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

В. В. Подтопельный

ТЕОРИЯ АНАЛИЗА КОМПЬЮТЕРНЫХ АТАК

Учебно-методическое пособие по практическим занятиям
для студентов специальности 10.05.03
«Информационная безопасность автоматизированных систем»
специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2026

УДК 004.056.5(075)

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

Подтопельный, В. В.
Теория анализа компьютерных атак: учебно-методическое пособие по практическим занятиям для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем» / В. В. Подтопельный. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2026. – 62 с.

Учебно-методическое пособие включает в себя рассмотрение практических вопросов в области защиты информации по дисциплине «Теория анализа компьютерных атак». В учебно-методическом пособии приведен набор практических работ для изучения и закрепления материала дисциплины. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы дисциплины.

Учебно-методическое пособие предназначено для студентов 3-го курса специальности 10.05.03 «Информационная безопасность автоматизированных систем» и смежных специальностей.

Табл. 9, список лит. – 16 наименований

Учебно-методическое пособие рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 29 сентября 2026 г., протокол № 7

УДК 004.056.5(075)

© Федеральное государственное бюджетное образовательное учреждение высшего образования «Калининградский государственный технический университет», 2026 г.
© Подтопельный В. В., 2026 г.

ОГЛАВЛЕНИЕ

Введение 4
Практическое занятие № 1. Специфика применения методов обнаружения атак и анализа компьютерных атак 8
Практическое занятие № 2. Использование методов вычислительного интеллекта для анализа компьютерных атак 13
Практическое занятие № 3. Специфика анализа атак как процессов угроз 18
Практическое занятие № 4. Аналитическое моделирование процессов реализации угроз 24
Практическое занятие № 5. Методика анализа и регулирования рисков при реализации нескольких угроз 29
Практическое занятие № 6. Метод натурного и имитационного моделирования процессов компьютерных атак и противодействия им 34
Практическое занятие № 7. Метод экспериментальной оценки эффективности компьютерных атак 39
Практическое занятие № 8. Метод оценки эффективности активного противодействия компьютерным атакам на критически важные информационные системы 44
Дополнительные методические материалы и примеры расчётов 49
Задания для самостоятельной работы 55
Описание текущего контроля 58
Заключение 60
Литература 61

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». Пособие разработано в соответствии с требованиями утверждённой рабочей программы дисциплины и ориентировано на подготовку специалистов, способных решать задачи обнаружения, анализа и моделирования компьютерных атак на информационные системы.

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;

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».

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. Задачи освоения материала пособия предполагают, что в итоге освоения студент должен:

знать (теоретический базис):

– способы поиска и анализа уязвимостей: методы обнаружения атак (сигнатурные, поведенческие, гибридные) и метрики их качества (Precision, Recall, F1, AUC ROC). методики оценки рисков (SLE, ARO, ALE, FAIR, матрица рисков) и модели регулирования устойчивости;

– методы учета уязвимостей, метрические спецификации уязвимостей и угроз: методы планирования эксперимента (полный и дробный факторный план, Монте-Карло) и статистической обработки данных;

– методы моделирования компьютерных атак и их исследование, и методы анализа компьютерных атак: формальные модели атак (деревья атак, сети Петри, марковские цепи, CyberKillChain, MITRE ATT&CK), аналитические модели динамики атак и противодействия (системы дифференциальных уравнений, модели массового обслуживания, SIR-модель;

уметь (практические навыки):

– осуществлять поиск уязвимостей (настраивать и использовать системы обнаружения вторжений (Suricata) и анализаторы трафика (Wireshark, Scapy));

– моделировать компьютерные атаки и анализировать, и прогнозировать с учетом специфики информационных систем и нарушителей (строить графы (деревья атак, сети Петри, сетевые графики) и рассчитывать вероятности реализации угроз);

– использовать методы определения метрических характеристик уязвимостей (планировать и проводить имитационные эксперименты на стендовом полигоне, обрабатывать результаты статистическими методами (доверительные интервалы, проверка гипотез).

В практических работах приведены подробные сведения обизучаемых 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.

Пособие содержит восемь практических занятий, соответствующих основным разделам рабочей программы дисциплины. Каждое занятие включает цель и перечень необходимых материалов; развёрнутое Методический материал к выполнению заданий с определениями, формулами и математическими моделями; практические задания, требующие аналитических расчётов и интерпретации результатов; методические указания по порядку выполнения; требования к отчёту и защите; контрольные вопросы для самопроверки.

Задания ориентированы на развитие навыков формализации процессов атак, применения вероятностных, статистических и оптимизационных моделей, а также критического анализа получаемых численных результатов. Особое внимание уделено математизации постановок задач: используются аппарат теории вероятностей и математической статистики, теория марковских процессов, элементы теории игр, методы оптимизации и численные методы решения дифференциальных уравнений.

Особое внимание при выполнении заданий следует уделять корректности математических выкладок, обоснованности принятых допущений и содержательной интерпретации численных результатов. Формальный ответ без пояснения прикладного смысла полученной величины не считается полным. При построении моделей необходимо явно указывать область применимости и ограничения используемого математического аппарата.

В процессе работы над заданиями студентам рекомендуется вести рабочую тетрадь или электронный журнал с промежуточными расчётами, графиками и замечаниями. Это существенно упрощает подготовку итогового отчёта и защиту работы. При возникновении затруднений следует обращаться к преподавателю в установленные часы консультаций.

Шкала оценок уровня (таблица А) содержит требования к завершающей аттестации – зачету и экзамену.

Помимо данного УМП, 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 GeneralPublicLicense (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 "OpenValueSubscription").

2. Офисное приложение MS OfficeStandard 2016 (получаемое по программе Microsoft "OpenValueSubscription").

3. Kaspersky Endpoint Security.

4. Google Chrome (GNU).

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

6. MathCAD 15 M020.

7. Python (GNU/Linux,macOSи Windows).

8. PascalABC.Net.

9. 1C:Enterprise 8.

10. blender

11. GPSS World Student Version

12. Microsoft Visual Studio Code (получаемое по программе Microsoft "Open Value Subscription").

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

14. Аппаратно-программный комплекс шифрования (допустимо использвание АПКШ «Континент» или др.)

15. DLP-система (допустимо использвание DLP SecureTower)

16. Системы защиты информации (допустимо использвание СЗИ Dallas Lock и др.)

Практическое занятие № 1. Специфика применения методов обнаружения атак и анализа компьютерных атак

Общие сведения

Цель: сформировать навыки решения типовых и прикладных задач из в области применения сигнатурных, поведенческих и гибридных методов обнаружения атак и анализа компьютерных атак; освоить расчёт метрик качества обнаружения (precision, recall, F1, AUC ROC) и приобрести навыки настройки свободно распространяемой системы обнаружения вторжений Suricata для выявления сетевых атак.

Перечень знаний и умений для достижения цели:

Знать: классификацию методов обнаружения атак; структуру матрицы ошибок и метрики качества (Precision, Recall, F1, FPR, AUC ROC); синтаксис и логику правил систем обнаружения вторжений (на примере Suricata).

Литература: [7] С. М. Климов и др. (разделы о рубежах противодействия и паспортах атак); [12] Ю. М. Краковский (методы и средства защиты информации); [5] NIST SP 800-61 (руководство по обработке инцидентов).

Уметь: настраивать правила IDS для перехвата специфичных атак (например, SSH brute-force); генерировать тестовый сетевой трафик (scapy); рассчитывать метрики качества детектирования по собранным журналам событий.

Литература: [7] С. М. Климов и др. (разделы о рубежах противодействия и паспортах атак); [12] Ю. М. Краковский (методы и средства защиты информации); [5] NIST SP 800-61 (руководство по обработке инцидентов); [13] А. А. Магазев (противодействие сетевым атакам в ЛВС); [5] NIST SP 800-61

Материалы, оборудование, программное обеспечение: ПК с ОС KaliLinux, система обнаружения атак Suricata, анализатор трафика Wireshark, генератор пакетов scapy, сканер Nmap, стендовый полигон с сегментом ЛВС, Python 3 с библиотеками NumPy, SciPy, Matplotlib, scikit–learn.

1. Методический материал по выполнению практических заданий

Под компьютерной атакой в соответствии с методикой С. М. Климова, М. П. Сычёва и А. В. Астрахова понимается целенаправленное программно–аппаратное воздействие на информационно-телекоммуникационные средства, приводящее к нарушению или снижению эффективности выполнения технологических циклов управления в критически важной информационной системе (ИС). Своевременное обнаружение атак является первым и одним из ключевых этапов технологии противодействия, поскольку от оперативности

обнаружения зависят последующие действия по анализу, нейтрализации и активному противодействию.

Классификация методов обнаружения

Современные системы обнаружения атак (СОА, в англоязычной литературе – IDS, IntrusionDetectionSystem) подразделяются по характеру используемых признаков на три основных класса: сигнатурные, поведенческие (на основе аномалий) и гибридные. Сигнатурный метод основан на сопоставлении наблюдаемых событий с заранее подготовленным набором сигнатур известных атак. Он обеспечивает высокую точность обнаружения известных атак, но бесполезен против атак, для которых сигнатуры ещё не разработаны. Поведенческий метод формирует профиль нормального поведения системы и фиксирует отклонения от него. Этот метод способен выявлять ранее неизвестные атаки (zero–day), но порождает значительное количество ложных срабатываний. Гибридный подход сочетает оба принципа, дополняя их методами функционального анализа.

По расположению датчиков СОА подразделяются на сетевые (NIDS, анализирующие трафик в сегменте ЛВС) и хостовые (HIDS, контролирующие события на отдельном АРМ или сервере). По характеру реагирования различают пассивные IDS, которые только регистрируют события, и активные IPS (IntrusionPreventionSystem), способные блокировать или переадресовывать подозрительные соединения. Дополнительно выделяют прикладной уровень анализа – системы защиты веб–приложений (WAF), такие как ModSecurity.

Рубежи противодействия и паспорт атаки

В соответствии с методикой Климова противодействие атакам организуется на семи рубежах: удалённого доступа, ЛВС, доступа к АРМ, операционной системы, системы управления базами данных, специального программного обеспечения и геоинформационной системы. На каждом рубеже размещаются соответствующие датчики СПКА, непрерывно собирающие данные о событиях и состояниях защищаемой системы. Совокупность событий, поступающих с разных рубежей, позволяет восстановить сквозной сценарий атаки и сопоставить его с её паспортом – структурированным описанием, содержащим идентификатор, наименование, класс, вектор реализации, признаки (сигнатуры) и рекомендации по нейтрализации.

Метрики качества обнаружения

Для количественной оценки эффективности СОА используются метрики классификации, основанные на матрице ошибок (confusionmatrix). При бинарной классификации «атака / норма» различают истинно положительные (TP – атака обнаружена), ложно положительные (FP – ложное срабатывание), истинно отрицательные (TN – норма правильно классифицирована) и ложно отрицательные (FN – атака пропущена) исходы. На основе этих значений рассчитываются:

$$Precision = TP/(TP + FP). \quad (1.1)$$

$$Recall(TPR) = TP/(TP + FN)\ . \quad (1.2)$$

$$F1 = 2 \cdot Precision \cdot Recall/(Precision + Recall). \quad (1.3)$$

$$FPR = FP/(FP + TN). \quad (1.4)$$

Кривая ROC (ReceiverOperatingCharacteristic) строится в координатах TPR (по оси ординат) и FPR (по оси абсцисс) при варьировании порога решающего правила. Площадь под ROC–кривой (AUC ROC) служит сводной метрикой качества классификатора: AUC = 0,5 соответствует случайному угадыванию, AUC = 1,0 – идеальному классификатору. На практике значение AUC ≥ 0,90 считается высоким. Байесовский подход основан на сравнении апостериорных вероятностей. По формуле Байеса $P(attack \vee x) = P(x \vee attack) \cdot P(attack)/P\,(x)$. Решение принимается в пользу атаки, если P(attack | x) >γ. Оптимальный порог минимизирует средний риск $R = cFP \cdot \alpha \cdot P(normal) + cFN \cdot \beta \cdot P(attack)$.

В условиях сильного дисбаланса классов рекомендуется использовать метрики, устойчивые к дисбалансу, такие как PR–AUC и коэффициент корреляции Мэтьюса $MCC = (TP \cdot TN - FP \cdot FN)/\sqrt{[(TP + FP)(TP + FN)(TN + FP)(TN + FN)]}$. Специфика применения методов зависит от уровня наблюдения: сетевой (NIDS), хостовый (HIDS) или прикладной.

2. Методические указания к практическому занятию и порядок выполнения заданий. Задания

Задание 1

1. Установить и настроить Suricata в среде KaliLinux, проверить работоспособность на тестовом интерфейсе; определить максимальное число правил N, при котором загрузка процессора L (по формуле 1.5) не превышает 70 %, приняв M = 1000 пак/с, C = 8 операций/пакет, R = 10^8 операций/с.

2. Сгенерировать с помощью scapy серию тестовых пакетов, имитирующих сканирование портов (TCP SYN scan) и подбор паролей по SSH, и перехватить их Wireshark’ом; для каждого типа атаки подсчитать TP, FP, TN, FN по журналу Suricata.

3. Рассчитать значения Precision, Recall, F1 и FPR по формулам (1.1)–(1.4) отдельно для сигнатурного и поведенческого модулей; сравнить с табличными значениями из таблицы 1.1 и объяснить расхождения.

4. Построить ROC–кривую по 11 точкам (порог от 0 до 1 с шагом 0,1), рассчитать AUC ROC методом трапеций и сделать вывод о качестве классификатора; определить оптимальный порог по критерию максимума F1.

5. Разработать собственное правило Suricata для обнаружения характерного признака атаки (например, sequenceof TCP SYN packets к различным портам за короткий интервал) и оценить его вклад в повышение Recall при допустимом снижении Precision (не более чем на 0,02).

6. Рассчитать информативность (informationgain) признаков «число уникальных портов в секунду» и «средняя длина пакета» по выборке из 1000 записей и сделать вывод о целесообразности их включения в поведенческую модель. Рассмотреть возможность использования АПКШ «Континент» или др., DLP-систем (на примере DLP SecureTower), системы защиты информации (СЗИ Dallas Lock и др.) для обнаружения признаков атак.

7. Сформулировать выводы о применимости сигнатурного, поведенческого и гибридного методов для защиты типовой ИС; указать, на каких рубежах противодействия целесообразно использовать каждый из методов.

Задание 2

1. Задана выборка из N = 10 000 наблюдений, из которых Na = 800 соответствуют атакам. Сигнатурный детектор обнаружил 720 атак и выдал 45 ложных тревог. Аномальный детектор при пороге $\tau 1$ обнаружил 650 атак и выдал 180 ложных тревог; при пороге $\tau 2$ – 780 атак и 420 ложных тревог. Рассчитайте для каждого детектора значения Precision, Recall, FPR, F1–score и Accuracy. Постройте сравнительную таблицу. Сделайте вывод о предпочтительности детекторов при разных приоритетах (минимизация пропусков / минимизация ложных тревог).

2. Предполагая, что условные распределения скора детектора для атакующего и нормального трафика аппроксимируются нормальными законами с параметрами ($\mu_a = 3{,}2$; $\sigma_a = 1{,}1$) и ($\mu_n = 0{,}5$; $\sigma_n = 0{,}9$), а P(attack) = 0,08, найдите байесовский порог γ^*, минимизирующий среднюю стоимость ошибки при cFP = 1, cFN = 5. Вычислите α и β. Постройте графики плотностей.

3. Постройте аналитическую модель ROC–кривой для детектора с нормальными распределениями скоров из задания 2. Выразите TPR и FPR через функцию распределения нормального закона. Рассчитайте AUC численным интегрированием с шагом $\Delta\tau = 0{,}05$. Сравните с теоретической оценкой AUC для двух нормальных распределений.

4. Рассмотрите гибридную схему: сигнатурный детектор применяется первым, аномальный с порогом τ_1 – только к объектам, не сработавшим по сигнатуре. Оцените итоговые TP, FP, FN, TN, Precision, Recall и F1–score гибридной системы. Сравните с отдельными детекторами.

5. Сформулируйте и количественно обоснуйте рекомендации по выбору метода и настройке порога для сценариев: (а) критическая инфраструктура с $cFN/cFP \geq 20$; (б) высоконагруженная сеть с допустимым уровнем ложных тревог $\leq 0{,}5$ %. Приведите оценки ожидаемого риска.

Пояснение к порядку выполнения работы

В рамках занятия студент выполняет настройку Suricata на учебном стенде, генерирует тестовый трафик и собирает статистику срабатываний. По результатам строится матрица ошибок и рассчитываются метрики качества.

Базовое правило Suricata имеет вид:

alert tcp $EXTERNAL_NET any –> $HOME_NET 22 (msg:"SSH brute–force"; flow:to_server; detection_filter:trackby_src, count 5, seconds 30; sid:1000001;)

При обработке N правил с интенсивностью трафика M пакетов в секунду и сложности правила C (среднее число проверок на пакет) оценочная загрузка процессора составляет:

$$L = N \cdot M \cdot C / R, \tag{1.5}$$

где R – производительность процессора (операций/с). По этому соотношению подбирается максимальное N, при котором загрузка не превышает 70 %.

Таблица 1.1 – Сравнительные метрики методов обнаружения атак

Метрика	Сигнатурный	Поведенческий	Гибридный
Precision	0,95–0,99	0,60–0,85	0,90–0,97
Recall (известные атаки)	0,90–0,98	0,70–0,90	0,92–0,98
Recall (zero–day)	0,00–0,10	0,40–0,70	0,50–0,80
FPR	0,001–0,01	0,02–0,10	0,005–0,03
AUC ROC	0,90–0,98	0,75–0,90	0,92–0,98

Требования к отчёту и защите

Защита предполагает опрос по материалу, изложенному в отчёте. Отчёт должен быть оформлен: требуется наличие титульного листа, указание цели практического занятия, последовательное изложение выполненных расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания. Проверяется знание теоретического материала с учётом ответов на контрольные вопросы. Задаются вопросы по пунктам, приведённым в разделе «Порядок выполнения работы». Критерии к оценке защиты отчёта студентом приведены в таблице 9.1.

Контрольные вопросы для самопроверки

1. Дайте определение компьютерной атаке по методике С. М. Климова.

2. Чем система обнаружения вторжений (IDS) отличается от системы предотвращения вторжений (IPS)?

3. Какие классы методов обнаружения атак вы знаете? Сформулируйте их преимущества и недостатки.

4. Что такое сигнатура атаки и из каких элементов состоит правило Suricata?

5. Перечислите семь рубежей противодействия, выделяемых по методике Климова.

6. Запишите формулы для расчёта Precision, Recall, F1 и FPR; поясните смысл каждой метрики.

7. Что такое ROC–кривая и площадь под ней (AUC ROC)? При каких значениях AUC классификатор считается качественным?

8. Что такое паспорт компьютерной атаки и для чего он используется в технологии противодействия атакам?

9. В чём принципиальное различие сигнатурных и аномальных методов обнаружения атак? Приведите примеры инструментов каждого класса.

10. Как связаны вероятность ложной тревоги α и вероятность пропуска β с выбором порога детектирования?

11. Что характеризует площадь под ROC–кривой (AUC)? Какое значение соответствует идеальному и случайному детектору?

12. Как формула Байеса используется при принятии решения об атаке? Как стоимость ошибок влияет на выбор порога?

13. Какие преимущества даёт гибридный подход? В чём его возможные недостатки?

14. Почему в условиях сильного дисбаланса классов Accuracy может быть неинформативной? Какие альтернативы предпочтительны?

15. Чем отличается сетевой уровень обнаружения атак от хостового и прикладного?

Практическое занятие № 2. Использование методов вычислительного интеллекта для анализа компьютерных атак

Общие сведения

Цель: сформировать навыки применения методов вычислительного интеллекта (нейронных сетей, нечёткой логики, методов опорных векторов, ансамблей деревьев решений) для решения задачи классификации и распознавания компьютерных атак; приобрести навыки построения, обучения и количественной оценки моделей классификаторов сетевого трафика.

Перечень знаний и умений для достижения цели:

Знать: принципы работы искусственных нейронных сетей, метода опорных векторов (SVM) и ансамблевых методов (RandomForest); понятие информационного выигрыша (InformationGain) и кросс-валидации.

Литература: [9] Bishop M.ComputerSecurity: ArtandScience (применение машинного обучения в безопасности); [12] Ю. М. Краковский.

Уметь: выполнять предобработку данных (нормализация, one-hotencoding); обучать модели классификации на наборах данных (NSL-KDD/CICIDS2017); оценивать устойчивость модели с помощью k-блочной кросс-валидации.

Литература: [9] M. Bishop.; [8] W. Stallings (основы анализа сетевых данных).

Материалы, оборудование, программное обеспечение: ПК с ОС KaliLinux или Ubuntu, интерпретатор Python 3 с библиотеками NumPy, SciPy, Pandas, Matplotlib, scikit–learn, TensorFlow; набор данных NSL–KDD (или CICIDS2017); стендовый полигон; средства виртуализации.

1. Методический материал к выполнению заданий

Методы вычислительного интеллекта применяются в задачах анализа компьютерных атак, когда классические сигнатурные подходы оказываются недостаточными – например, для выявления ранее неизвестных атак, обнаружения скрытых закономерностей в больших объёмах сетевого трафика или автоматической классификации сценариев нарушителя. К методам вычислительного интеллекта относят искусственные нейронные сети, нечёткую логику, эволюционные (генетические) алгоритмы, а также более широкие семейства методов машинного обучения – методы опорных векторов (SVM), деревья решений, ансамбли (RandomForest, GradientBoosting), алгоритмы кластеризации (k–means, DBSCAN) и оценки плотности.

Нейросетевой подход к обнаружению атак

Искусственная нейронная сеть прямого распространения представляет собой композицию простых пороговых элементов (нейронов), каждый из которых формирует взвешенную сумму входов и применяет к ней нелинейную функцию активации. Выход j-го нейрона вычисляется по формуле:

$$y_j = \varphi(\Sigma(w_{ij} \cdot x_i) + b_j), \quad (2.1)$$

где w_{ij} – вес связи, b_j – смещение, φ – функция активации (сигмоидальная, ReLU, гиперболический тангенс). Обучение производится на размеченной выборке с использованием алгоритма обратного распространения ошибки, минимизирующего функцию потерь:

$$L = -\Sigma[y \cdot log(\hat{y}) + (1-y) \cdot log(1-\hat{y})], \qquad (2.2)$$

где y – истинная метка; ŷ – предсказанная вероятность класса атаки.

Метод опорных векторов и ансамбли

Метод опорных векторов (SVM) строит разделяющую гиперплоскость, максимизирующую зазор между классами. В случае линейно неразделимых данных применяется ядровое преобразование $K(x_i, x_j)$ – радиальная базисная функция (RBF), полиномиальное ядро, сигмоидальное ядро. Ансамбли (RandomForest, GradientBoosting) объединяют m деревьев решений; итоговое предсказание определяется голосованием (для классификации) или усреднением (для регрессии). Случайный лес обладает пониженной дисперсией по сравнению с отдельным деревом, а градиентный бустинг последовательно корректирует ошибки предыдущих моделей.

Методы аномалий и оценка качества.

Для обучения без учителя применяются алгоритмы выявления аномалий: IsolationForest, One–Class SVM, автокодировщики. Изолирующий лес строит множество деревьев случайного разбиения; аномалии изолируются за меньшее число шагов, что даёт численный показатель аномальности – anomalyscore в диапазоне [0, 1]. Оценка качества классификации производится по уже введённым метрикам (1.1–1.4), а также с использованием кросс–валидации: выборка разбивается на k блоков, модель обучается на k–1 блоке и тестируется на оставшемся; процесс повторяется k раз, результаты усредняются. Для оценки неопределённости строится доверительный интервал среднего значения метрики.

Важной характеристикой является информативность признаков. Информационный выигрыш (informationgain) признака A относительно целевой переменной C вычисляется как уменьшение энтропии Шеннона:

$$IG(A) = H(C) - \Sigma\big(\vee Cv \vee\vee C \vee \cdot H(Cv)\big), \qquad (2.3)$$

где $H(C) = -\Sigma p_i \cdot log2(p_i)$ – энтропия целевой переменной, а суммирование по v – по значениям признака A. Признаки с наибольшим IG включаются в модель.

2. Методические указания к практическому занятию и порядок выполнения заданий. Задания

Задания 1

1. Установить и настроить рабочее окружение: Python 3, библиотеки scikit–learn, NumPy, Pandas, Matplotlib; загрузить набор данных NSL–KDD, разделить выборку на обучающую (70 %) и тестовую (30 %).

2. Выполнить предварительную обработку данных: нормализовать числовые признаки по формуле (2.4), закодировать категориальные признаки (protocol_type, service, flag) методом one–hot.

3. Обучить классификатор атак – многослойный перцептрон с тремя слоями (ReLU–активация) и метод опорных векторов с RBF–ядром; построить матрицу ошибок на тестовой выборке.

4. Рассчитать метрики качества классификации (Accuracy, Precision, Recall, F1, AUC ROC) по формулам (1.1)–(1.4) и сравнить с табличными значениями из таблицы 2.1; результаты представить в виде отдельной таблицы.

5. Применить 5-блочную кросс-валидацию; рассчитать выборочное среднее и 95%-ный доверительный интервал для F1–меры; сделать вывод об устойчивости модели.

6. Рассчитать информационный выигрыш IG(A) для всех 41 признака по формуле (2.3); отобрать 10 наиболее информативных признаков и переобучить модель; сравнить F1 до и после отбора.

7. Применить алгоритм IsolationForest ($n_{estimators} = 100$) для обнаружения аномалий; построить распределение anomalyscore для нормального трафика и атак; определить порог, при котором $FPR \leq 0{,}05$, и рассчитать соответствующий Recall.

8. Сравнить полученные результаты с показателями сигнатурного метода (из практического занятия № 1) и сформулировать выводы о применимости методов вычислительного интеллекта для анализа компьютерных атак; указать, при каких условиях каждый подход имеет преимущество. Рассмотри возможность использования АПКШ «Континент» или др., DLP-систем (на примере DLP SecureTower), системы защиты информации (СЗИ Dallas Lock и др.) для процессов анализа компьютерных атак.

Задания 2

1. Рассмотрите задачу классификации сетевых соединений. Обучающая выборка содержит 5000 нормальных и 1200 атакующих соединений. Постройте модель логистической регрессии. Запишите выражение для градиента функции потерь. Выполните не менее 20 итераций градиентного спуска с шагом $\eta = 0{,}01$. Приведите динамику L(w). Оцените Precision и Recall.

2. Сформулируйте задачу отбора подмножества из 15 признаков с помощью генетического алгоритма. Закодируйте хромосому как битовую строку длины 15. Предложите функцию приспособленности с учётом F1–score и штрафа за число признаков. Опишите операторы скрещивания и мутации ($pm = 0{,}05$).

3. Для набора из 200 точек в двумерном пространстве признаков выполните кластеризацию k–means при $K = 3$. Рассчитайте J и средний индекс силуэта. Сравните с $K = 2$ и $K = 4$.

4. Сравните вычислительную сложность шага градиентного спуска и генерации генетического алгоритма. При каких соотношениях параметров ГА предпочтительнее или дороже?

5. Предложите архитектуру нейронной сети для многоклассовой классификации типов атак (DoS, Probe, R2L, U2R, Normal). Запишите softmax и категориальную кросс–энтропию. Укажите методы регуляризации.

Примечание. Для заданий 1 и 3 удобно использовать scikit–learn. При реализации градиентного спуска «вручную» контролируйте численную устойчивость. Для задания 2 достаточно математической постановки и псевдокода

В рамках занятия студент реализует на Python классификатор атак на наборе данных NSL–KDD (или CICIDS2017), проводит обучение и оценку качества, а также анализ информативности признаков.

NSL–KDD содержит 41 признак (длительность соединения, протокол, число байтов, число неудачных попыток входа и т. п.) и 5 классов (Normal, DoS, Probe, R2L, U2R). Перед обучением признаки нормализуются:

$$x' = (x - \mu)/\sigma, \tag{2.4}$$

где μ – выборочное среднее; σ – стандартное отклонение. Категориальные признаки кодируются методом one–hot. Выборка разделяется на обучающую (70 %) и тестовую (30 %).

Таблица 2.1 – Ожидаемые метрики моделей классификации на NSL–KDD

Модель	**Accuracy**	**Precision**	**Recall**	**F1**	**AUC ROC**
Логистичес-кая регрессия	0,81	0,78	0,76	0,77	0,87
SVM (RBF–ядро)	0,83	0,82	0,79	0,80	0,90
Случайный лес	0,86	0,85	0,83	0,84	0,93
Градиентный бустинг	0,88	0,87	0,85	0,86	0,94
Нейросеть (3 слоя, ReLU)	0,89	0,88	0,86	0,87	0,95

Качество модели оценивается путём построения матрицы ошибок и расчёта метрик по формулам (1.1–1.4). Для устойчивости результатов применяется k–блочная кросс–валидация (k = 5 или 10).

Требования к отчёту и защите

Защита предполагает опрос по материалу, изложенному в отчёте. Отчёт должен быть оформлен: требуется наличие титульного листа, указание цели практического занятия, последовательное изложение выполненных расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания. Проверяется знание теоретического материала с учётом ответов на контрольные вопросы. Задаются вопросы по пунктам, приведённым в разделе «Порядок выполнения работы». Критерии к оценке защиты отчёта студентом приведены в таблице 9.1.

Контрольные вопросы для самопроверки

1. Что такое вычислительный интеллект? Какие семейства методов он включает?
2. Опишите устройство искусственного нейрона и запишите формулу (2.1) для его выхода.
3. Что такое функция потерь и как она используется при обучении нейронной сети? Запишите формулу (2.2).
4. Чем обучение с учителем отличается от обучения без учителя применительно к задаче обнаружения атак?
5. Опишите принцип метода опорных векторов и назначение ядерных функций.
6. Запишите формулы для расчёта Precision, Recall, F1 и AUC ROC; поясните их смысл.
7. Что такое k–блочная кросс–валидация и для чего она применяется?
8. Что такое информационный выигрыш признака? Запишите формулу (2.3).
9. Какие недостатки имеют методы вычислительного интеллекта при построении СПКА?

Практическое занятие № 3. Специфика анализа атак как процессов реализации угроз

Общие сведения

Цель: сформировать навыки решения типовых и прикладных задач в области анализа компьютерных атак как процессов реализации угроз; приобрести навыки построения деревьев атак, описания сценариев на основе фреймворков CyberKillChain и MITRE ATT&CK, параметризации атак в терминах методики Климова, а также количественной оценки риска как произведения вероятности реализации угрозы на величину ущерба.

Перечень знаний и умений для достижения цели:

Знать: концепции CyberKillChain и фреймворка MITRE ATT&CK; структуру дерева атак с логическими операциями AND/OR; базовые формулы расчёта риска и среднего времени компрометации (MTTC).

Литература: [7] С. М. Климов и др. (моделирование процессов реализации угроз); [11] Е. В. Дойникова (оценивание защищённости); [6] MITRE ATT&CKFramework.

Уметь: строить формализованные деревья атак; сопоставлять этапы сценария с тактиками и техниками MITRE ATT&CK; рассчитывать сквозную вероятность обнаружения и уровень риска сценария.

Литература: [7] С. М. Климов и др.; [6] MITRE ATT&CKFramework.

Материалы, оборудование, программное обеспечение: ПК с ОС KaliLinux, средства построения графов (draw.io, LibreOfficeDraw, либо Python + networkx), анализатор трафика Wireshark, журнал СОА Suricata, платформа MITRE ATT&CK Navigator, стендовый полигон с АРМ имитатора атак и защищаемого сегмента.

1. Методический материал к выполнению заданий

Анализ компьютерных атак как процессов реализации угроз предполагает рассмотрение атаки не как единичного события, а как временной последовательности состояний и событий, разворачивающейся на интервале выполнения технологического цикла управления (ТЦУ) в ИС. Согласно методике Климова, динамика реализации атаки описывается цепочкой состояний $S0 \rightarrow S1 \rightarrow \ldots \rightarrow Sr$ (штатное функционирование) и $Y_{A0} \rightarrow Y_{Ai} \rightarrow Y_{Ai+1}$ (воздействие атаки), при этом события атаки протекают параллельно с процессами сбора, обработки и передачи информации. Противодействие описывается параметрами $z_{ПД1}$, …, $z_{ПД(j+n)}$, характеризующими применение средств защиты на различных рубежах.

В теории марковских процессов принятия решений компьютерная атака рассматривается как процесс последовательного или параллельного выполнения этапов: разведка, проникновение, закрепление, развитие, воздействие, сокрытие следов. Конечный автомат атаки задаётся пятёркой $(Q, \Sigma, \delta, q_0, F)$. Сеть Петри $N = (P, T, P_{re}, P_{os}t, M_0)$ позволяет моделировать параллелизм и синхронизацию.

Марковская цепь с дискретным временем: $p(n+1) = p(n)\ P$. Стационарное распределение $\pi = \pi^*P$, $\Sigma\ \pi_i = 1$. Для непрерывного времени используется генератор Q: $dp/dt = p^*Q$. Время пребывания в состоянии i имеет экспоненциальное распределение с параметром $-\ q_{ii}$. Вероятность успешной реализации атаки за время T – вероятность достижения поглощающего состояния «успех».

Анализ позволяет выявлять критические этапы, на которых воздействие средств защиты даёт максимальный эффект. Вычисляют вероятности прохождения через состояния, средние времена пребывания и чувствительность итоговой вероятности успеха к изменению интенсивностей переходов.

Модель угрозы и модель нарушителя

Угроза безопасности информации представляет собой возможную причину нарушения конфиденциальности, целостности или доступности информации в ИС (триада CIA). Реализация угрозы через конкретный сценарий действий нарушителя образует компьютерную атаку. Модель нарушителя содержит описание целей, мотивации, уровня подготовки, доступных ресурсов и возможных способов действия нарушителя. Модель угрозы представляет собой совокупность сценариев, направленных на эксплуатацию отдельных уязвимостей ИС. Базовая модель риска описывается соотношением:

$$R = P \cdot U, \tag{3.1}$$

где R – уровень риска, P – вероятность реализации угрозы за рассматриваемый период, U – величина ожидаемого ущерба. При реализации нескольких угроз одновременно общий риск вычисляется с учётом их взаимного влияния и возможной ковариации.

Деревья атак и CyberKillChain

Дерево атак – иерархическая структура, в корне которого находится цель атаки (например, нарушение конфиденциальности базы данных), а листьями являются элементарные действия нарушителя. Узлы дерева объединяются логическими операциями: AND (все дочерние действия должны быть выполнены) и OR (достаточно одного). Вероятность реализации корневого события для AND–узла равна произведению вероятностей дочерних узлов, для OR–узла – дополнению до единицы произведения дополнений:

$$P = \prod P_i;\ P = 1 - \prod(1 - P_i). \tag{3.2}$$

Связанной моделью является концепция CyberKillChain, описывающая типовые этапы атаки: рекогносцировка (reconnaissance), подготовка оружия (weaponization), доставка (delivery), эксплуатация (exploitation), установка (installation), командование и контроль (command and control), целевые действия (actions on objectives). Каждый этап может быть обнаружен соответствующими датчиками СПКА с вероятностью p_i; сквозная вероятность обнаружения атаки вычисляется как дополнение до единицы вероятности пропуска на всех этапах.

Фреймворк MITRE ATT&CK

Фреймворк MITRE ATT&CK классифицирует тактики (T) и техники (T) атакующих, образуя матрицу из 14 тактик (Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact, Resource Development, Reconnaissance) и более чем 600 техник. Сопоставление журнала COA с матрицей ATT&CK позволяет оценить покрытие защитных средств и вычислить долю обнаруживаемых техник. Среднее время компрометации (Mean Time To Compromise, MTTC) вычисляется по формуле:

$$MTTC = \Sigma(t_i \cdot p_i)/\Sigma\, p_i \qquad (3.3)$$

где t_i – время реализации i-го этапа, p_i – вероятность его успешного выполнения. Показатель MTTC используется для ранжирования сценариев нарушителя и обоснования приоритетов защиты.

2. Методические указания к практическому занятию и порядок выполнения заданий. Задания

Задание 1

1. Постройте конечный автомат для атаки «фишинг → установка вредоносного ПО → эксфильтрация данных». Определите Q, Σ, δ, F. Укажите переходы успеха и блокировки. Приведите диаграмму.

2. Представьте атаку сетью Петри. Введите позиции и переходы. Задайте начальную разметку. Постройте дерево достижимости. Укажите тупиковые разметки и разметки успеха.

3. Марковская модель: S_0 (начальное), S_1 (разведка), S_2 (проникновение), S3 (успех), S4 (обнаружено). Интенсивности: q_{01}=0,5; q_{12}=0,3; q_{23}=0,4; q_{14}=0,2; q_{24}=0,25. Составьте Q. Найдите вероятности при t=5 ч. Вычислите вероятность достижения S_3 к t=10 ч.

4. Введите восстановление из S_4 в S_0 с интенсивностью 0,1. Как изменится процесс? Вычислите стационарные вероятности или среднее время до S3.

5. Сформулируйте критерий критичности этапа (вероятность прохождения, уменьшение вероятности успеха при отключении, среднее время). Рассчитайте для S_1 и S_2.

Задание 2

1. Выбрать компьютерную атаку из открытого реестра (сканирование сети, подбор паролей по SSH, эксплуатация уязвимости веб–приложения, DDoS–атака, фишинг с эксплуатацией макросов) и описать её как процесс реализации конкретной угрозы при использовании в инфраструктуре АПКШ «Континент»

или др., DLP-систем (на примере DLP SecureTower), системы защиты информации (СЗИ Dallas Lock и др.)

2. Построить дерево атак для выбранного сценария с указанием логических операций AND/OR; для каждого листа экспертно оценить вероятность (в диапазоне 0,1–0,9) и по формуле (3.2) рассчитать вероятность корневого события.

3. Сопоставить этапы сценария с этапами CyberKillChain; для каждого этапа указать датчик СПКА, способный его обнаружить, и присвоить значение p_i по таблице 3.1 (или обоснованно его скорректировать).

4. По формуле (3.4) рассчитать сквозную вероятность пропуска атаки и соответствующую вероятность обнаружения; проанализировать, как изменится результат при удалении двух любых датчиков.

5. Отобразить сценарий на матрицу MITRE ATT&CK с использованием ATT&CK Navigator; рассчитать долю охваченных тактик и техник; определить этапы, на которых охват ниже 50 %.

6. Заполнить формализованное описание (паспорт) процесса реализации угрозы в обозначениях Климова: BY_i, $\xi_{воз.\ уяз}$, S_i, Y_i, τ_i, $Z_ПД_i$; по формуле (3.3) рассчитать MTTC для сценария.

7. По формуле (3.1) рассчитать уровень риска $R = P \cdot U$ для выбранного сценария, приняв вероятность P из дерева атак (пункт 2), а ущерб U – экспертно в денежном выражении; сравнить с типичными порогами (низкий $< 10^5$ руб., средний 10^5–10^6, высокий $> 10^6$).

8. Провести тестовую реализацию выбранной атаки на стендовом полигоне (в учебном сегменте ЛВС), собрать журналы датчиков и сопоставить фактические события с разработанным формализованным описанием; сделать выводы об адекватности модели.

В рамках занятия студент выбирает типовой сценарий атаки, строит его формализованное описание в виде дерева атак, отображает этапы на CyberKillChain и MITRE ATT&CK, а также рассчитывает количественные показатели риска.

Таблица 3.1 – Вероятности обнаружения атак по этапам killchain

Этап killchain	**Датчик СПКА**	**Вероятность обнаружения p_i**
Reconnaissance	NIDS (Zeek)	0,70
Weaponization	Антивирус (ClamAV)	0,40
Delivery	WAF (ModSecurity)	0,85
Exploitation	HIDS (OSSEC)	0,60
Installation	HIDS (Sysmon)	0,50

Этап killchain	Датчик СПКА	Вероятность обнаружения p_i
Command&Control	NIDS (Suricata)	0,75
Actionsonobjectives	SIEM (Splunk)	0,80

Сквозная вероятность пропуска атаки (т. е. вероятность того, что ни один датчик не сработает) рассчитывается по формуле:

$$P\text{проп} = \prod(1 - p_i) \quad (3.4)$$

Сквозная вероятность обнаружения, следовательно, равна $P_{обн} = 1 – P_{проп}$. Для данных таблицы 3.1 это значение составит примерно 0,99966 (четыре девятки). Однако при корреляции датчиков (например, зависимость HIDS и SIEM от одной журнальной базы) фактическое значение может быть значительно ниже.

Требования к отчёту и защите

Защита предполагает опрос по материалу, изложенному в отчёте. Отчёт должен быть оформлен: требуется наличие титульного листа, указание цели практического занятия, последовательное изложение выполненных расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания. Проверяется знание теоретического материала с учётом ответов на контрольные вопросы. Задаются вопросы по пунктам, приведённым в разделе «Порядок выполнения работы». Критерии к оценке защиты отчёта студентом приведены в таблице 9.1.

Контрольные вопросы для самопроверки

1. В чём заключается специфика анализа атак как процессов реализации угроз?
2. Что такое модель угрозы и модель нарушителя? Какие элементы они включают?
3. Опишите структуру дерева атак и логические операции AND/OR; запишите формулы (3.2) для расчёта вероятностей.
4. Перечислите этапы CyberKillChain и укажите, какие датчики СПКА могут обнаруживать каждый из них.
5. Что такое фреймворк MITRE ATT&CK и какие тактики в нём выделяются?
6. Запишите формулы (3.1) для риска и (3.3) для среднего времени компрометации (MTTC).

7. Какие параметры использует методика Климова для описания процесса реализации угрозы?

8. Как влияет корреляция датчиков на фактическую сквозную вероятность обнаружения атаки?

9. Чем сеть Петри удобнее конечного автомата при моделировании атак?

10. Как строится матрица генератора непрерывной марковской цепи?

11. Что такое поглощающее состояние и как оно используется в моделях атак?

12. Как вычислить среднее время до успешной реализации атаки?

13. Какие ограничения имеет марковская модель?

14. Что такое дерево достижимости сети Петри?

15. Как использовать анализ чувствительности интенсивностей при выборе мер защиты?

Практическое занятие № 4. Аналитическое моделирование процессов реализации угроз

Общие сведения

Цель: сформировать навыки решения типовых и прикладных задач в области применения аналитического моделирования процессов реализации угроз на основе дифференциальных уравнений динамики атак и противодействия; приобрести практические навыки численного решения системы уравнений методом Эйлера, расчёта коэффициента противодействия компьютерным атакам $K_{ПКА}(t)$ и анализа его чувствительности к параметрам λY, λПКА, τЗ, δπП.

Перечень знаний и умений для достижения цели:

Знать: аналитические модели динамики атак (адаптация моделей Ланчестера, SIR-модели); понятие коэффициента противодействия КПКА(t)КПКА(t) и критическое влияние запаздывания обнаружения (τЗ).

Литература: [7] С. М. Климов и др. (аналитическое моделирование); [11] Е. В. Дойникова (модели управления кибербезопасностью); [10] R. Anderson. SecurityEngineering (системная динамика угроз).

Уметь: численно решать системы дифференциальных уравнений методом Эйлера; строить графики зависимостей $K_{ПКА}(t)$ при различных параметрах; проводить анализ чувствительности модели.

Литература: [7] С. М. Климов и др.

Материалы, оборудование, программное обеспечение: ПК с установленными средствами вычислений (Python 3 с NumPy, SciPy, Matplotlib; либо LibreOfficeCalc), справочные данные по типовым значениям

интенсивностей атак и противодействия, методические материалы монографии Климова С.М.

1. Методический материал к выполнению заданий

Аналитическое моделирование процессов реализации угроз предполагает описание динамики взаимодействия нарушителя и средств противодействия атакам с помощью дифференциальных или разностных уравнений. В методике Климова для аналитического описания процессов противодействия компьютерным атакам используются модели типа моделей Ланчестера, адаптированные к информационному противоборству. Переменными модели выступают относительное количество преодолённых рубежей противодействия x(t) и относительное число атак, доведённых нарушителем до определённого этапа, y(t).

Аналитические модели позволяют получить замкнутые выражения либо качественные характеристики процессов реализации угроз. Классическая SIR–модель: $dS/dt = -\beta SI$, $dI/dt = \beta SI - \gamma I$, $dR/dt = \gamma I$. Базовое репродуктивное число $R0 = \beta/\gamma$. При $R0 > 1$ возникает эпидемия.

Для DDoS применяют модели массового обслуживания. Система M/M/1: $\rho = \lambda/\mu$, $L = \rho/(1-\rho)$, $W = 1/(\mu-\lambda)$. При $\rho \to 1$ время ответа стремится к бесконечности. Аналитическое моделирование даёт возможность исследовать устойчивость равновесий, бифуркации и чувствительность к параметрам.

При переходе к реалистичным моделям учитывают неоднородность узлов, топологию, адаптивное поведение атакующего и запаздывание реакции защиты, что приводит к уравнениям с запаздыванием и моделям на графах.

Дифференциальные уравнения динамики атак

Динамика атаки и противодействия описывается системой уравнений, в которой скорость изменения x(t) пропорциональна интенсивности воздействия атак λY, а скорость изменения y(t) – интенсивности противодействия λПКА. Параметр λY характеризует среднее число атак, проводимых нарушителем за единицу времени, параметр λПКА – среднее число успешно нейтрализованных атак за ту же единицу времени. Решение системы при начальных условиях x(0) = 1 (все рубежи целы) и y(0) = 0 даёт аналитическое выражение для коэффициента противодействия $K_{\text{ПКА}}(t)$:

$$K_{\text{ПКА}}(t) = 1 - \lambda Y \cdot t + 0{,}5 \cdot \lambda Y \cdot \lambda\text{ПКА} \cdot \delta\pi\text{П} \cdot t^2 \qquad (4.1)$$

где δπП – относительное количество средств противодействия, приходящихся на один рубеж $C_{\text{ПКА}}$. Эта формула позволяет вычислять коэффициент противодействия для случая, когда одной атаке с интенсивностью λY противодействует один рубеж $C_{\text{ПКА}}$ с интенсивностью λПКА.

Учёт запаздывания обнаружения

Реальные системы обнаружения атак всегда имеют запаздывание τЗ, обусловленное временем анализа, корреляции и принятия решения. С учётом этого запаздывания формула принимает вид:

$$K_{\text{ПКА}}(t) = 1 - \lambda Y \cdot t + 0{,}5 \cdot \lambda Y \cdot \lambda\text{ПКА} \cdot \delta\pi\text{П} \cdot (t - \tau\text{З})^2 \qquad (4.2)$$

Анализ этой зависимости показывает, что при $0 \le t \le \tau$З противодействие отсутствует (πП = 0) и атака развивается беспрепятственно; начиная с момента t = τЗ, противодействие включается и $K_{\text{ПКА}}(t)$ начинает возрастать. Величина τЗ, таким образом, является критическим параметром, определяющим эффективность $C_{\text{ПКА}}$: при малых τЗ нарушитель не успевает преодолеть даже один рубеж противодействия, а при больших τЗ атака может успешно продвинуться на несколько рубежей.

Влияние числа рубежей

Аналитическая модель также позволяет оценить влияние числа рубежей противодействия. При использовании семи рубежей СПКА параметр δπП меняется с дискретностью 1/7 в интервале от 1 до 0. Анализ показывает, что уменьшение числа рубежей (с 7 до 5 или до 3) приводит к возрастанию числа обнаруженных атак y(t), но относительное число непреодолённых рубежей x(t) при этом уменьшается: x3(t=5) < x7(t=5). Это демонстрирует необходимость противодействия атакам на семи рубежах СПКА.

Численное решение методом Эйлера

Для сложных систем уравнений, не допускающих аналитического решения, применяется численное интегрирование методом Эйлера. Итерационная формула для системы уравнений dx/dt = f(t, x, y), dy/dt = g(t, x, y) имеет вид:

$$x_{n+1} = x_n + h \cdot f(t_n, x_n, y_n); y_{n+1} = y_n + h \cdot g(t_n, x_n, y_n) \qquad (4.3)$$

где h – шаг интегрирования. Для устойчивости шаг выбирается из условия $h \le 1 / (2 \cdot \max|\lambda Y, \lambda\text{ПКА}|)$. Чувствительность $K_{\text{ПКА}}(t)$ к изменению параметра α вычисляется как частная производная $\partial K/\partial\alpha$, а её относительное значение $\partial K/K : \partial\alpha/\alpha$ характеризует эластичность модели по данному параметру.

2. Порядок выполнения работы

Задание 1

1. Для SIR с β=0,4; γ=0,15; S(0)=0,99; I(0)=0,01 найдите R0. Проинтегрируйте на [0,50]. Определите tmax и Imax. Оцените R(∞). Постройте графики.

2. Введите патчинг с интенсивностью ν. Исследуйте Imax при ν=0,05; 0,10; 0,20. Постройте Imax(ν).

3. Сервер: λ_l=50 с−1, 1/μ=0,01 с. Найдите λ_a* при ρ≥0,95. Постройте W(λ_a).

4. Модифицируйте модель с фильтрацией атакующих пакетов с вероятностью p_f. Найдите минимальный p_f для устойчивости при λ_a=80 с−1.

5. Сформулируйте задачу оптимального управления ν(t) с ограничением затрат и критерием min ∫I(t)dt. Запишите гамильтониан Понтрягина.

Задание 2.

1. Изучить аналитические модели динамики атак и противодействия по методике Климова; записать исходные формулы (4.1) и (4.2) для K_ПКА(t) без учёта и с учётом запаздывания τЗ.

2. Используя Python (NumPy, Matplotlib) или LibreOfficeCalc, построить таблицу значений K_ПКА(t) на интервале t ∈ [0, 10] с шагом h = 0,5 при параметрах из таблицы 4.1: λY = 0,1; λПКА = 0,3; δπП = 1,0; τЗ = 0,5.

3. Построить семейство графиков $K_{\text{ПКА}}(t)$при различных значениях τЗ (0; 0,5; 1; 2) и проанализировать влияние запаздывания обнаружения на эффективность противодействия; определить t*, при котором $K_{\text{ПКА}}(t^*) = 0{,}5$ для каждого τЗ.

4. Построить зависимость $K_{\text{ПКА}}(t)$при числе рубежей противодействия n = 7, 5 и 3; для каждого случая рассчитать δπП = 1/n; объяснить различия с точки зрения методики Климова; рассчитать площадь под кривой $K_{\text{ПКА}}(t)$на интервале [0, 10].

5. Численно решить систему дифференциальных уравнений методом Эйлера по формуле (4.3) с шагом h = 0,1; сравнить результат с аналитическим решением (4.2); оценить относительную погрешность $\delta K = |K_{\text{аналит}} - K_{\text{числ}}| / K_{\text{аналит}}$.

6. Рассчитать чувствительность S_α по формуле (4.4) для параметров λY, λПКА, τЗ, δπП при типовых значениях; составить таблицу чувствительностей; выделить критические параметры ($|S_\alpha| > 1$).

7. Сформулировать выводы о критических параметрах, определяющих эффективность противодействия, и предложить конкретные меры по их улучшению для типовой ИС: уменьшение τЗ за счёт корреляции событий в SIEM, повышение λПКА за счёт расширения базы сигнатур и т. п.

В рамках занятия студент численно решает систему дифференциальных уравнений динамики атак и противодействия методом Эйлера, а также строит семейство кривых $K_{\text{ПКА}}(t)$ при различных значениях параметров.

Таблица 4.1 – Типовые параметры аналитической модели противодействия

Параметр	Обозначение	Типовое значение	Размерность
Интенсивность атак	λY	0,10	1/ед. времени
Интенсивность противодействия	λПКА	0,30	1/ед. времени
Относит. число СПКА на рубеж	δπП	1,0	—
Запаздывание обнаружения	τЗ	0,5	ед. времени
Число рубежей	n	7	—

Чувствительность коэффициента противодействия к изменению параметра α рассчитывается по формуле:

$$S\alpha = (\alpha / K_{\text{ПКА}}(t)) \cdot (\partial K_{\text{ПКА}}(t) / \partial \alpha) \qquad (4.4)$$

При |Sα| > 1 параметр считается критическим – малое изменение вызывает большее относительное изменение K_ПКА. По результатам расчётов строится таблица чувствительностей для всех параметров модели.

Требования к отчёту и защите

Защита предполагает опрос по материалу, изложенному в отчёте. Отчёт должен быть оформлен: требуется наличие титульного листа, указание цели практического занятия, последовательное изложение выполненных расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания. Проверяется знание теоретического материала с учётом ответов на контрольные вопросы. Задаются вопросы по пунктам, приведённым в разделе «Порядок выполнения работы». Критерии к оценке защиты отчёта студентом приведены в таблице 9.1.

Контрольные вопросы для самопроверки

1. На чём основано аналитическое моделирование процессов реализации угроз по методике Климова?

2. Запишите формулу (4.1) для коэффициента противодействия $K_{\text{ПКА}}(t)$(t) без учёта запаздывания.

3. Как влияет запаздывание обнаружения τЗ на вид зависимости K_ПКА(t)? Запишите формулу (4.2).

4. Какое практическое значение имеет параметр δπП (относительное число средств противодействия на один рубеж)?

5. Как число рубежей противодействия (3, 5, 7) влияет на эффективность защиты ИС?

6. Опишите численный метод Эйлера для решения системы дифференциальных уравнений; запишите формулу (4.3).

7. Как рассчитывается чувствительность коэффициента противодействия к параметру по формуле (4.4)?

8. Какие меры можно предложить для уменьшения τЗ и повышения λПКА в реальной СПКА?

9. Что означает $R_0 > 1$ в модели распространения вредоносного ПО?

10. Каковы основные предположения SIR–модели?

11. Как связана интенсивность заявок с отказом в обслуживании в M/M/1?

12. В чём идея принципа максимума Понтрягина применительно к управлению распространением ВПО?

13. Какие модели адекватны для атак на целостность данных?

14. Как топология сети влияет на скорость распространения червя?

15. Что такое положение равновесия и как исследуется его устойчивость?

Практическое занятие № 5. Методика анализа и регулирования рисков при реализации нескольких угроз

Общие сведения

Цель: сформировать навыки решения типовых и прикладных задач в области применения анализа и регулирования рисков, возникающих при реализации нескольких угроз безопасности информации; приобрести навыки построения матрицы рисков, расчёта ожидаемых годовых потерь (ALE), обоснования мер регулирования и количественной оценки остаточного риска с использованием весовых коэффициентов методики Климова.

Перечень знаний и умений для достижения цели:

Знать: количественные показатели риска (SLE, ARO, ALE); методологии оценки рисков (NIST SP 800-30, FAIR); модель регулирования устойчивости по Климову с использованием весовых коэффициентов $\alpha\Pi j$ и βCi.

Литература: [11] Е. В. Дойникова; [4] NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments; [7] С. М. Климов и др.

Уметь: строить матрицу рисков 5×5 и определять приоритеты обработки; рассчитывать экономическую эффективность контрмер ($E>0$); применять модель FAIR для оценки частоты и магнитуды потерь.

Литература: [4] NIST SP 800-30 Rev. 1; [11] Е. В. Дойникова.

Материалы, оборудование, программное обеспечение: ПК с табличным процессором (LibreOfficeCalc или MicrosoftExcel), справочные материалы по методикам оценки рисков (NIST SP 800–30, ISO/IEC 27005, FAIR, OCTAVE), методические материалы по методике Климова, перечни типовых угроз.

1. Методический материал к выполнению заданий

Риск нарушения информационной безопасности определяется как функция от вероятности реализации угрозы и величины потенциального ущерба. Базовая модель риска описывается соотношением (3.1): R = P · U, где R – уровень риска, P – вероятность реализации угрозы за рассматриваемый период, U – величина ожидаемого ущерба. При реализации нескольких угроз одновременно общий риск вычисляется с учётом их взаимного влияния и возможной ковариации. Регулирование риска заключается в выборе мер защиты, снижающих вероятность P или ущерб U до приемлемого уровня, при котором остаточный риск не превышает заданного порога.

Количественные показатели риска

В количественной модели риска используются следующие показатели. Единичная потеря (SingleLossExpectancy, SLE) – ущерб от одной реализации угрозы; годовая частота реализации (AnnualizedRateofOccurrence, ARO) – ожидаемое число реализаций за год; ожидаемые годовые потери (AnnualizedLossExpectancy, ALE) рассчитываются по формуле:

$$ALE = SLE \cdot ARO \tag{5.1}$$

После внедрения контрмеры стоимость которой составляет C_к, остаточные годовые потери составят ALE_ост = SLE_ост · ARO_ост, а экономическая эффективность контрмеры – разность:

$$E = (ALE - ALE_{\text{ост}}) - C\text{к} \tag{5.2}$$

Контрольная мера считается экономически оправданной при E > 0; в противном случае её применение нецелесообразно с финансовой точки зрения.

Методики оценки рисков

На практике применяется ряд формализованных методик оценки рисков: NIST SP 800–30 (США), OCTAVE (CarnegieMellon), FAIR (FairStandardsInstitute), методика ФСТЭК России, а также методики, основанные на стандарте ISO/IEC 27005. Все они опирают на общую последовательность шагов: идентификация активов и их критичности, выявление угроз и уязвимостей, оценка вероятностей и ущербов, расчёт рисков, выбор мер обработки. Различия состоят в степени формализации, шкалах измерения и форме представления результатов.

Матрица рисков

Матрица рисков представляет собой таблицу, по строкам которой откладываются уровни вероятности (например, низкая, средняя, высокая, критическая), а по столбцам – уровни ущерба. На пересечении указывается уровень риска от 1 до 25 или по категориям «низкий», «средний», «высокий», «критический». Матрица позволяет наглядно сопоставлять угрозы по их значимости и выбирать приоритеты обработки. Для каждой клетки матрицы определяются типовые меры регулирования: принятие (для низкого риска), снижение (для среднего и высокого), передача (через страхование) или избегание (отказ от технологии).

Регулирование по Климову

В методике Климова регулирование устойчивости функционирования ИС в условиях нескольких угроз осуществляется с использованием весовых коэффициентов. Повышение устойчивости описывается суммой произведений вероятности устойчивости функционирования РУФ и весовых коэффициентов α_Пj, характеризующих отдельные средства регулирования: настройку СПКА, регулирование СЗИ от несанкционированного доступа, динамическую настройку параметров ИС, устранение уязвимостей, полноту исходных данных об информационных акциях нарушителя. Снижение устойчивости учитывается через весовые коэффициенты βCi, соответствующие типам атак: «ложная информация», «функциональное поражение», «разрыв соединения». Двойное неравенство задаёт диапазоны изменения этих сумм:

$$1 \geq \Sigma(\text{РУФ} + \alpha_{\text{П}j}) \geq 0{,}7; 1 \geq \Sigma(\text{РУФ} - \beta_{\text{C}i}) \geq 0{,}5; \alpha_{\text{П}j}\text{П}j, \beta_{\text{C}i} \in] \qquad (5.3)$$

Совместное применение классических методик оценки рисков и модели регулирования по Климову позволяет получить количественные оценки эффективности мер противодействия и обосновать распределение ресурсов между отдельными рубежами защиты.

2. Методические указания к практическому занятию и порядок выполнения заданий. Задания

Задание 1

1. Для SIR с β=0,4; γ=0,15; S(0)=0,99; I(0)=0,01 найдите R0. Проинтегрируйте на [0,50]. Определите t_{max} и I_{max}. Оцените R(∞). Постройте графики.

2. Введите патчинг с интенсивностью ν. Исследуйте Imax при ν=0,05; 0,10; 0,20. Постройте Imax(ν).

3. Сервер: λ_l=50 с−1, 1/μ=0,01 с. Найдите λ_{a*} при ρ≥0,95. Постройте W(λ_a).

4. Модифицируйте модель с фильтрацией атакующих пакетов с вероятностью p_f. Найдите минимальный p_f для устойчивости при λ_a=80 с−1.

5. Сформулируйте задачу оптимального управления ν(t) с ограничением затрат и критерием min ∫I(t)dt. Запишите гамильтониан Понтрягина.

Задание 2

1. Составить перечень из 8–10 типовых угроз для фрагмента ИС (сканирование сети, подбор паролей, эксплуатация уязвимостей веб–приложения, DDoS–атака, фишинг с malware, инсайдерская утечка, эксплуатация RDP, атака на API).

2. Для каждой угрозы экспертно оценить SLE (тыс. руб.) и ARO (1/год); по формуле (5.1) рассчитать ALE; результаты свести в таблицу вида 5.1.

3. Построить матрицу рисков 5×5 (5 уровней вероятности × 5 уровней ущерба), разместить в её клетках перечисленные угрозы; определить приоритеты регулирования (зелёная, жёлтая, оранжевая, красная зоны).

4. Для каждой угрозы предложить конкретную меру регулирования (снижение вероятности за счёт настройки СПКА, снижение ущерба за счёт резервирования, передача риска через страхование, принятие); оценить стоимости контрмер $C_к$.

5. По формуле (5.2) рассчитать экономическую эффективность E каждой контрмеры; выделить меры, для которых $E > 0$ (оправданы к внедрению); объяснить отказ от мер с $E \leq 0$.

6. Применить модель регулирования по Климову: присвоить значения $\alpha_{Пj}$ (для 5 средств повышения устойчивости) и βCi (для 3 типов атак) из диапазона [0,15; 0,45]; проверить выполнение двойного неравенства (5.3) для суммы по всем мерам и атакам.

7. Рассчитать остаточный риск $R_{ост}$ для каждой угрозы после внедрения выбранных контрмер; убедиться, что $R_{ост}$ниже заданного порога (например, 100 тыс. руб.); при превышении предложить дополнительные меры.

8. Применить модель FAIR к одной из угроз: оценить LossEventFrequency (LEF) и LossMagnitude (LM) в денежном выражении; рассчитать Risk = LEF · LM; сравнить с ALE из пункта 2 и объяснить расхождения.

9. Подготовить итоговый отчёт с обоснованием выбранного распределения ресурсов по рубежам противодействия и прогнозируемым уровнем остаточного риска.

В рамках занятия студент составляет перечень типовых угроз для фрагмента ИС, экспертно оценивает вероятности и ущербы, строит матрицу рисков и рассчитывает показатели ALE, эффективность контрмер и остаточный риск с учётом коэффициентов $\alpha_{Пj}$ и βCi.

Таблица 5.1 – Пример количественной оценки рисков для типовой ИС

Угроза	SLE, тыс. руб.	ARO	ALE, тыс. руб.	Уровень
Подбор паролей по SSH	150	3,0	450	Средний
Эксплуатация уязв. веб–прил.	850	0,4	340	Средний
DDoS–атака	300	1,2	360	Средний
Фишинг с malware	1200	0,8	960	Высокий
Инсайдерская утечка	2000	0,2	400	Средний

После внедрения контрмеры (например, MFA для SSH) новые значения SLEост и AROост пересчитываются, и по формуле (5.2) определяется экономическая эффективность. Контрмера считается оправданной, если E > 0, а остаточный риск $R_{ост} = SLE_{ост} \cdot ARO_{ост}$ ниже приемлемого порога.

Требования к отчёту и защите

Защита предполагает опрос по материалу, изложенному в отчёте. Отчёт должен быть оформлен: требуется наличие титульного листа, указание цели практического занятия, последовательное изложение выполненных расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания. Проверяется знание теоретического материала с учётом ответов на контрольные вопросы. Задаются вопросы по пунктам, приведённым в разделе «Порядок выполнения работы». Критерии к оценке защиты отчёта студентом приведены в таблице 9.1.

Контрольные вопросы для самопроверки

1. Что такое риск нарушения информационной безопасности и как он вычисляется в базовой модели (3.1)?
2. Что такое SLE, ARO и ALE? Запишите формулу (5.1).
3. Как определяется экономическая эффективность контрмеры по формуле (5.2)?
4. Перечислите этапы процесса оценки рисков по методике NIST SP 800–30.
5. Что такое матрица рисков и как она строится? Какие зоны выделяются?

6. Какие виды обработки рисков вы знаете? Приведите пример для каждого.

7. Какие весовые коэффициенты использует методика Климова для регулирования устойчивости функционирования ИС? Запишите формулу (5.3).

8. В чём заключается различие между коэффициентами $\alpha_{\Pi j}$ (повышения устойчивости) и β_{Ci}(снижения устойчивости)?

9. Какова сущность модели FAIR и как она соотносится с классической моделью ALE?

10. Что означает $R_0 > 1$ в модели распространения вредоносного ПО?

11. Каковы основные предположения SIR–модели?

12. Как связана интенсивность заявок с отказом в обслуживании в M/M/1?

13. В чём идея принципа максимума Понтрягина применительно к управлению распространением ВПО?

14. Какие модели адекватны для атак на целостность данных?

15. Как топология сети влияет на скорость распространения червя?

16. Что такое положение равновесия и как исследуется его устойчивость?

Практическое занятие № 6. Метод натурного и имитационного моделирования процессов компьютерных атак и противодействия им

Общие сведения

Цель: сформировать навыки решения типовых и прикладных задач в области применения методов натурного и имитационного моделирования процессов противодействия компьютерным атакам на ИС; приобрести практические навыки разработки плана эксперимента, расчёта необходимого числа испытаний по формулам Бокса–Уилсона, проведения имитационных экспериментов методом Монте–Карло и количественной оценки метрик MTTD и MTTR.

Перечень знаний и умений для достижения цели:

Знать: этапы метода натурного и имитационного моделирования по Климову; формулы расчёта необходимого числа испытаний (полный и дробный факторный план Бокса-Уилсона); метрики оперативности реагирования (MTTD, MTTR).

Литература: [7] С. М. Климов и др. (экспериментальная оценка на стендовом полигоне); [11] Е. В. Дойникова.

Уметь: разрабатывать план имитационного эксперимента; рассчитывать доверительные интервалы для метрик по формулам математической статистики; применять дробные факторные планы для сокращения вычислительных затрат.

Литература: [7] С. М. Климов и др.

Материалы, оборудование, программное обеспечение: стендовый полигон с сегментом ЛВС, АРМ имитатора атак, макет ИС (целевой АРМ, серверы сбора измерений и электронной почты), макеты СПКА, имитаторы информационной нагрузки, ПК с ОС KaliLinux, Python 3 с NumPy и SciPy, средства статистической обработки данных, методические материалы монографии Климова.

1. Методический материал к выполнению заданий

Метод натурного и имитационного моделирования процессов противодействия компьютерным атакам на ИС разработан для экспериментальной оценки эффективности применения методов, моделей и алгоритмов путём испытаний макетов средств противодействия в условиях, близких к реальным, на стендовом полигоне. Метод основан на пошаговой стратегии экспериментальной оценки параметров атак при воздействии на рубежи ИС, контроле устойчивости функционирования системы, натурном моделировании и выборе средств противодействия. В основе метода лежит теория моделирования и анализа сложных систем и метод Монте–Карло.

Семь шагов метода

Метод выполняется в виде следующей последовательности шагов:

1. Формализация натурного и имитационного моделирования процессов противодействия компьютерным атакам на ИС.
2. Разработка моделирующих алгоритмов.
3. Реализация имитационных и натурных моделей на стендовом полигоне в виде совокупности макетов АРМ.
4. Планирование натурного и имитационного моделирования (экспериментальных исследований).
5. Проведение натурного и имитационного моделирования (экспериментальных исследований).
6. Проверка выполнения требований к устойчивости функционирования ИС и требований к $C_{ПКА}$ по готовности к противодействию атакам.
7. Анализ и интерпретация результатов моделирования.

На первом шаге определяются исходные параметры моделирования (события и состояния BY_i, $\xi_{воз.уяз}$, Si, Y_i, τi, $Z_{ПДi}$), временной интервал моделирования и необходимые ресурсы. На втором шаге разрабатывается моделирующий алгоритм, реализующий унифицированную имитационную модель противодействия, включающую блоки планирования технологических операций, управления моделью, моделирования рубежей противодействия, генерации атак, моделирования средств противодействия, оценки методов и выбора вариантов.

Событийный способ имитации

В основе рассматриваемого метода лежит событийный способ имитации и натурного воспроизведения воздействий атак на ИС. Применение метода предполагает, что на временном интервале выполнения ТЦУ имеется своя характерная последовательность состояний и событий; множество событий и состояний воздействия атак конечно; детализация представления ИС соответствует макетам базовых АРМ, размещённых в составе ЛВС стендового полигона; интенсивность и объём поступления потоков входной информации и воздействий атак моделируются соответствующими имитаторами.

Планирование эксперимента и число испытаний

Планирование эксперимента позволяет найти такую совокупность доминирующих факторов, при которой достигается уменьшение числа необходимых испытаний и повышение экономичности экспериментов. Формализация процессов противодействия позволяет определить объём факторного пространства при основных ограничениях на метод Бокса–Уилсона: существование только одного оптимума и наличие не более 15 факторов. Необходимое общее количество испытаний имитационных и натурных моделей на стендовом полигоне определяется соотношением:

$$No = \prod l_i, i = 1, \ldots, k \qquad (6.1)$$

где l_i – число уровней i–го фактора, k – количество факторов в эксперименте. При нормальном законе распределения значений оцениваемых параметров необходимое число испытаний, обеспечивающих статистически гарантированные результаты с заданной ошибкой $\varepsilon_м$ и средним квадратическим отклонением σ_м, вычисляется по формуле:

$$Nи = (t_ф \cdot \sigma_м)^2 / \varepsilon_м^2 \qquad (6.2)$$

где $t_ф$ – квантиль нормального распределения, определяемый с использованием таблиц функции Лапласа (для доверительной вероятности 0,95 – $t_ф$ = 1,96). Для уменьшения N_o применяются дробные факторные планы типа $2^{(k-p)}$, где p – число генерирующих соотношений; например, план $2^{(5-1)}$ содержит 16 опытов вместо 32.

Метрики MTTD и MTTR

По результатам имитационных экспериментов рассчитываются метрики оперативности реагирования: MTTD (MeanTimetoDetect) – среднее время от начала атаки до её обнаружения; MTTR (MeanTimetoRespond) – среднее время от обнаружения до завершения реагирования. Доверительный 95%–ный интервал для среднего значения μ метрики M рассчитывается по формуле:

$$\mu \pm t_0{,}025 \cdot \sigma / \sqrt{N} \qquad (6.3)$$

где σ – выборочное стандартное отклонение, N – число опытов, t_0,025 = 1,96 для больших выборок.

Риск i–й угрозы $R_i = P_i \cdot U_i$. Совокупный риск $R = \Sigma R_i$ (аддитивная модель). Регулирование: $x_j \in \{0,1\}$ – индикатор меры стоимостью c_j; $P_{i'} = P_i \cdot \prod_j (1 - e_{ij}x_j)$. Задача: $\min \Sigma P_{i'}U_i$ при $\Sigma c_j x_j \le B$, $x_j \in \{0,1\}$ – целочисленное программирование. Для $x_j \in [0,1]$ – нелинейное программирование.

Методика включает идентификацию угроз, оценку вероятностей и ущербов, расчёт рисков, оптимизацию контрмер, оценку остаточного риска. При зависимых угрозах учитывают корреляции и каскадные эффекты.

2. **Методические указания к практическому занятию и порядок выполнения заданий. Задания**

Задание 1

1. Угрозы: P_1=0,30 U_1=500; P_2=0,15 U_2=2000; P_3=0,40 U_3=300. Рассчитайте риски. Постройте матрицу рисков (пороги вероятности 0,20/0,35, ущерба 400/1000).

2. Меры: c=(100,250,180,320); e = [[0,6;0,3;0,0;0,4], [0,2;0,7;0,5;0,1], [0,4;0,0;0,6;0,3]]; B=500. Найдите оптимальный набор полным перебором. Вычислите остаточный риск.

3. Допустите $x_j \in [0,1]$. Решите задачу нелинейного программирования. Сравните с целочисленным решением.

4. Введите ρ_{12}=0,6. Предложите корректировку совокупного риска через ковариацию. Как изменится оптимальный набор?

5. Постройте приближённый фронт Парето (риск vs стоимость).
Выберите компромиссное решение

Примечание. Полный перебор 16 вариантов легко выполняется скриптом. Для NLP используйте scipy.optimize.minimize.

Задание 2

1. Изучить описание стендового полигона: перечислить его базовые компоненты (АРМ имитатора атак, целевые АРМ, ССИ, СЭП, макеты СПКА) и схему их взаимодействия в сегменте ЛВС.

2. Сформулировать постановку задачи на моделирование: выбрать целевые показатели (вероятность устойчивого функционирования ИС, MTTD, MTTR), задать факторы и их уровни по таблице 6.1.

3. Разработать моделирующий алгоритм эксперимента, представляющий собой упрощённую реализацию унифицированной имитационной модели по методике Климова; описать блоки алгоритма и их взаимодействие.

4. Рассчитать необходимое общее число испытаний N_o по формуле (6.1) для полного факторного плана при k = 5, l_i= 3 (ответ: 243); рассчитать число прогонов N_и по формуле (6.2) при $t_ф$= 1,96, $σ_м$= 0,05, $ε_м$= 0,01 (ответ: 96).

5. Применить дробный факторный план $3^{(5-1)}$, сократить число опытов до 81; составить матрицу планирования с генерирующим соотношением x5 = x1·x2·x3.

6. Провести серию из 50 прогонов имитационной модели методом Монте–Карло; для каждого зафиксировать $K_{ПКА}$, MTTD и MTTR; построить гистограммы распределения этих показателей.

7. Рассчитать выборочное среднее и 95%-й доверительный интервал для MTTD и MTTR по формуле (6.3); сделать вывод об устойчивости результатов и необходимом объёме выборки.

8. Проверить выполнение требований к устойчивости функционирования ИС (РУФ ≥ 0,7) и готовности $C_{ПКА}$; проанализировать, при каких комбинациях факторов требования выполняются; построить поверхность отклика $K_{ПКА}(t)$ от двух наиболее значимых факторов.

9. Составить итоговый план проведения экспериментов на стендовом полигоне: указать последовательность опытов, ожидаемые результаты, требования к ресурсам.

В рамках занятия студент составляет план эксперимента для оценки эффективности СПКА, рассчитывает необходимое число испытаний N_o и $N_и$, проводит серию из 50 прогонов имитационной модели (или испытаний на полигоне) методом Монте–Карло и рассчитывает метрики MTTD и MTTR с доверительными интервалами.

Таблица 6.1 – Факторы имитационного эксперимента и их уровни

Фактор	**Обозначение**	**Уровни**	**Число уровней l_i**
Число рубежей СПКА	x1	3; 5; 7	3
Интенсивность атак	x2	0,05; 0,10; 0,20	3
Запаздывание обнаружения τ3	x3	0; 0,5; 1,0	3
Порог alert в SIEM	x4	0,7; 0,85; 0,95	3
Число датчиков	x5	2; 4; 6	3

Полный факторный план по формуле (6.1) составит $N_o = 3^5 = 243$ испытания. Применение дробного факторного плана $3^{(5-1)}$ сокращает это число до 81. Для каждого испытания рассчитывается значение $K_{ПКА}(t)$ и метрики

MTTD/MTTR; по выборке объёма $N_и$ (по формуле 6.2) строятся доверительные интервалы.

Требования к отчёту и защите

Защита предполагает опрос по материалу, изложенному в отчёте. Отчёт должен быть оформлен: требуется наличие титульного листа, указание цели практического занятия, последовательное изложение выполненных расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания. Проверяется знание теоретического материала с учётом ответов на контрольные вопросы. Задаются вопросы по пунктам, приведённым в разделе «Порядок выполнения работы». Критерии к оценке защиты отчёта студентом приведены в таблице 9.1.

Контрольные вопросы для самопроверки

1. Каково назначение метода натурного и имитационного моделирования процессов противодействия компьютерным атакам?
2. Перечислите семь шагов метода и кратко охарактеризуйте каждый из них.
3. Какие блоки входят в унифицированную имитационную модель противодействия по Климову?
4. Что такое событийный способ имитации и какие допущения он предполагает?
5. По какой формуле (6.1) рассчитывается необходимое общее число испытаний N_o? Поясните смысл входящих величин.
6. Как определяется число прогонов $N_и$ по формуле (6.2), обеспечивающее статистически гарантированные результаты?
7. Что такое дробный факторный план и каким образом он сокращает число опытов? Приведите пример.
8. Как рассчитывается доверительный интервал для метрик MTTD и MTTR по формуле (6.3)?
9. Каково типовое значение $t_ф$ для доверительной вероятности 0,95?

Практическое занятие № 7. Метод экспериментальной оценки эффективности компьютерных атак

Общие сведения

Цель: сформировать навыки решения типовых и прикладных задач в области применения метода экспериментальной оценки эффективности компьютерных атак; приобрести практические навыки проведения серии испытаний на стендовом полигоне, построения экспериментальных зависимостей коэффициента противодействия K_ПКА(t) от числа рубежей и

времени запаздывания обнаружения, а также количественной оценки вероятности прорыва атак через рубежи защиты.

Перечень знаний и умений для достижения цели:

Знать: формулы расчёта коэффициента противодействия КПКА(t) для множества атак; методику расчёта вероятности прорыва атаки через *n* рубежей защиты; основы статистической проверки гипотез (t-критерий, критерий $\chi 2$).

Литература: [7] С. М. Климов и др.; [13] А. А. Магазев; [5] NIST SP800-61.

Уметь: проводить серию испытаний на стендовом полигоне (или в имитационной среде); рассчитывать экспериментальные значения $K_{ПКА}(t)$ и оценивать их относительную погрешность (Δ) относительно теоретических моделей.

Литература: [7] С. М. Климов и др.

Материалы, оборудование, программное обеспечение: стендовый полигон с сегментом ЛВС, АРМ имитатора атак с инструментами KaliLinux, макет ИС, макеты СПКА с настраиваемым числом рубежей и временем реакции, средства сбора журналов и статистической обработки (Python 3 с NumPy, SciPy, Matplotlib; LibreOfficeCalc).

1. Методический материал к выполнению заданий

Метод экспериментальной оценки эффективности компьютерных атак предназначен для количественной оценки показателей, характеризующих способность нарушителя преодолеть рубежи противодействия СПКА. Метод основан на проведении серии экспериментов на стендовом полигоне, в которых имитатор атак генерирует поток атак с заданной интенсивностью νY, а макеты $С_{ПКА}$ противодействуют им с интенсивностью νПКА. По результатам экспериментов рассчитываются показатели: вероятность предупреждения, обнаружения и анализа атак, а также коэффициент противодействия компьютерным атакам $K_{ПКА}(t)$ на совокупности рубежей противодействия.

Коэффициент противодействия для множества атак

При воздействии множества атак с интенсивностью νY на совокупность рубежей СПКА, противодействующих с интенсивностью νПКА, коэффициент противодействия рассчитывается по формуле (7.1).

$$K_{ПКА}(t) = 1 - (\nu Y \cdot P_Y \cdot A_{YO} / r_{СПКА}) \cdot t + 0{,}5 \cdot (\nu Y \cdot \nu ПКА \cdot P_Р \cdot \pi_{OY} \cdot \pi П / r_{СПКА}) \cdot t^2 \quad (7.1)$$

где P_Y – вероятность воздействия атаки, A_YO – относительное число атак, $r_{СПКА}$ – число рубежей $С_{ПКА}$, $P_Р$ – вероятность противодействия, π_{OY} и $\pi_П$ – вероятности обнаружения и нейтрализации атаки. Для случая одной атаки и

одного рубежа формула упрощается до выражения $K_{ПКА}(t) = 1 – \lambda Y \cdot t + 0{,}5 \cdot \lambda Y \cdot \lambda ПКА \cdot \delta\pi П \cdot t^2$.

Влияние запаздывания обнаружения

Влияние запаздывания τЗ обнаружения атак стороной защиты на значение коэффициента противодействия иллюстрируется двумя характерными сценариями. При средних значениях τЗ компьютерная атака нарушителя успевает преодолеть один–два рубежа из семи, после чего дальнейшее развитие ситуации определяется соотношением интенсивностей. При малой величине τЗ характер изменения коэффициента противодействия не позволяет нарушителю преодолеть даже один рубеж СПКА. Зависимости $K_{ПКА}(t)$ наглядно показывают роль оперативности предупреждения, обнаружения и анализа атак на рубежах противодействия.

Влияние числа рубежей

Сравнение зависимостей $K_{ПКА}(t)$ при использовании 7, 5 и 3 рубежей противодействия показывает: с уменьшением числа рубежей относительное число обнаруженных атак возрастает ($y3(t) > y7(t)$), а относительное число непреодолённых рубежей у стороны защиты уменьшается ($x3(t) < x7(t)$). Это демонстрирует необходимость противодействия атакам на семи рубежах СПКА: только в этом случае обеспечивается достаточный запас по эффективности защиты. Влияние относительного числа средств противодействия, приходящихся на один рубеж δπП, дополнительно иллюстрирует важность сбалансированного распределения датчиков СПКА по рубежам.

Вероятность прорыва атак

Вероятность прорыва атаки через n рубежей защиты при вероятности нейтрализации на каждом рубеже $p_н$ вычисляется как:

$$Рпрор = (1 – p_н)^n \qquad (7.2)$$

Например, при $p_н = 0{,}7$ и $n = 7$, $Рпрор = 0{,}3^7 \approx 2{,}2 \cdot 10^{-4}$; при $n = 3$ – $Рпрор = 0{,}3^3 = 0{,}027$. Таким образом, увеличение числа рубежей с 3 до 7 снижает вероятность прорыва в 122 раза.

Показатели для оценки

По результатам экспериментальной оценки определяются значения для числа средств противодействия и времени обнаружения атак на каждом рубеже. Эти показатели позволяют оценить возможности комплексного противодействия атакам на базе компонентов СПКА, СЗИ от несанкционированного доступа и антивирусных средств, а также выбрать рациональные варианты построения средств противодействия атакам, при которых сохраняется заданная устойчивость функционирования ИС.

Эффективность атаки характеризуется вероятностью успеха p, средним временем T, ущербом U. При $X \sim Bin(n,p)$ оценка $\hat{p}=X/n$; ДИ $\hat{p} \pm z\sqrt{[\hat{p}(1-\hat{p})/n]}$. Для

сравнения средних – t–критерий или Манна–Уитни. Размер эффекта Коэна d=(μ1−μ2)/σ. Планирование объёма: $n \approx (z\alpha/2 + z\beta)^2 \cdot 2\sigma^2/\delta^2$.

Для таблиц сопряжённости – χ^2 или точный тест Фишера.

2. Методические указания к практическому занятию и порядок выполнения заданий. Задания

Задание 1

1. n=40, успехов 17. Постройте 95%-ный ДИ для p. Проверьте H0: p=0,30 при α=0,05.

2. Две модификации по 25 опытов: $\bar{T}_1$=12,4; $\bar{T}_2$=9,7; s_1=3,1; s_2=2,8. Проверьте равенство средних (t–критерий). Рассчитайте d.

3. Найдите n для обнаружения δ=2 мин при σ≈3, α=0,05, мощности 0,80.

4. Таблица 2×2 «обнаружена/не обнаружена» для двух систем защиты. Примените χ^2 или Фишера.

5. Предложите план факторного эксперимента 2^2 (версия ПО × наличие IDS) на вероятность успеха.

Задание 2

1. Изучить методику экспериментальной оценки эффективности компьютерных атак по Климову; записать исходные формулы (7.1) для K_ПКА(t) для множества атак и упрощённую для одной атаки.

2. Подготовить стендовый полигон к экспериментам: настроить макет ИС, развернуть СПКА с заданным числом рубежей (например, 7), установить имитатор атак с возможностью настройки интенсивности νY.

3. Рассчитать по формуле (7.2) теоретическую вероятность прорыва для n = 3, 5, 7 и $p_н$ = 0,7; 0,8; 0,9; заполнить таблицу 7.1; сделать вывод о влиянии числа рубежей.

4. Провести серию испытаний (не менее Nи = 50, рассчитанного в практическом занятии № 6) с различными значениями числа рубежей СПКА (3, 5, 7) и времени запаздывания τЗ (0; 0,5; 1; 2); для каждого испытания зафиксировать количество обнаруженных, нейтрализованных и пропущенных атак.

5. По результатам испытаний построить экспериментальные зависимости $K_{ПКА}(t)$ для всех комбинаций параметров; по формуле (7.3) рассчитать относительную погрешность Δ относительно теоретических значений из практического занятия № 4.

6. Построить гистограммы экспериментальных значений Рпрор для n = 3, 5, 7; сопоставить с теоретическими значениями из таблицы 7.1; рассчитать выборочное среднее и 95%-ный доверительный интервал для $P_{прор}$.

7. По результатам серии экспериментов построить поверхность отклика $K_{ПКА}$ от двух факторов (n, τЗ); определить оптимальные значения факторов, при которых $K_{ПКА} \geq 0{,}8$ при минимальных затратах ресурсов СПКА.

8. Сформулировать выводы о применимости метода экспериментальной оценки эффективности атак; определить рациональное число рубежей противодействия и требуемое время обнаружения для типовой ИС; подтвердить выполнение условия $\Delta \leq 5$ %.

В рамках занятия студент проводит серию испытаний на стендовом полигоне (или имитационной модели) при различных значениях числа рубежей СПКА и времени запаздывания τЗ, рассчитывает экспериментальные значения $K_{ПКА}(t)$ и сопоставляет их с теоретическими.

Таблица 7.1 – Вероятность прорыва атак через n рубежей защиты

n рубежей	**δπП**	**Рпрор ($p_н$=0,7)**	**Рпрор ($p_н$=0,8)**	**Рпрор ($p_н$=0,9)**
3	0,333	$2{,}70 \cdot 10^{-2}$	$8{,}00 \cdot 10^{-3}$	$1{,}00 \cdot 10^{-3}$
5	0,200	$2{,}43 \cdot 10^{-3}$	$3{,}20 \cdot 10^{-4}$	$1{,}00 \cdot 10^{-5}$
7	0,143	$2{,}19 \cdot 10^{-4}$	$1{,}28 \cdot 10^{-5}$	$1{,}00 \cdot 10^{-7}$

Относительная погрешность экспериментальных значений K_ПКА относительно теоретических рассчитывается по формуле:

$$\Delta = |K_{эксп} - K_{теор}| / K_{теор} \cdot 100\ \% \qquad (7.3)$$

При $\Delta \leq 5$ % экспериментальная модель считается адекватной; при $\Delta > 10$ % требуется корректировка параметров модели.

Требования к отчёту и защите

Защита предполагает опрос по материалу, изложенному в отчёте. Отчёт должен быть оформлен: требуется наличие титульного листа, указание цели практического занятия, последовательное изложение выполненных расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания. Проверяется знание теоретического материала с учётом ответов на контрольные вопросы. Задаются вопросы по пунктам, приведённым в разделе «Порядок выполнения работы». Критерии к оценке защиты отчёта студентом приведены в таблице 9.1.

Контрольные вопросы для самопроверки

1. Каково назначение метода экспериментальной оценки эффективности компьютерных атак?
2. Запишите формулу (7.1) коэффициента противодействия $K_{ПКА}(t)$ для множества атак.
3. Как влияет запаздывание обнаружения $\tau З$ на значения $K_{ПКА}(t)$ в двух рассмотренных сценариях?
4. Как изменяются показатели x(t) и y(t) при уменьшении числа рубежей противодействия с 7 до 3?
5. Что такое относительное число средств противодействия, приходящихся на один рубеж ($\delta\pi П$), и как оно влияет на эффективность защиты?
6. Как рассчитывается вероятность прорыва атаки через n рубежей защиты по формуле (7.2)?
7. Как определяется относительная погрешность экспериментальных значений по формуле (7.3)?
8. При каких значениях Δ экспериментальная модель считается адекватной?
9. Какие практические рекомендации можно сформулировать по результатам экспериментальной оценки?
10. В чём различие доверительного интервала и интервала предсказания?
11. Когда предпочесть непараметрический критерий?
12. Как связан объём выборки с мощностью критерия?
13. Что такое размер эффекта и почему он важен?
14. Какие этические ограничения существуют при экспериментальной оценке атак?
15. В чём идея точного теста Фишера?
16. Что такое взаимодействие факторов в факторном эксперименте?

Практическое занятие № 8. Метод оценки эффективности активного противодействия компьютерным атакам на критически важные информационные системы

Общие сведения

Цель: сформировать навыки решения типовых и прикладных задач в области оценки эффективности активного противодействия компьютерным атакам на ИС; приобрести практические навыки построения сетевого графика противодействия, расчёта вероятности отражения атаки, применения игровых методов для выбора оптимальной стратегии защиты и количественной оценки коэффициента информационного превосходства защитника над нарушителем.

Перечень знаний и умений для достижения цели:

Знать: структуру сетевого графика противодействия и метод расчёта критического пути; основы антагонистических игр с нулевой суммой (платёжная матрица, цена игры, равновесие Нэша); понятие коэффициента информационного превосходства (Кип).

Литература: [7] С. М. Климов и др.; [11] Е. В. Дойникова; [9] M. Bishop (теория игр в контексте компьютерной безопасности).

Уметь: строить сетевой график и рассчитывать минимальное время отражения атаки (ТкритТкрит); решать матричные игры для выбора оптимальной смешанной стратегии защиты; рассчитывать вероятность достижения информационного превосходства на основе циклов OODA.

Литература: [7] С. М. Климов и др.; [11] Е. В. Дойникова.

Материалы, оборудование, программное обеспечение: ПК с табличным процессором (LibreOfficeCalc или MicrosoftExcel), средствами построения графов (LibreOfficeDraw, draw.io, либо Python + networkx), стендовый полигон с развёрнутыми IPS и SIEM, методические материалы монографии Климова, справочные данные по типовым сценариям атак.

1. Методический материал к выполнению заданий

Метод оценки эффективности активного противодействия компьютерным атакам на ИС предназначен для обоснования рационального плана применения средств защиты в условиях конфликтного взаимодействия нарушителя (сторона С) и защитника (сторона В). Метод включает пять основных элементов: разработку сетевого графика противодействия, расчёт вероятности отражения компьютерной атаки, выбор средств активного противодействия на основе игровых методов, расчёт вероятности достижения информационного превосходства стороны В над стороной С и расчёт коэффициента информационного превосходства.

Сетевой график противодействия

Сетевой график противодействия компьютерным атакам на ИС необходим для рационального планирования активного противодействия и позволяет: определить порядок применения средств противодействия атакам; реализовать активное противодействие в кратчайшие сроки; минимизировать затраты вычислительного ресурса ИС и ущерб для устойчивого выполнения ТЦУ. Сетевой график представляется ориентированным графом, вершины которого соответствуют отдельным действиям СПКА, а дуги – логической последовательности их выполнения. Критический путь графа определяет минимально возможное время отражения атаки; рассчитывается по формуле:

$$Tкрит = max\Sigma ti \quad (8.1)$$

где t_i – длительность i-го действия; суммирование ведётся по всем полным путям графа от начальной до конечной вершины.

Вероятность отражения атаки

Вероятность отражения компьютерной атаки P_отр определяется как произведение вероятностей обнаружения, анализа и нейтрализации атаки на соответствующих рубежах СПКА:

$$P\text{отр} = P_{\text{обн}} \cdot P_{\text{н}} \cdot P_{\text{нейт}} \quad (8.2)$$

где $P_{обн}$ – вероятность обнаружения атаки датчиками, $P_{ан}$ – вероятность корректного анализа в SIEM, $P_{нейт}$ – вероятность успешной нейтрализации средствами IPS. Она зависит от качества датчиков, скорости корреляции событий и правильности выбранной стратегии противодействия.

Игровые методы выбора стратегии

Выбор средств активного противодействия на основе игровых методов сводит задачу защиты к антагонистической игре двух лиц с нулевой суммой. Сторона С (нарушитель) выбирает стратегии реализации атаки из множества $\{s_1, \ldots, s_m\}$, сторона В (защитник) – стратегии противодействия из множества $\{1, \ldots, dn\}$. Платёжная матрица игры $A = ||a_{ij}||$ содержит значения эффективности пар (s_i, d_j), характеризующие, например, вероятность отражения атаки или ожидаемый ущерб. Цена игры в смешанных стратегиях вычисляется по формуле:

$$v = max_p min_j \sum_i p_i \cdot a_{ij} = max_p min_j \sum_i q_i \cdot a_{ij} \quad (8.3)$$

где p и q – смешанные стратегии сторон В и С соответственно. Решение игры в смешанных стратегиях даёт оптимальное распределение частот применения каждой из стратегий защитника, при котором достигается минимальный гарантированный уровень защиты.

Информационное превосходство

Информационное превосходство стороны В над стороной С характеризуется её способностью получать, обрабатывать и использовать информацию о намерениях и действиях нарушителя быстрее и полнее, чем это способен делать нарушитель. Вероятность достижения информационного превосходства определяется отношением времени цикла OODA (Observation–Orientation–Decision–Action) защитника к аналогичному времени нарушителя:

$$P\text{ИП} = tOODA(C)/(tOODA(C) + tOODA(B)) \quad (8.4)$$

Коэффициент информационного превосходства K_ИП рассчитывается как отношение числа успешно нейтрализованных атак к числу атак, достигших цели, за рассматриваемый период:

$$КИП = N\,\text{нейтр}/N\,\text{достиг} \quad (8.5)$$

Значение $К_{ип} \geq 1$ означает, что защитник опережает нарушителя; значения $К_{ип} < 1$ указывают на необходимость усиления СПКА. Совместное применение сетевого графика, расчёта вероятности отражения, игровых методов и расчёта коэффициента информационного превосходства позволяет получить количественные оценки эффективности активного противодействия и обосновать распределение средств защиты по рубежам ИС.

Активное противодействие включает блокировку, дезинформацию, honeypot и т. п. Показатели: P_d, T_r, P_r, K_f=Fafter/Fbefore. Теоретико-игровой подход: платёжная матрица U(a,d); равновесие Нэша в смешанных стратегиях. Для игры 2×2: $p * (u_{22} - u_{21})/(u_{11} - u\ \ 12 - u_{21} + u_{22})$. Эффективность $E = (R_0 - R_d)/R_0$.

Метрики живучести учитывают способность продолжать критические функции. Более сложные постановки – игры с неполной информацией, повторяющиеся и дифференциальные игры.

2. Методические указания к практическому занятию и порядок выполнения заданий. Задания

Задание 1

1. Состояния после атаки: отказ (1000), деградация (400), штатный (0). Без защиты: 0,25; 0,45; 0,30. С защитой: 0,08; 0,27; 0,65. Рассчитайте ожидаемый ущерб и E.

Задан2. Игра 2×2: U=[[80,30],[50,90]]. Найдите смешанное равновесие Нэша и значение игры.

3. Добавьте стоимости защиты (20 и 5). Найдите новое равновесие.

4. Предложите показатель живучести, зависящий от Pd, Tr, Pr. Обоснуйте форму.

5. Сформулируйте задачу динамической оптимизации на горизонте T. Запишите уравнение Беллмана.

Задание 2

1. Изучить состав метода оценки эффективности активного противодействия по Климову; перечислить его пять основных элементов и кратко охарактеризовать каждый.

2. Для заданного сценария атаки на типовую ИС разработать сетевой график противодействия по данным таблицы 8.1; по формуле (8.1) определить критический путь и оценить минимальное время Ткрит отражения атаки.

3. По формуле (8.2) рассчитать вероятность отражения Ротр для типовых значений $P_{обн}$ = 0,85, $P_{ан}$ = 0,90, $P_{нейт}$ = 0,80; провести анализ чувствительности $P_{отр}$

к изменению каждой компоненты; определить, какая компонента даёт наибольший прирост $P_{отр}$ при увеличении на 0,05.

4. Построить матрицу игры 4×4 для взаимодействия нарушителя (4 стратегии реализации) и защитника (4 стратегии противодействия), заполнив её значениями вероятности отражения; найти оптимальные смешанные стратегии защитника симплекс–методом или графически; вычислить цену игры v по формуле (8.3).

5. По результатам имитационного эксперимента (используя данные практического занятия № 7) собрать статистику Nнейтр и Nдостиг; по формуле (8.5) рассчитать коэффициент информационного превосходства КИП; сделать вывод о соотношении сторон ($K_{ИП} \geq 1$ или $K_{ИП} < 1$).

6. По формуле (8.4) рассчитать вероятность P_ИП для типовых значений tOODA(B) = 12 мин (сторона защиты) и t_{OODA}(C) = 25 мин (сторона нарушителя); определить, как изменится РИП при сокращении tOODA(B) на 30 %.

7. Сформулировать итоговые рекомендации по построению активного противодействия для типовой ИС: определить приоритетные рубежи защиты, требуемое время реакции $T_{крит}$, минимально приемлемые значения $P_{отр}$ и $K_{ИП}$, состав СПКА.

8. Оценить экономическую эффективность предложенных мер: рассчитать ALE до и после внедрения активного противодействия (используя методику из практического занятия № 5); обосновать целесообразность применения игрового подхода к выбору контрмер.

В рамках занятия студент строит сетевой график противодействия для заданного сценария атаки, рассчитывает критический путь и вероятность отражения, составляет и решает матричную игру, а также оценивает коэффициент информационного превосходства.

Таблица 8.1 – Действия сетевого графика противодействия

Действие СПКА	**Длительность t_i, мин**	**Предшественники**
Срабатывание датчика	0,5	—
Корреляция в SIEM	1,5	1
Анализ аналитиком L1	5,0	2
Эскалация на L2	10,0	3
Применение контрмеры	2,0	4
Верификация устранения	8,0	5

Сумма длительностей на критическом пути определяет минимальное время отражения атаки $T_{крит}$. По формуле (8.2) рассчитывается вероятность

отражения $P_{отр}$; при типовых значениях $P_{обн} = 0,85$, $P_{ан} = 0,90$, $P_{нейт} = 0,80$ получаем $P_{отр} = 0,612$. Для повышения эффективности рекомендуется параллельное выполнение анализа и эскалации.

Требования к отчёту и защите

Защита предполагает опрос по материалу, изложенному в отчёте. Отчёт должен быть оформлен: требуется наличие титульного листа, указание цели практического занятия, последовательное изложение выполненных расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания. Проверяется знание теоретического материала с учётом ответов на контрольные вопросы. Задаются вопросы по пунктам, приведённым в разделе «Порядок выполнения работы». Критерии к оценке защиты отчёта студентом приведены в таблице 9.1.

Контрольные вопросы для самопроверки

1. Какие пять элементов включает метод оценки эффективности активного противодействия по Климову?
2. Что такое сетевой график противодействия и для чего он предназначен?
3. Как определяется критический путь сетевого графика по формуле (8.1)?
4. Запишите формулу (8.2) для вероятности отражения атаки $P_{отр}$; поясните её компоненты.
5. Как формализуется задача выбора стратегии защиты в виде антагонистической игры? Что такое цена игры v и как она вычисляется по формуле (8.3)?
6. Что такое информационное превосходство стороны В над стороной С? Запишите формулу (8.4) для РИП.
7. Как рассчитывается коэффициент информационного превосходства К_ИП по формуле (8.5)?
8. Какие значения КИП указывают на необходимость усиления СПКА? Какова целевая граница?
9. Как соотносятся результаты данного занятия с результатами практического занятия № 5 (регулирование рисков)?

Дополнительные методические материалы и примеры расчётов

В данном пункте приведены развёрнутые пояснения и дополнительные примеры, которые рекомендуется использовать при подготовке к практическим занятиям и при выполнении заданий. Эти материалы дополняют теоретические введения соответствующих занятий и способствуют более глубокому усвоению математического аппарата.

К практическому занятию № 1. Дополнительные сведения о ROC–анализе и выборе порога

ROC–кривая полностью характеризует способность детектора различать два класса при всех возможных порогах. Точка (0,0) соответствует порогу, при котором ни один объект не объявляется атакой; точка (1,1) – порогу, при котором все объекты объявляются атаками. Идеальный детектор проходит через точку (0,1). Площадь AUC может быть интерпретирована как вероятность того, что случайно выбранный объект класса «атака» получит более высокий скор, чем случайно выбранный объект класса «норма».

При известной стоимости ошибок оптимальный порог находится из условия равенства отношения правдоподобия отношению априорных вероятностей, умноженному на отношение стоимостей. Если плотности вероятности скоров заданы аналитически (например, нормальными законами), порог может быть найден численно путём минимизации функции среднего риска на сетке значений τ.

Пример 1. Пусть $\mu_a=3$, $\sigma_a=1$, $\mu n=0$, $\sigma n=1$, P(attack)=0,1, cFN=10, cFP=1. Тогда средний риск как функция порога τ имеет минимум в окрестности $\tau\approx1{,}6\ldots1{,}8$ (конкретное значение зависит от точного вида интегралов ошибок). Студентам рекомендуется построить график $R(\tau)$ и убедиться в наличии единственного минимума.

Пример 2. За сутки в сети зафиксировано 1000 событий. Из них 100 – реальные атаки. Сигнатурный детектор (Suricata) обнаружил 80 атак, но при этом выдал 20 ложных срабатываний на легитимный трафик.

Нужно рассчитать Precision, Recall, F1 и FPR.

Ожидаемый ответ: TP = 80, FN = 20, FP = 20, TN = 880.

Precision = 80 / (80+20) = 0,80.

Recall = 80 / (80+20) = 0,80.

F1 = 2 * (0,8 * 0,8) / (0,8 + 0,8) = 0,80.

FPR = 20 / (20 + 880) = 0,022.

Детектор имеет хороший баланс, но 2,2 % ложных тревог могут утомлять аналитика.

К практическому занятию № 2. Дополнительные сведения о градиентном спуске и генетических алгоритмах

Сходимость градиентного спуска для логистической регрессии гарантируется при достаточно малом постоянном шаге η, поскольку функция потерь выпукла. На практике скорость сходимости можно ускорить, используя адаптивные методы (Adam) или методы второго порядка (L–BFGS). При большом объёме данных применяют мини–пакетный (mini–batch) градиентный спуск.

В генетическом алгоритме качество решения существенно зависит от баланса между исследованием (exploration) и использованием (exploitation).

Слишком высокая вероятность мутации превращает поиск в случайный; слишком низкая – приводит к преждевременной сходимости. Рекомендуемые значения pm обычно лежат в диапазоне 0,01–0,1; вероятность скрещивания pc – в диапазоне 0,6–0,9. Элитизм (сохранение лучшей особи) повышает устойчивость алгоритма.

Пример. Для обучения модели на датасете NSL-KDD используется алгоритм k-means для кластеризации сетевого трафика на 3 группы (K=3).

Нужно объяснить, как оценить качество разбиения с помощью индекса силуэта (SilhouetteIndex).

Нужно рассчитать среднее расстояние от точки до точек своего кластера (a) и до точек ближайшего чужого кластера (b). Коэффициент силуэта для точки = (b - a) / max(a, b). Значение варьируется от -1 до 1. Чем ближе к 1, тем лучше разбиение. Сравниваем средние значения для K=2, 3 и 4 и выбираем K с максимальным индексом.

К практическому занятию № 3. Дополнительные сведения о марковских моделях атак

Для цепи с поглощающими состояниями матрицу переходных вероятностей (или генератор) удобно записывать в канонической форме, выделяя блок переходных состояний Q и блок поглощения R. Тогда фундаментальная матрица $N = (I - Q)^{(-1)}$ даёт средние времена пребывания в переходных состояниях до поглощения. Вероятности поглощения в конкретных поглощающих состояниях находятся из матрицы B = N R.

Эти величины имеют прямую интерпретацию в задачах безопасности: элемент матрицы B указывает вероятность того, что атака, начавшаяся в данном состоянии, завершится успехом (или будет обнаружена). Среднее время до поглощения характеризует «окно возможности» для средств защиты.

Пример. Атака начинается в состоянии S0. Вероятность перехода из S0 в S1 (разведка) за 1 час равна 0,5. Вероятность перехода из S1 в S2 (проникновение) – 0,3.

Нужно найти вероятность того, что атака достигнет S2 за 2 часа (при условии, что переходы происходят последовательно).

Ожидаемый ответ: для достижения S2 за 2 часа атака должна перейти S0→S1 на первом часу (P=0,5) и S1→S2 на втором часу (P=0,3). Итоговая вероятность = 0,5 * 0,3 = 0,15 (или 15 %). Это показывает, что за 2 часа атака с такими параметрами имеет низкий шанс на успех, но с течением времени он растет.

К практическому занятию № 4. Дополнительные сведения о SIR и моделях массового обслуживания

В SIR–модели при постоянных коэффициентах существует первый интеграл, позволяющий выразить I как функцию S: $I(S) = I0 + S0 - S + (\gamma/\beta)$

ln(S/S0). Максимум I достигается при $S = \gamma/\beta = 1/R0$ (если $S0 > 1/R0$). Это соотношение полезно для быстрой оценки пиковой нагрузки на систему защиты.

В моделях массового обслуживания с приоритетами или с отказом (системы с потерями) формулы для вероятностей состояний усложняются. Для простейшей системы M/M/1/K с ограниченной очередью вероятность отказа (потери пакета) равна $p^K = (1-\rho)\rho^K / (1-\rho^{(K+1)})$. Эта величина может интерпретироваться как вероятность успешного «забивания» сервера атакующим потоком.

Пример. Интенсивность атак $\lambda Y = 0,1$ (1/час), интенсивность противодействия $\lambda ПКА = 0,3$ (1/час). Запаздывание обнаружения $\tau 3 = 0,5$ часа.

Нужно рассчитать коэффициент противодействия К_ПКА(t) на момент времени t = 2 часа, используя формулу (4.2).

Ожидаемый ответ:

$К_{ПКА}(2) = 1 - 0,1*2 + 0,5*0,1*0,3*(2 - 0,5)^2 = 1 - 0,2 + 0,015 * 2,25 = 1 - 0,2 + 0,03375 = 0,83375$. Через 2 часа система противодействует примерно на 83 %. Если бы $\tau 3$ было меньше (например, 0,1 ч), коэффициент был бы выше.

К практическому занятию № 5. Дополнительные сведения об оптимизации мер защиты

Задача выбора оптимального набора мер защиты относится к классу задач о ранце (knapsack) с нелинейной целевой функцией (из–за мультипликативные снижения вероятностей). При малом числе мер (до 15–20) допустим полный перебор или метод ветвей и границ. При большем числе применяют метаэвристики: генетические алгоритмы, имитацию отжига, муравьиные алгоритмы.

Если меры могут внедряться частично, целевая функция становится гладкой (или кусочно–гладкой), и применимы методы нелинейного программирования с ограничениями. Важно проверять, что найденный локальный минимум является глобальным (например, путём многократного запуска с разных начальных точек).

Пример. Угроза «Фишинг с malware». Единичная потеря (SLE) при успешной атаке оценивается в 1200 тыс. руб. Ожидаемая частота реализации (ARO) — 0,8 раз в год.

Нужно рассчитать ожидаемые годовые потери (ALE) и предложить контрмеру, если её стоимость 500 тыс. руб., а остаточный ALE составит 300 тыс. руб. Ожидаемый ответ: ALE = 1200 * 0,8 = 960 тыс. руб. Экономическая эффективность контрмеры (E) = $(ALE - ALE_{ост}) - С_к = (960 - 300) - 500 = +160$ тыс. руб. Контрмера экономически оправдана, так как $E > 0$.

К практическому занятию № 6. Дополнительные сведения о методе Монте–Карло

При оценке вероятности редкого события простая выборка требует N порядка 1/p или больше. Метод выборки по значимости изменяет распределение

генерации так, чтобы интересующее событие происходило чаще; несмещённость оценки восстанавливается введением весовых коэффициентов, равных отношению исходной и новой плотностей. Эффективность метода характеризуется отношением дисперсий.

В дискретно–событийном моделировании важное значение имеет корректная обработка одновременных событий и выбор генераторов псевдослучайных чисел с достаточным периодом и статистическими свойствами.

Пример. В эксперименте участвуют 5 факторов (k=5), каждый имеет 3 уровня (l_i=3).

Нужно рассчитать необходимое общее число испытаний (N0) для полного факторного плана.

Ожидаемый ответ: по формуле (6.1) $N_0 = 3^5 = 243$ испытания.

Если использовать дробный факторный план $3^{(5-1)}$, количество испытаний сократится до 81, что существенно экономит ресурсы стенда, но снижает точность оценки взаимодействий факторов.

К практическому занятию № 7. Дополнительные сведения о планировании экспериментов

Мощность критерия $1-\beta$ – вероятность отвергнуть ложную нулевую гипотезу. При фиксированных α и δ увеличение n повышает мощность. На практике часто задают желаемую мощность 0,8 или 0,9 и вычисляют необходимый объём выборки. Формулы планирования основаны на нормальном приближении и могут требовать поправки при малых n или сильной асимметрии.

Размер эффекта Коэна дополняет p–value информацией о практической значимости. Даже при очень малом p–value (большой выборке) эффект может быть пренебрежимо мал с прикладной точки зрения, и наоборот.

Пример. Защита состоит из n = 7 рубежей. Вероятность нейтрализации атаки на каждом рубеже $p_н = 0,8$.

Нужно рассчитать вероятность прорыва атаки ($P_{проп}$) и сравнить с системой из 3 рубежей.

Ожидаемый ответ:

Для n=7: $P_{проп} = (1 - 0,8)^7 = 0,2\text{^}7 = 0,0000128$ (0,00128%).

Для n=3: $P_{проп} = 0,2^3 = 0,008$ (0,8%).

Увеличение числа рубежей с 3 до 7 снижает вероятность прорыва в 625 раз. Это доказывает необходимость эшелонированной защиты

К практическому занятию № 8. Дополнительные сведения о теории игр в кибербезопасности

Равновесие в смешанных стратегиях интерпретируется как рандомизация действий, не позволяющая противнику гарантированно эксплуатировать детерминированную стратегию. В задачах защиты – это может соответствовать

случайному выбору режимов мониторинга или случайному размещению ложных целей.

При наличии нескольких равновесий Нэша выбор конкретного равновесия может определяться дополнительными критериями (равновесие, доминирующее по риску; равновесие, максимизирующее безопасность защитника и т. д.). В динамических постановках естественным аппаратом является теория дифференциальных игр и уравнения Гамильтона–Якоби–Айзекса.

Пример. Игра 2×2. Матрица выигрышей (эффективность защиты) для стратегий нарушителя (строки) и защитника (столбцы):

U = [[80, 30], [50, 90]].

Нужно найти цену игры в смешанных стратегиях (v) и оптимальные вероятности применения стратегий.

Проверяем наличие седловой точки: min в строках (30; 50), max в столбцах (80; 90). Седловой точки нет, значит, решение в смешанных стратегиях.

Решаем систему уравнений:

80p + 50(1-p) = 30p + 90(1-p) → 30p + 50 = 90 - 60p → 90p = 40 → p = 4/9.

Цена игры v = 80(4/9) + 50(5/9) = 320/9 + 250/9 = 570/9 ≈ 63,3.

Защитник должен случайным образом выбирать стратегии с вероятностями 4/9 и 5/9, чтобы гарантировать средний уровень защиты 63,3.

Задания для самостоятельной работы

Практическое занятие № 1. Специфика применения методов обнаружения атак

Задания для самостоятельной работы:

1. Теоретический анализ: изучите раздел 1 пособия. Выпишите определения Precision, Recall, F1, FPR и AUC ROC. Объясните, почему в условиях сильного дисбаланса классов (например, когда атак 0,1 % от всего трафика) метрика Accuracy неинформативна (см. контрольный вопрос 14 на стр. 13).

2. Практический расчет (по данным Задания 2, п. 1 на стр. 11):

Имеется выборка: N=10000 наблюдений, Na=800 (атаки). Сигнатурный детектор: обнаружил 720 атак, 45 ложных тревог. Постройте матрицу ошибок (TP, FP, TN, FN) для сигнатурного детектора. Вычислите Precision, Recall, F1 и FPR по формулам (1.1–1.4). Сравните полученные значения с таблицей 1.1 (стр. 12) и объясните, укладываются ли они в заявленный диапазон.

3. Разработка правила. Напишите синтаксис правила для Suricata, которое будет генерировать оповещение (alert) при попытке подключения к порту 22 (SSH) более 5 раз за 30 секунд с одного IP-адреса (используйте пример базового правила на стр. 12 как шаблон). Поясните назначение каждого элемента правила.

Практическое занятие № 2. Использование методов вычислительного интеллекта

Задания для самостоятельной работы:

1. Изучение метрик. Прочитайте методический материал к выполнению заданий пособия на страницах 15–16. Запишите формулу (2.3) для информационного выигрыша IG(A). Объясните, как энтропия Шеннона H(C)связана с неопределенностью целевой переменной.

2. Анализ архитектуры нейросети (по Заданию 2, п. 5 на стр. 17): Предложите архитектуру нейронной сети для многоклассовой классификации (Normal, DoS, Probe, R2L, U2R).

Сколько нейронов должно быть на входном слое (с учетом 41 признака в NSL-KDD)? Сколько на выходном слое? Какую функцию активации использовать на выходном слое (softmax) и какую функцию потерь применить (категориальная кросс-энтропия)?

3. Расчет кодирования (по Заданию 1, п. 2 на стр. 16): объясните, зачем для категориальных признаков (protocol_type, service, flag) применяется метод one-hotencoding. Приведите пример: как будет закодирован признак protocol_type со значениями tcp, udp, icmp, если в выборке встречаются все три типа?

Практическое занятие № 3. Специфика анализа атак как процессов реализации угроз

Задания для самостоятельной работы:

1. Построение дерева атак (по Заданию 2, п. 2 на стр. 22): Выберите сценарий атаки «Фишинг → Установка вредоносного ПО → Эксфильтрация данных». Постройте дерево атак с логическими операциями AND/OR. *Экспертно оцените* вероятности листьев (в диапазоне 0,1–0,9). Рассчитайте вероятность реализации корневого события (успешной эксфильтрации) по формуле (3.2) на стр. 22.

2. Анализ по CyberKillChain (по Заданию 2, п. 3 на стр. 22). Сопоставьте этапы выбранного вами сценария с этапами CyberKillChain. Используя таблицу 3.1 (стр. 25), определите, какие датчики СПКА смогут обнаружить каждый этап, и выпишите соответствующие вероятности обнаружения p*i*.

3. Расчет MTTC. Используя данные из Задания 1, п. 3 (стр. 21) для марковской модели (интенсивности q_{01}, q_{12} и т. д.), объясните, как вычислить среднее время до компрометации. Запишите формулу (3.3) и поясните, для чего этот показатель используется на практике.

Практическое занятие № 4. Аналитическое моделирование процессов реализации угроз

Задания для самостоятельной работы:

1. Анализ формулы (4.2) (стр. 26). Запишите формулу для коэффициента противодействия $K_{ПКА}(t)$ с учетом запаздывания $\tau З$. Объясните, почему при $0 \le t \le \tau З$ противодействие отсутствует (чему равен $K_{ПКА}$ в этот момент?).

2. Ручной расчет (по Заданию 2, п. 2 на стр. 27). Используя параметры из таблицы 4.1 (λY=0,1; λПКА=0,3; δπП=1,0; $\tau З$=0,5), рассчитайте значение $K_{ПКА}(t)$ для моментов времени t=1 и t=3. Покажите ход вычислений.

3. Изучите материал про SIR-модель (стр. 25). Объясните физический смысл базового репродуктивного числа $R_0=\beta/\gamma$. Что происходит с распространением вредоносного ПО, если $R_0>1$? Предложите, как можно снизить R_0 (например, через «патчинг» с интенсивностью ν, как в Задании 1, п. 2 на стр. 27).

Практическое занятие № 5. Методика анализа и регулирования рисков

Задания для самостоятельной работы:

1. Расчет рисков (по Заданию 2, п. 2 на стр. 32). Для угрозы «Подбор паролей по SSH» экспертно заданы: SLE=150тыс. руб., ARO=3,0 (раза в год). Рассчитайте ожидаемые годовые потери ALE по формуле (5.1). Определите уровень риска (низкий, средний, высокий), если пороги: низкий <105<105 руб., средний 105−106 руб., высокий >106 руб.

2. Оценка контрмеры (по Заданию 2, п. 5 на стр. 32). Предложена контрмера (внедрение MFA) стоимостью C_k=200 тыс. руб., которая снижает ARO до 1,0 при том же SLE. Рассчитайте новый $ALE_{ост}$ и экономическую эффективность E по формуле (5.2). Сделайте вывод: оправдана ли эта контрмера экономически (E>0)?

3. Модель Климова. Изучите раздел про регулирование по Климову (стр. 31). Объясните разницу между коэффициентами $\alpha\Pi j$ (повышение устойчивости) и βC_i (снижение устойчивости). Приведите по одному примеру меры для каждого коэффициента.

Практическое занятие № 6. Метод натурного и имитационного моделирования

Задания для самостоятельной работы:

1. Планирование эксперимента (по Заданию 2, п. 4 на стр. 37): в эксперименте участвуют k=5 факторов, каждый имеет l_i=3 уровня. Рассчитайте необходимое общее число испытаний N_0 для полного факторного плана по формуле (6.1).

2. Рассчитайте число прогонов N_i по формуле (6.2), если $t_ф$=1,96, σM=0,05, εM=0,01. Поясните, зачем нужны оба этих числа.

3. Дробный факторный план. Объясните, что такое дробный факторный план 3(5−1) и почему он сокращает число опытов с 243 до 81 (см. стр. 38). В чем заключается компромисс при использовании такого плана (что теряется)?

4. Метрики MTTD/MTTR. Изучите раздел про метрики оперативности. Запишите формулу (6.3) для доверительного интервала. Предположим, вы провели 50 испытаний, и среднее время обнаружения (MTTD) составило 12 минут со стандартным отклонением 3 минуты. Рассчитайте 95%-й доверительный интервал для MTTD.

Практическое занятие № 7. Метод экспериментальной оценки эффективности атак

Задания для самостоятельной работы:

1. Расчет вероятности прорыва (по Заданию 2, п. 3 на стр. 42). Защита состоит из n=5 рубежей. Вероятность нейтрализации атаки на каждом рубеже $p_н$ =0,7. Рассчитайте вероятность прорыва $P_{проп}$ по формуле (7.2). Сравните результат с табличным значением для n=5и $p_н$=0,7 в таблице 7.1. Как изменится $P_{проп}$, если увеличить число рубежей до 7?

Статистическая проверка гипотез (по Заданию 1, п. 1 на стр. 42). В серии из n=40 испытаний атака была успешно отражена 17 раз. Постройте 95%-ный доверительный интервал для вероятности успешного отражения p. Проверьте нулевую гипотезу H_0:p=0,30 при уровне значимости α=0,05.

2. Оценка адекватности модели: Изучите формулу (7.3) на стр. 47. Экспериментальное значение $К_{ПКА}$составило 0,78, а теоретическое – 0,80. Рассчитайте относительную погрешность Δ. Сделайте вывод: является ли модель адекватной (при условии Δ≤5 %)?

Практическое занятие № 8. Метод оценки эффективности активного противодействия

Задания для самостоятельной работы:

1. Сетевой график (по Заданию 2, п. 2 на стр. 48). Используя данные таблицы 8.1 (стр. 53), постройте сетевой график противодействия (ориентированный граф). Определите критический путь. Рассчитайте минимальное время отражения атаки $T_{крит}$ по формуле (8.1). Объясните, какие действия лежат на критическом пути и почему их задержка недопустима.

2. Теория игр (по Заданию 1, п. 2 на стр. 47). Дана платежная матрица игры 2x2 для нарушения (строки) и защиты (столбцы): U=[80305090].Проверьте наличие седловой точки (найдите минимумы по строкам и максимумы по столбцам).Найдите цену игры v и оптимальные смешанные стратегии (вероятности p и $1-p$) аналитически, как показано в примере на стр. 58–59.

3. Информационное превосходство. Время цикла OODA защитника tOODA(B) =12 мин, нарушителя – tOODA(C)=25 мин. Рассчитайте вероятность достижения информационного превосходства РИП по формуле (8.4). Определите, как изменится РИП, если время реакции защитника сократится на 30 % (до 8,4 мин).

Описание текущего контроля

Текущий контроль по дисциплине «Теория анализа компьютерных атак» проводится с целью проверки уровня освоения практического материала и формирования компетенции ОПК-13. Текущий контроль осуществляется в форме выполнения и защиты практических занятий (№ 1–8), предусмотренных настоящим учебно-методическим пособием.

Виды текущего контроля:

1. **Текущая работа на занятии:** проверка готовности к занятию (знание теоретического материала), выполнение заданий практикума (расчёты, настройка ПО, моделирование, работа на стенде), ведение рабочей тетради.

2. **Отчёт по практическому занятию:** оформленный документ, содержащий титульный лист, цель работы, последовательное изложение расчётов и экспериментов, подписанные скриншоты хода работы, выводы по каждому пункту задания.

3. **Защита отчёта:** устный опрос по материалам отчёта, проверка знания теоретического материала и ответы на контрольные вопросы для самопроверки.

Текущий контроль проводится последовательно, по мере прохождения тем дисциплины. На каждом практическом занятии (согласно расписанию) студент выполняет задания и оформляет отчёт. Защита отчёта проводится на текущем или следующем занятии в соответствии с учебным планом. Итоговая аттестация по дисциплине (зачёт/экзамен) выставляется на основе результатов текущего контроля (защиты всех 8 практических работ) и ответов на завершающем этапе. Критерии положительной оценки изложены в таблице 9.1.

Таблица 9.1 – Шкала оценок уровня

Оценка			
Неудовлетво-рительный	**Пороговый**	**Углубленный**	**Продвинутый**
«2» (неудовлетво-рительно)	**«3» (удовлетво-рительно)**	**«4» (хорошо)**	**«5» (отлично)**
Работа выполнена в полном объеме. Отчет не оформлен и представлен. При защите отчетных материалов правильные ответы даны менее чем на 50 % включительно. Материал излагается непоследователь но, сбивчиво, не представляет определенной системы знаний по работе	Работа выполнена в полном объеме. Отчет оформлен и представлен. При защите отчетных материалов правильные ответы на 51–64 % вопросов. Допускаются нарушения в последовательнос ти изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи	Работа выполнена в полном объеме. Отчет оформлен и представлен. При защите отчетных материалов правильные ответы на 65–94 % вопросов. Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументирован-ный и доказательный характер	Работа выполнена в полном объеме. Отчет оформлен и представлен. При защите отчетных материалов правильные ответы даны на 95–100 % вопросов. Ответы на поставленные в билете вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстри-руются глубокие знания предмета

ЗАКЛЮЧЕНИЕ

Выполнение практических заданий по дисциплине «Теория анализа компьютерных атак» позволяет сформировать у студентов целостное представление о современных методах обнаружения, анализа и моделирования компьютерных атак на критически важные информационные системы. Восемь практических занятий охватывают полный цикл задач: от настройки систем обнаружения атак и применения методов вычислительного интеллекта до аналитического и имитационного моделирования процессов реализации угроз, оценки эффективности атак и активного противодействия.

Особенностью данного пособия является математическая формализация заданий: в каждом занятии присутствуют количественные модели – дифференциальные уравнения динамики атак, формулы расчёта коэффициента противодействия, метрики качества классификации (precision, recall, F1, AUC ROC), формулы рисков (ALE, SLE, ARO), коэффициенты информационного превосходства. Такой подход обеспечивает формирование у студентов навыков не только качественного, но и количественного анализа компьютерных атак, что соответствует современным требованиям к специалистам в области информационной безопасности.

В результате прохождения практикума студент овладевает навыками работы со свободно распространяемыми средствами защиты информации (Snort, Suricata, Zeek, Wireshark, scapy, Python–библиотеками машинного обучения), приобретает опыт проведения экспериментов на стендовом полигоне и интерпретации полученных результатов, а также осваивает методики анализа и регулирования рисков, связанные с реализацией нескольких угроз одновременно.

Полученные знания и навыки могут быть использованы при выполнении курсовых и выпускных квалификационных работ, а также в профессиональной деятельности специалистов по защите информации. Для углублённого изучения материала рекомендуется обратиться к монографиям С. М. Климова, М. П. Сычёва, А. В. Астрахова «Экспериментальная оценка противодействия компьютерным атакам на стендовом полигоне» и Е. В. Дойниковой, И. В. Котенко «Оценивание защищённости и выбор контрмер для управления кибербезопасностью», а также к нормативным документам в области защиты информации (ФЗ–149, ФЗ–152, ГОСТ Р 57580, серии NIST SP 800).

ЛИТЕРАТУРА

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) транзакций. Положения по безопасности финансовых транзакций.
4. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. – Gaithersburg: NIST, 2012. – 95 p.
5. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide. – Gaithersburg: NIST, 2012. – 79 p.
6. MITRE ATT&CK Framework [Электронный ресурс]. – URL: https://attack.mitre.org (дата обращения: 01.09.2026).
7. Климов, С. М. Экспериментальная оценка противодействия компьютерным атакам на стендовом полигоне / С. М. Климов, М. П. Сычёв, А. В. Астрахов. – Москва: Радиотехника, 2017. – 112 с.
8. Stallings, W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 7th ed. – Boston: Pearson, 2017. – 768 p.
9. Bishop, M. Computer Security: Art and Science / M. Bishop. – Boston: Addison-Wesley, 2019. – 1104 p.
10. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. – 3rd ed. – Hoboken: Wiley, 2020. – 1056 p
11. Дойникова, Е. В. Оценивание защищённости и выбор контрмер для управления кибербезопасностью: монография / Е. В. Дойникова, И. В. Котенко. – Москва: РАН, 2021. – 184 с.
12. Краковский, Ю. М. Методы и средства защиты информации: учеб. пособие для вузов / Ю. М. Краковский. – Санкт-Петербург: Лань, 2024. – 272 с.
13. Магазев, А. А. Противодействие сетевым атакам в локальных сетях: учеб. пособие / А. А. Магазев, М. В. Щерба, Е. В. Щерба. – Омск: ОмГТУ, 2021. – 119 с.
14. Подтопельный, В. В. Аудит информационной безопасности: учеб. пособие для студентов специальности 10.05.03 / В. В. Подтопельный. – Калининград: БГАРФ, 2023. – Ч. 1. – 171 с.
15. Баланов, А. Н. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 680 с.
16. Баланов, А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2025. – 280 с.

Локальный электронный методический материал

Подтопельный Владислав Владимирович

ТЕОРИЯ АНАЛИЗА КОМПЬЮТЕРНЫХ АТАК

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 4,6. Печ. л. 3,9.

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