ АНАЛИЗА КОМПЬЮТЕРНЫХ АТАК

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 4,8. Печ. л. 3,7.

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