

• Мониторинг системы - предназначен для визуального мониторинга выполнения в реальном времени MegaMatcher ABIS.

MegaMatcher ABIS API - это интерфейс на основе веб-сервисов (RESTful), разработанный для простой и быстрой интеграции со сторонними системами. Он обеспечивает все необходимые функции, включая управление идентификацией, вынесение решений и системное администрирование.

Список литературы :

1. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. – М.: МГТУ им. Н. Э. Баумана, 2016. – 252 с.
2. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности. – Санкт-Петербург: Питер, 2017. – 256 с.
3. Сесин Е.М. Системы идентификации личности, основанные на интеграции нескольких биометрических характеристик человека / Е.М. Сесин, В.М. Белов // Доклады ТУСУРа. – № 2(25), часть 2. – 2012. – С. 175-179.
4. Ручай А.Н. Текстозависимая верификация диктора: математическая модель, статистические исследования, комплекс программ. – Saarbrücken: LAP LAMBERT Academic Publishing, 2012. – 144 с.
5. Ушмаев О.С. Сервисно-ориентированный подход к разработке мультибиометрических технологий // Информатика и ее применения. – 2008. – Т. 2. Вып. 3. – С. 41-53.
6. <https://neurotechnology.co/sistema-de-identificacion-biometrica-automatizado-megamatcher/>

ИНТЕРАКТИВНОЕ ОБУЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Жомуродов Дустмурод Мамасолиевич, Баратов Жасур Рустамович

Джизакский филиал Национального университет Узбекистана,

dustmurod@jbnuu.uz, jasurjon2187@gmail.com

Аннотация: Анализируются современные методы обучения в области кибербезопасности, включая применение виртуальной и дополненной реальности, киберигры и тестирование на проникновение. Исследуются технологии VR/AR для создания интерактивных сценариев и виртуальных лабораторий, а также разработка приложений AR для обнаружения угроз. Описываются практические применения тестирования на проникновение в виртуальной среде. Представлены современные подходы к обучению и развитию навыков в области кибербезопасности.

Ключевые слова: кибербезопасность, виртуальная реальность (VR), Дополненная реальность (AR), тестирование на проникновение, киберигры, интерактивное обучение, виртуальные лаборатории, обнаружение угроз, технологии обучения, современные методы обучения, инновации в кибербезопасности, геймификация в обучении

В современном мире обучение в области кибербезопасности становится всё более критичным из-за сложности киберугроз. Использование современных технологий, включая виртуальную и дополненную реальность (VR и AR), открывает новые перспективы для инновационных методов обучения. Например, создание симуляций атак и защиты, виртуальных лабораторий и киберигр способствует эффективному обучению. Применение приложений AR позволяет обнаруживать угрозы в реальном времени, а тестирование на проникновение в виртуальной среде обеспечивает безопасный практический опыт.

Симуляции атак и защиты представляют собой важный метод обучения, который включает в себя следующие этапы:

Создание виртуальной среды: использование VR/AR для построения виртуальных сетевых инфраструктур, имитирующих реальные организации с серверами, устройствами и базами данных.

Сценарии атак и угроз: разработка разнообразных сценариев кибератак, включая атаки на сетевые узлы, социальную инженерию и фишинг, основанные на реальных ситуациях.

Обучение в реальном времени: студенты взаимодействуют с виртуальным пространством, сталкиваясь с ситуациями, требующими выявления и реагирования на киберугрозы.

Моменты обучения: предоставление моментов обучения в реальном времени, таких как предупреждения о подозрительной активности и анализ сетевого трафика, для предотвращения атак.

Оценка результатов: система автоматически оценивает реакции учащихся, предоставляя обратную связь и рекомендации для улучшения навыков.

Этот метод помогает студентам применять теоретические знания на практике, делая обучение более интересным и эмоционально вовлекающим. Существует множество онлайн-платформ и симуляторов для обучения кибербезопасности, предлагающих различные сценарии атак и защиты, а также практические задания в реальном времени.

TryHackMe (<https://tryhackme.com/>): бесплатная платформа с интерактивными уроками, заданиями и лабораториями для практики навыков в реальном времени. Очки зарабатываются за выполнение заданий.

Kaspersky Interactive Protection Simulation (KIPS): интерактивная командная игра от Лаборатории Касперского для топ-менеджеров, где противостоят атакам и учатся методам защиты (https://www.kaspersky.ru/about/press-releases/2023_laboratoriya-kasperskogo-obnovila-svoyu-onlajn-igru-pro-kiberbezopasnost).

Blue Team vs. Red Team Simulator: стратегический симулятор, где команды Синих (безопасники) и Красных (хакеры) соревнуются. Игра возможна как против ИИ, так и с другими игроками по сети:

(<https://habr.com/ru/companies/timeweb/articles/646551/>).

Модель угроз виртуальной среды: пусть V обозначает виртуальную среду, A - множество возможных атак, а D - множество возможных защитных мер. Тогда можно представить модель угроз как тройку (V, A, D) , где, варьируя состав A и D , мы моделируем различные сценарии атак и защиты.

Модель реакции на атаки: пусть $R(a, d)$ представляет собой функцию реакции на атаку a при использовании защитной меры d . Тогда мы можем определить эффективность защиты как $E(d) = \sum_{a \in A} R(a, d)$, где сумма берется по всем возможным атакам.

Модель оценки результатов: пусть S обозначает систему оценки реакций учащихся на сценарии атак. Мы можем определить функцию оценки как $F(s)$, где s представляет собой результаты реакции учащихся на симуляции атак.

Эти модели помогают количественно оценить эффективность обучения и анализировать результаты студентов, что позволяет улучшать процесс обучения кибербезопасности.

Обучение через взаимодействие в VR и AR использует виртуальную и дополненную реальность для создания интерактивных сценариев обучения кибербезопасности. Виртуальное пространство разрабатывается для имитации офисов, центров обработки данных и других сценариев, где учащиеся взаимодействуют с элементами среды, анализируют уязвимости, обучаются реагировать на кибератаки и получают обратную связь о своих действиях. Многопользовательское взаимодействие способствует коллективному обучению. Этот метод активизирует участие студентов, что обеспечивает более глубокое усвоение материала.

Виртуальные лаборатории в обучении кибербезопасности используют технологии VR и AR для практических упражнений по настройке сетевых устройств и

анализу трафика. Создается виртуальное пространство с устройствами, такими как серверы, маршрутизаторы и IoT. Учащиеся настраивают устройства, анализируют трафик и внедряют системы безопасности. Это дает возможность применять теоретические знания на практике без риска повреждения реальной инфраструктуры. Обратная связь системы помогает улучшать навыки студентов. Виртуальные лаборатории предоставляют более доступный и масштабируемый способ обучения, чем традиционные лаборатории.

Создание киберигр в обучении кибербезопасности – метод, использующий игровые элементы и виртуальное окружение. Этот подход включает:

Разработку виртуального мира: создание игрового окружения, отражающего сетевые структуры или офисные пространства.

Задачи и миссии: внутри виртуального мира создаются различные задачи, включая анализ уязвимостей и обнаружение вредоносных программ.

Интерактивные головоломки и сценарии: Игроки взаимодействуют с виртуальным миром, решая головоломки, выполняя задания и применяя навыки кибербезопасности, например, анализируя логи, осуществляя атаки на системы или разрабатывая стратегии защиты.

Эволюция процесса: киберигры могут развиваться по мере продвижения игрока, повышая сложность задач и уровни, что стимулирует постоянное обучение и развитие навыков.

Соревновательный и кооперативный режимы: игроки могут сражаться друг с другом для проверки своих навыков или сотрудничать в решении сложных задач безопасности.

Обратная связь и статистика: система предоставляет обратную связь об успехах и ошибках игроков, а также статистику их прогресса.

Реальные сценарии и угрозы: игры используют реальные сценарии и угрозы, приближая опыт к реальным ситуациям в области кибербезопасности.

Стимулирующее обучающее окружение: Этот метод обучения создает захватывающее окружение, повышая мотивацию и развивая навыки в области кибербезопасности.

Аугментированная реальность (AR) применяется в кибербезопасности для обнаружения угроз в реальном времени. Вот как это работает:

Разработка AR-приложений: создаются приложения AR для мобильных и других устройств, добавляющие виртуальные элементы через камеру.

Сканирование объектов: Приложения сканируют физические объекты, такие как комнаты или серверные стойки, с использованием камеры и датчиков.

Обнаружение угроз и уязвимостей: AR-приложения находят уязвимости, открытые порты и несанкционированные устройства в отсканированных объектах.

Предоставление информации: Информация об угрозах выводится на экран устройства в реальном времени, с возможностью взаимодействия для получения дополнительных рекомендаций.

Обучение и логирование: Пользователи получают обучение по обнаружению и устранению угроз, а также ведется логирование для анализа и улучшения системы.

Этот метод позволяет студентам и специалистам по кибербезопасности практиковаться в обнаружении угроз в реальных сценариях.

Тестирование на проникновение в виртуальной среде — это метод обучения, который включает в себя проведение pen testing в виртуальной среде для приобретения опыта в обнаружении и устранении уязвимостей. Процесс включает следующие шаги:

Создание виртуальной среды: разработчики создают виртуальное окружение, имитирующее реальную инфраструктуру организации.

Выбор целей тестирования: определяются системы и приложения, подвергаемые атакам для проверки на наличие уязвимостей.

Проведение тестов на проникновение: эксперты по кибербезопасности или учащиеся проводят тесты, используя аналогичные реальным сценариям техники.

Обнаружение угроз: в процессе тестирования выявляются угрозы и уязвимости, такие как нарушения безопасности и несанкционированный доступ к данным.

Устранение уязвимостей: после обнаружения уязвимостей приступают к их устранению, включая обновление программного обеспечения и настройку брандмауэров.

Логирование и анализ результатов: Результаты тестирования логируются и анализируются для выявления обнаруженных угроз и разработки рекомендаций по улучшению безопасности.

Обратная связь и улучшение: Эксперты или учащиеся получают обратную связь для дальнейшего совершенствования своих навыков.

Этот метод обучения предоставляет практический опыт, аналогичный реальным сценариям, и способствует развитию навыков в области кибербезопасности. Современные технологии, такие как виртуальная и дополненная реальность, киберигры и тестирование на проникновение в виртуальной среде, обогащают обучение, предоставляя студентам и профессионалам реальные сценарии для применения знаний и навыков. Однако необходимо учитывать безопасность обучения и оценивать эффективность методов в цифровую эпоху, требующую постоянного обновления и совершенствования подходов к борьбе с киберугрозами.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Xolbutayevich T. O., Mamasoliyevich J. D. O‘QUV JARAYONIDA TO‘LDIRILGAN REALLIK TEXNOLOGIYALARIDAN FOYDALANISH //International Journal of Contemporary Scientific and Technical Research. – 2022. – С. 334-338.
2. Abdumo‘minovich S. A., Xolbutayevich T. O., Mamasoliyevich J. D. To‘ldirilgan reallik sun’iy intellekt bilan kelajak texnologiyasiga aylanmoqda //International Journal of Contemporary Scientific and Technical Research. – 2022. – С. 187-190.
3. Jomurodov D., Meliyeva M. THE ADVANTAGES OF IMPLEMENTING AUTOMATED SYSTEMS IN COMPUTER SCIENCE LEARNING //International Scientific and Practical Conference on Algorithms and Current Problems of Programming. – 2023.
4. Тангиров Х. Э., Жомуродов Д. М., Муродкосимова Ш. Х. АХБОРОТ-ТАЪЛИМ МУҲИТИДА ЎҚИТИШНИ ИНДИВИДУАЛЛАШТИРИШНИНГ МУҲИМ ЖИҲАТЛАРИ //инновации в педагогике и психологии. – 2021. – Т. 4. – №. 6.
5. Zhomurodov D., Ulashev A., Tozhiyev A. THE SYSTEM FOR DETERMINING THE QUALIFICATIONS OF INDUSTRY EXPERTS //Евразийский журнал академических исследований. – 2023. – Т. 3. – №. 4 Special Issue. – С. 280-289.
6. Жомуродов Д., Мелиева М. ИННОВАЦИИ В ОБУЧЕНИИ: НОВЫЕ ПОДХОДЫ К РАБОТЕ С МАССИВАМИ В ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММАХ //Uz-Conferences. – 2023. – Т. 1. – №. 1. – С. 867-872.
7. Kayumov O. et al. ELECTRONIC PLATFORM FOR RECOGNITION AND TEACHING OF SIGN LANGUAGE PICTURES BASED ON UZBEK GRAMMAR //International Journal of Contemporary Scientific and Technical Research. – 2023. – С. 263-268.

ОПТИМИЗАЦИЯ И УЛУЧШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ АЛГОРИТМА ШИФРОВАНИЯ BLOWFISH

Жомуродов Дустмурод Мамасолиевич, Баратов Жасур Рустамович

Джизакский филиал Национального университет Узбекистана,

dustmurod@jbnuu.uz, jasurjon2187@gmail.com

Аннотация: Статья представляет всестороннее исследование методов оптимизации и повышения производительности алгоритма шифрования Blowfish. Применение стратегий оптимизации, таких как оптимизация S-box, алгоритмическая оптимизация и оптимизация таблицы ключей, демонстрируется в контексте повышения безопасности и эффективности S-box, что улучшает общую безопасность алгоритма. Эмпирические оценки и анализ безопасности подтверждают эффективность этих методов в повышении эффективности и надежности Blowfish для современных криптографических приложений.

Ключевые слова: Алгоритм Blowfish, шифрование, криптография, оптимизация, эффективность, криптографические атаки.

Алгоритм шифрования Blowfish является краеугольным камнем в области блочных шифров с симметричным ключом, обеспечивая баланс между безопасностью и производительностью. Однако с развитием вычислительных ресурсов традиционные алгоритмы шифрования с трудом удовлетворяют требованиям современных приложений. В данной статье основное внимание уделяется изучению методов оптимизации и улучшению таблиц S-box для повышения производительности алгоритма Blowfish при сохранении гарантий безопасности.

Алгоритм шифрования Blowfish работает с блоками данных по 64 бита и поддерживает ключи длиной от 32 до 448 бит. Он осуществляет шифрование и расшифровку, используя структуру Фейстеля и зависит от S-блоков. Несмотря на эффективность, этот алгоритм становится уязвимым для атак с течением времени, не отвечая требованиям современных криптографических приложений [4].

Алгоритм состоит из двух основных этапов: расширение ключа и шифрование информации. На этапе расширения ключа исходный ключ (длиной до 448 бит) дополняется 18 нижними к ключам по 32 бита и преобразуется в 4 собственных 32-битных S-блока. Общий размер расширенных ключей составляет $(18 + 256 * 4) * 32 = 33344$ бита или 4168 байт, что обеспечивает достаточную организацию данных.

Параметры:

- Скрытый ключ K (от 32 до 448 бит);
- 32-битные ключи шифрования $(P_1, \dots, P_{18})$;
- 32-битные таблицы подстановки (S_1, S_2, S_3, S_4) S – box:
 $S_1[0], S_1[1], \dots, S_1[255]; \quad S_2[0], S_2[1], \dots, S_2[255];$
 $S_3[0], S_3[1], \dots, S_3[255]; \quad S_4[0], S_4[1], \dots, S_4[255].$

Специальный символ « $\oplus$ », изображенный на рисунке 1, обозначает операцию XOR (исключающее ИЛИ), а символ « $\boxplus$ » обозначает метод простого сложения. В случае, если