Инженерный вестник Дона, №7 (2025)
ivdon.ru/ru/magazine/archive/n7y2025/10229

Платформа для обмана злоумышленника - критерии её функциональности, сильные и слабые стороны, тренды

А.М. Тихонов

Финансовый университет при правительстве Российской Федерации

Аннотация: Цель статьи – произвести обзор критериев, которые влияют на функциональность платформы для обмана злоумышленников (Deception platform), выявить сильные и слабые стороны технологии, рассмотреть текущие тренды и зоны для проведения дальнейших исследований. Метод изучения - анализ существующих статей в рецензируемых российских и зарубежных источниках, агрегация исследований, формирование выводов исходя из проанализированных источников. В статье рассматриваются основные и ситуативные метрики, на которые стоит обращать внимание при выборе и оценки ловушки – стоимость внедрения, сложность проектирования, риск компрометации, собранные данные, сила обмана, доступные соединения, коэффициент ложных срабатываний, атрибуция атаки, сложность атаки, время до компрометации, разнообразие взаимодействий, ранее предупреждение, эффективность отражения атак, влияние на поведение атакующего, угрозы, выявленные с помощью ловушки, устойчивость. Приведен разбор сильных и слабых сторон технологии Deception, на которые стоит обращать внимание при её использовании. Проведен обзор трендов развития Deception-платформ, а также областей исследования, в которых платформа недостаточно изучена.
Ключевые слова: инфраструктура ложных целей, ловушки, приманки, платформа для обмана злоумышленника, сеть ловушек.

Введение

В настоящее время объем информации, обрабатываемой организациями, продолжает постоянно расти. Вместе с этим, количество и вариативность атак, направленных на такие организации, продолжает также увеличиваться. Регулярно в новостях мы сталкиваемся с информацией об утечке персональных данных, которые были похищены из очередной компании. Злоумышленники все чаще прибегают к использованию хорошо спланированных атак, направленных против конкретной жертвы-организации, они могут находиться внутри неё длительное время, регулярно улучшая для себя плацдарм для проведения эффективной атаки. Одним из средств борьбы с такими типами атак является платформа для обмана злоумышленника (Deception platform) – это централизованно управляемые системы для организаций, предназначенные для создания, распространения и

управления всей обманчивой средой и связанными с ней архитектурными элементами, которые часто виртуализируются и по существу неотличимы от реальных активов и используются в качестве приманки для привлечения и обнаружения злоумышленника [1]. По сути, технология Deception Platform является прямым продолжением идеи технологии размещения ловушек (Honeypot), но включает в себя не только ловушки, но и приманки, центр управления и разворачивания по всей инфраструктуре, а также возможность мониторинга всех ложных активов в едином месте. Для ознакомления с технологией автор рекомендует к прочтению статью «Обзор технологий для обмана злоумышленника (ловушки, приманки, перемещение целей, платформа обмана), их классификация и взаимодействие» [2], в текущей статье будут рассмотрены критерии функциональности Deception платформы, её сильные и слабые стороны, а также тренды и зоны для будущих исследований.

Критерии функциональности

Для того чтобы понять, насколько эффективно будет работать платформа Deception, необходимо выявить её основные метрики функциональности. Поскольку основными её элементами являются ловушки и приманки, а обман злоумышленника в первую очередь строится именно на ловушках (Honeypot), постольку необходимо выявить основные критерии функциональности ловушек (Рис. 1):

1. Стоимость внедрения. Эта метрика количественно оценивает стоимость внедрения ловушки, рассматривая её с точки зрения требуемых вычислительных ресурсов. Эта метрика является важной особенно для организаций, которые имеют ограниченные вычислительные мощности для внедрения решения [3]. При применении коммерческих решений также важно учитывать стоимость лицензии, внедрения и поддержки ловушки.

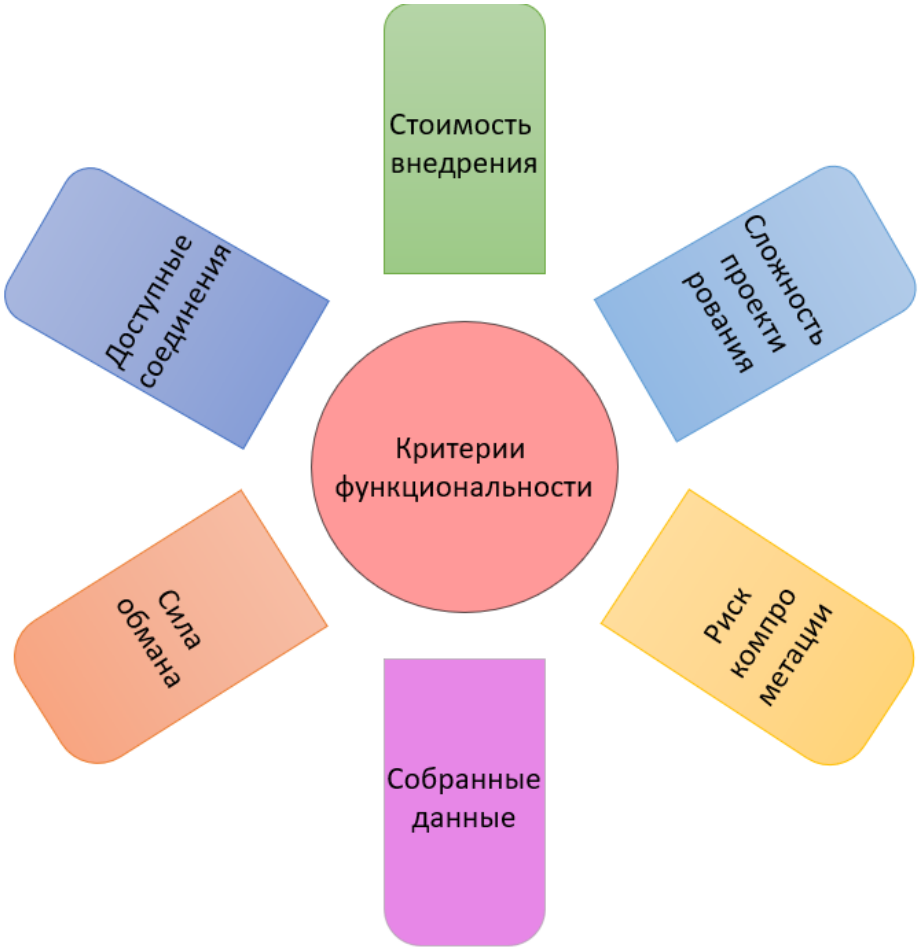

Рис. 1. – Основные критерии функциональности

2. Сложность проектирования. Эта метрика определяет сложность на этапе проектирования алгоритмов, необходимых для работы ловушки. Ловушки с более высоким показателем требуют серьезных усилий и большего количества времени на этапе проектирования [4]. Это время также влияет на общие сроки внедрения проекта, его сложность и стоимость.

3. Риск компрометации. Этот показатель оценивает уровень риска, который возникает при компрометации ловушки злоумышленником [5]. Эта метрика наиболее влиятельной выступает при построении сети ловушек около критически важных активов организации. Чем ниже этот показатель, тем ниже риски и выше шансы защитить ценные активы.

4. Собранные данные. Метрика количественно оценивает объем данных (качество и полноту), собираемых ловушкой во время её работы.

Команде защиты следует сфокусировать свое внимание на ловушках, которые собирают как можно больше данных о злоумышленниках, зачастую именно они будут наиболее эффективны [6]. Исключения могут составлять те случаи, когда для тщательного изучения злоумышленника требуется использовать ловушку с высоким уровнем взаимодействия. Такая ловушка соберет больше данных, но, если злоумышленник имеет высокий уровень подготовки и хороший набор средств, вероятно, он сможет получить доступ над ловушкой и продолжить свою атаку, используя её как плацдарм для развития.

5. Сила обмана. Метрика показывает эффективность механизмов обмана ловушки. Чем дольше злоумышленник будет думать, что взаимодействует с реальным активом, тем лучше. Оценка силы обмана имеет решающее значение для определения способности ловушки эффективно обманывать и отвлекать злоумышленников. Некоторые ловушки могут быть просты с точки зрения их внедрения и настройки, но, к сожалению, как правило такие ловушки проще выявляются злоумышленником [7]. Чтобы создать ловушки, обладающие высокой силой обмана, можно использовать методику маскировки ловушек под реальные активы. Зачастую эффективность таких ловушек может быть увеличена при использовании сети honeynet, состоящей из хорошо замаскированных ловушек honeypot.

6. Доступные соединения. Эта метрика измеряет количество соединений, с которыми ловушка должна активно взаимодействовать. Эта метрика начинает играть роль в тот момент, когда имеется определенная пропускная способность в сети или другие ограничения, связанные с ресурсами. Выбор ловушки с высоким значением этого параметра гарантирует, что она будет работать оптимально в рамках ограничений сети [8].

Эти метрики функциональности обеспечивают структурированную

основу для оценки и выбора наиболее подходящего типа ловушек, основываясь на конкретных сетевых параметрах, целях и имеющихся ресурсах. Та платформа Deception будет работать лучше, ловушки и приманки в которой будут более функциональными.

Существует еще ряд критериев, которые можно ситуативно вводить для оценки качества работы ловушек и приманок, они приведены ниже:

1) Коэффициент ложных срабатываний. Коэффициент ложных срабатываний определяет частоту, с которой легитимные пользователи сети, не относящиеся к команде защиты, взаимодействуют с ловушками и вызывают их срабатывание. Минимизация этого коэффициента поможет ловушкам не мешать нормальной работе организации, команда защиты сможет сфокусироваться на реально важных инцидентах безопасности [9].

2) Атрибуция атаки. Атрибуция атаки количественно определяет, насколько точно ловушка выявляет происхождение атаки и личность злоумышленника. Чем лучше атрибуция, тем более ценная и точная информация может быть получена о месторасположении злоумышленника, его связях и мотивах [10].

3) Сложность атаки. Эта метрика измеряет, насколько сложной была атака, направленная на ловушку. Чем сложнее проводимая атака, тем, скорее всего, выше уровень подготовки у злоумышленника, тем может быть более ценно его взаимодействие с ловушками. Его взаимодействие с ловушкой может сообщить нам о качестве нашей ловушки [11].

4) Время до компрометации. Эта метрика отражает время, которое потребуется злоумышленнику для взлома защиты ловушки. Чем дольше ловушка способна противостоять компрометации, тем больший объем сведений о злоумышленнике и времени для его идентификации, анализа действий и реагирования на вторжение будет у команды защиты. Вместе с этим, чем дольше злоумышленник будет взаимодействовать с ловушкой, тем

меньше времени у него будет на взаимодействие с ценным активом, тем больший потенциал своей атаки он раскроет, тем яснее станут его намерения команде защиты [12].

5) Разнообразие взаимодействий. Разнообразие взаимодействий оценивает вариативность способов взаимодействия злоумышленников с ловушкой. Чем больший набор доступных взаимодействий предоставляет ловушка, тем больше она может становиться похожей на реальный актив, и тем больший спектр атак на ней сможет реализовать злоумышленник [13].

6) Раннее предупреждение. Метрика раннее предупреждение измеряет, насколько быстро ловушка обнаружит злоумышленника и оповестит о нем команду защиты. Чем быстрее это произойдет, тем больше будет времени для противодействия атаке [14].

7) Эффективность отражения атак. Эта метрика показывает, насколько хорошо ловушка переводит фокус злоумышленников с реальных активов организации на ложные. Чем выше эта метрика, тем меньше вероятность взаимодействия злоумышленника с реальным активом, тем выше уровень защиты в сети [15].

8) Влияние на поведение атакующего. Эта метрика оценивает влияние на поведение атакующего, оценивает то, изменил ли он свою тактику, стратегию или методы после встречи с ловушкой. Выявление изменений в поведении атакующего может сигнализировать команде защиты об адаптации стратегии злоумышленника и о развивающихся угрозах [16].

9) Угрозы, выявленные с помощью ловушки. Этот параметр определяет, какое количество угроз может выявить ловушка при взаимодействии с злоумышленником и какое количество этих выявленных угроз могут быть применимы к реальной сети [17].

10) Устойчивость. Оценивает способность ловушки противодействовать атакам при этом не раскрывая себя. Чем более устойчива

ловушка к большему спектру атак злоумышленника, тем дольше она сможет проработать, и, возможно, обманывать злоумышленника [18].

Стоит отметить, что единой системы оценивания ловушек на текущий момент нет, авторы исследований приводят отдельные характеристики как ключевые при выборе ловушек. В этой сфере остается место для исследования и создания комплексной модели, которая поможет определять веса указанных выше функциональных характеристик в зависимости от задач и поможет с итоговым выбором ловушек.

Сильные и слабые стороны технологии Deception

Как и у любой технологии, у Deception платформ (в состав которых входят ловушки, приманки и может входить технология перемещения целей) есть свои сильные и слабые стороны.

Сильные стороны технологии:

1) Раннее обнаружение. Технология позволяет выявлять злоумышленника еще на ранних этапах его атаки, если ловушки и приманки расставлены корректно в сети [19].

2) Уменьшение количества ложных срабатываний. Deception система получает оповещение об инциденте в том случае, если кто-то взаимодействовал с ловушкой или приманкой. На деле же это происходит крайне редко так как ложные активы спрятаны от обычных пользователей, благодаря чему они не взаимодействуют [20].

3) Все предоставляемые данные ценны. Преимущество является логическим продолжением прошлого пункта так как практически не бывает ложных срабатываний, а все данные собираются о реальной атаке.

4) Предоставление большего количества сведений об атаке. Технология позволяет получить информацию о проводимой атаке, если злоумышленник раскроет свой потенциал на ловушке или приманке [21].

5) Запутывание инфраструктуры. С применением техник перемещения ловушки и приманки в сети могут меняться местами с реальными активами, в результате чего злоумышленник может быть сбит с толку и потратит значительно больше времени на то, чтобы добраться до целевого актива [22].

6) Создание ложной сети (honeynet), в которой будут располагаться только ловушки. При высокой степени подготовки и применении техник маскирования ловушек, поддельную сеть будет сложно отличить от реальной. Попав туда, злоумышленник может потратить огромное количество времени, чтобы догадаться, что он находится в ловушке, при этом передав о себе команде защиты много ценной информации [7].

7) Активная защита. Команда защиты строит проактивную защиту, навязывая сценарий развития атаки злоумышленнику. Таким образом инициатива может оставаться в руках команды защиты [17].

Слабые стороны технологии:

1) Сложность внедрения. Если речь идет о сложной сети и большом составе ловушек и приманок, то может быть сложно проработать на начальном этапе корректный состав и расположение элементов обмана, а также перемещения активов в сети [7].

2) Риск разоблачения. В случае, если ловушки и приманки в сети используются однородные, то есть в большей степени похожие друг на друга, то распознав одну ловушку и найдя её основные отличительные характеристики в сети, злоумышленник сможет их обходить. Побороться с этим можно с помощью использования неоднородных ловушек и приманок [5].

3) Риск не встретиться с злоумышленником. Если в каждом сегменте сети используются ловушки и приманки, есть шанс, что злоумышленник минует их. Таким образом мы не узнаем о проводимой атаке. Уменьшить этот риск возможно на этапе внедрения Deception платформы, где

необходимо рассчитать вероятность встречи злоумышленника с ложным активом за определенное количество его прыжков по сети. Исходя из этого расчета, можно выявить необходимое и достаточное количество ловушек и приманок [21].

4) Риск неправильной конфигурации. Неправильная настройка платформы Deception и её составляющих может привести к тому, что злоумышленник легко обнаружит наличие ловушек и приманок в сети, начнет действовать осторожнее, не взаимодействуя с ними [21].

5) Риск использования ловушек неправильного вида. Если в сети рядом с важным активом расставить ловушки с большим потенциалом взаимодействия, то есть вероятность, что злоумышленник, проведя на них атаку, сможет их использовать в качестве плацдарма для развития следующих атак. И наоборот – расставлять ловушки, с которыми практически невозможно взаимодействовать, далеко от ключевых активов не позволит команде защиты собрать достаточное количество ценной информации об атаке [23].

Тренды и области исследования

С учетом развития искусственного интеллекта, облачных технологий и роста объема данных, тенденции в развитии технологии могут быть следующие:

1) Подключение искусственного интеллекта для построения инфраструктуры ложных целей и выработка им корректных паттернов поведения на атаки различных видов благодаря собранным данным в единой базе данных безопасности. На зарубежных рынках такими базами данных (озерами данных) могут стать массивные хранилища от AWS, Google, IBM, Snowflake [24].

2) С учетом развития облачных технологий и растущей тенденции

частичного размещения инфраструктуры в облаке, появляется потребность в создании качественных ловушек и приманок, которые смогли бы защитить качественно облачные активы, при этом не требуя значительных вычислительных мощностей. Тенденция развития технологии обмана в этой сфере не нова, технология развивается в этом направлении несколько лет. Дополнительно, может потребоваться предоставление Deception как сервиса, который будет использовать облачные вычислительные мощности, быстрее разворачиваться и меньше стоить, благодаря чему технология станет доступна большему количеству организаций [24].

3) Увеличение интеграционных взаимодействий с другими системами. Реализация интеграционных взаимодействий с системами управления активами, системам управления уязвимостями, системам управления поверхностью атаки, управлению состоянием безопасности облака и другими позволит системам обмана получить более полную картину инфраструктуры организации и более эффективно использовать технологию обмана [25].

4) Использование искусственного интеллекта для анализа текущей инфраструктуры и активов организации с целью создания максимально схожей ложной инфраструктуры. Искусственный интеллект сможет помочь создать ловушки (поддельные активы и сервисы), приманки (поддельные файлы), синтетический сетевой трафик [26].

Из областей исследования, в которых технология Deception недостаточно изучена, можно выделить следующие:

1) Использование искусственного интеллекта для создания ловушек, приманок и сетевого трафика, схожих с настоящими активами, файлами и трафиком.

2) Исходя из расширяющегося количества вариантов различных ловушек и приманок, неосвещенной остается область исследования по определению их оптимального состава и количества для организаций разных

размеров.

3) Несмотря на то, что в сфере увеличения эффективности влияния ловушек и приманок на защищенность сети было написано немало работ [27], тем не менее еще есть место для улучшений, в связи с новыми создаваемыми угрозами.

4) Создание комплексной оценки эффективности ловушек, в соответствии с которой можно было бы выбрать наиболее функциональную ловушку корректного вида. Требуется модель, с помощью которой можно будет делать корректное сравнение ловушек, а также описанная пошаговая методика сравнения.

5) Изучение пользы от интеграционных взаимодействий различных решений (включая Deception платформу), описание выгоды использования комплекса решений, новые подходы по обеспечению безопасности сети с помощью комплекса проинтегрированных решений.

6) В основном исследования в области Deception и Honeypot базировались на модели Cyber Kill Chain для описания этапов развития атаки и противодействия ей. Работ по использованию MITRE ATT&CK для создания защиты с применением технологии обмана злоумышленника, несмотря на её популярность и ценность, мало, в этой сфере требуются дополнительные исследования.

Заключение

В результате исследования были выявлены и разобраны основные критерии функциональности платформы. Различные авторы статей, ссылки на работы которых были указаны выше, фокусируются в основном на конкретных критериях функциональности, но не предлагают комплексную оценку функциональности платформы, благодаря которой можно было бы

объективно выбрать наиболее подходящую платформу под большой спектр задач. Тем не менее, эти критерии можно разнести на 2 категории – основные и ситуативные. С учетом определения основных функциональных критериев, появляется возможность создания модели или методики, целью которой будет совместить в себе существующие критерии и присвоить им определенные коэффициенты в зависимости от поставленной задачи и важности самого критерия.

При сравнении плюсов и минусов использования технологии можно сделать следующий вывод – технология способна обнаруживать, запутывать и противодействовать злоумышленнику, который находится внутри сети. Тем не менее, технология является требовательной к тщательному выбору ловушек и приманок, их функциональным и техническим особенностям, регулярной поддержке и качественному мониторингу. Внедрять её стоит в том случае, если компания готова нарабатывать внутри себя компетенции в сфере Deception технологий и активно их применять. В противном случае, платформа обмана либо не поможет команде защиты, если злоумышленник не столкнется или обойдет ловушки, либо вовсе может стать плацдармом для развития атаки.

Текущие тренды показывают активное развитие технологии Deception, она идет в ногу с остальными технологиями в сфере IT. Потенциально наиболее вероятные и интересные тренды её развития связаны с применением в облачных инфраструктурах и использовании продвинутого искусственного интеллекта для генерации ловушек и приманок, распределению их по инфраструктуре, подсовыванию злоумышленнику ложных активов. Также технология может развиваться благодаря проведению различных интеграций с существующими решениями информационной безопасности. Вместе с развитием технологии, требуется и проведение её тщательного исследования, например в сфере применения

искусственного интеллекта, создания комплексной оценки эффективности ловушек, упрощения технологии для возможности использования компаниями малого и среднего размеров.

Литература

1. Путято М.М., Макарян А.С., Чич Ш. М., Маркова В.К. Исследование применения технологии Deception для предотвращения угроз кибербезопасности // Прикаспийский журнал: управление и высокие технологии, 2020, № 4 (52), С. 85-98. EDN: QXGGTW. DOI: doi.org/10.21672/2074-1707.2020.52.4.085-098

2. Тихонов А.М. Обзор технологий для обмана злоумышленника (ловушки, приманки, перемещение целей, платформа обмана), их классификация и взаимодействие // Инженерный вестник Дона, 2024. №11. URL: ivdon.ru/ru/magazine/archive/n11y2024/9651

3. Voris J., Jermyn J., Keromytis A. D., Stolfo S. J. Bait and Snitch: Defending Computer Systems with Decoys // in Proceedings of the Cyber Infrastructure Protection Conference, Strategic Studies Institute, 2013, С. 25. DOI: doi.org/10.7916/D8RN3H9SЫ

4. Almeshekah M.H., Spafford E.H. Cyber security deception // Cyber Deception, Springer, 2016, p. 25-52 DOI: doi.org/10.1007/978-3-319-32699-3_2

5. Anwar A.H., Kamhoua C.A. Honeypot Allocation for Cyber Deception under Uncertainty // IEEE Transactions on Network and Service Management Volume 19, Issue 3, 2022, С. 3438-3452. DOI: doi.org/10.1109/TNSM.2022.3179965

6. Ayeni O., Alese B., Omotosho L. Design and implementation of a medium interaction honeypot // International Journal of Computer Applications., Volume 70, 2013, №20, DOI: dx.doi.org/10.5120/12197-8136

7. Bilinski, M., Gabrys, R. Optimal placement of honeypots for network defense // 9th International Conference on Decision and Game Theory for Security,

Volume 11199 LNCS, 2018, С. 115-126. DOI: dx.doi.org/10.1007/978-3-030-01554-1_7

8. Bringer M.L., Chelmecki C.A. Recent advances and future trends in honeypot research // International Journal of Computer Network and Information Security, Volume 4, 2012, № 10, С. 63. DOI: dx.doi.org/10.5815/ijcnis.2012.10.07

9. Ochiai H., Honeyboost: Boosting honeypot performance with data fusion and anomaly detection // Expert Systems with Applications, Volume 201, September 2022, № 117073. DOI: doi.org/10.1016/j.eswa.2022.117073

10. Neal C. Attacker Attribution via Characteristics Inference Using Honeypot Data // 16th International Conference on Network and System Security, 2022, С. 155-169. DOI: dx.doi.org/10.1007/978-3-031-23020-2_9

11. Yuan J., Yang H., Kong Y. A highly interactive honeypot-based approach to network threat management // Future Internet, Volume 15, 2023, № 4, С. 127. DOI: doi.org/10.3390/fi15040127

12. Lim C., Budiarto E., Hobert K. Enhancing Cyber Attribution through Behavior Similarity Detection on Linux Shell Honeypots with ATT&CK Framework // 1st IEEE International Conference on Cryptography, Informatics, and Cybersecurity, 2023, С. 139-144. DOI: doi.org/10.1109/ICoCICs58778.2023.10276639

13. Pedersen J.M., Srinivasa S. Interaction matters: a comprehensive analysis and a dataset of hybrid IoT/OT honeypots // 38th Annual Computer Security Applications Conference, 2022, С. 742-755. DOI: doi.org/10.1145/3564625.3564645

14. Salimova H.R., A virtual honeypot framework // Central Asian Research Journal for Interdisciplinary Studies, Volume 2, Issue 5, 2022, С. 479-486.

15. Yamin M.M., Katt B. Use of cyber attack and defense agents in cyber ranges: A case study // Computers & Security, Volume 122, 2022, C. 102892, DOI: doi.org/10.1016/j.cose.2022.102892

16. Liu G., Ou X., Singhal A., Tabari A.Z. Revealing human attacker behaviors using an adaptive Internet of things honeypot ecosystem // 19ep IFIP International Conference on Digital Forensics, 2023, C. 73-90. DOI: dx.doi.org/10.1007/978-3-031-42991-0_5

17. Eng S., How K.C., Zhu Y. Honeypot for cybersecurity threat intelligence // Conference on Science, Engineering and Technology, 2023, C. 587-598.

18. Alissa K., Alqahtani M., Faiz T., Alyas T. Multi-cloud integration security framework using honeypots // Mobile Information Systems, 2022, C. 1-13. DOI: doi.org/10.1155/2022/2600712

19. Конкин Ю.В. Анализ особенностей построения систем защиты информации от несанкционированного доступа на основе ложных информационных систем // VII Международный научно-технический форум СТНО-2024. Сборник трудов. Том 3, С. 167-171. EDN: UZZJOA

20. Javadpour A. Dmaidps: a distributed multi-agent intrusion detection and prevention system for cloud iot environments // Cluster Computing, February Volume 26, Issue 1, 2023, C. 367-384 DOI: doi.org/10.1007/s10586-022-03621-3

21. Тихонов А.М. Платформа для создания распределенной инфраструктуры ложных целей как часть эшелонированной системы защиты // Известия Института Инженерной Физики, 2024, №3, С. 65-71 EDN: QSVNKO

22. Соколовский С.П. Moving target defense for securing Distributed Information Systems // Информатика: проблемы, методология, технологии, Сборник материалов XIX международной научно-методической конференции, 2019, С.639-643 EDN: ZFDMBF

23. Yuan J., Yang H., Kong Y. A highly interactive honeypot-based approach to network threat management // Future Internet, Volume 15, 2023, № 4, C. 127. DOI: doi.org/10.3390/fi15040127

24. «Deception technology use to grow in 2024 and proliferate in 2025» URL: csoonline.com/article/1246065/deception-technology-use-to-grow-in-2024-and-proliferate-in-2025.html (Дата обращения 18.05.2025)

25. Javadpour A., Taleb T., Ja'Fari F., A comprehensive survey on cyber deception techniques to improve honeypot performance // Computers & Security, Volume 140, 2024, №103792, DOI: doi.org/10.1016/j.cose.2024.103792

26. Onyekware U. Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey // Journal of Information Security, 2021, C. 250-269. DOI: doi.org/10.4236/jis.2021.124014

27. Zhang Li, Thing L. Three Decades of Deception Techniques in Active Cyber Defense - Retrospect and Outlook // Computers & Security, Volume 106, 2021, C. 102288, DOI: doi.org/10.1016/j.cose.2021.102288

References

1. Putjato M.M., Makarjan A.S., Chich Sh. M., Markova V.K. Prikaspijskij zhurnal: upravlenie i vysokie tehnologii, 2020, № 4 (52), EDN: QXGGTW. DOI: doi.org/10.21672/2074-1707.2020.52.4.085-098

2. Tihonov A.M. Inzhenernyj vestnik Dona, 2024, №11 URL: ivdon.ru/ru/magazine/archive/n11y2024/9651

3. Voris J., Jermyn J., Keromytis A. D., Proceedings of the Cyber Infrastructure Protection Conference, Strategic Studies Institute, 2013, pp. 25. DOI: doi.org/10.7916/D8RN3H9SЫ

4. Almeshekah M.H., Spafford E.H. Cyber Deception, Springer, 2016, pp. 25-52 DOI: doi.org/10.1007/978-3-319-32699-3_2

5. Anwar A.H., Kamhoua C.A., IEEE Transactions on Network and Service Management, Volume 19, Issue 3, 2022, pp. 3438-3452. DOI: doi.org/10.1109/TNSM.2022.3179965ЫI

6. Ayeni O., Alese B., International Journal of Computer Applications., Volume 70, 2013, P. 20, DOI: dx.doi.org/10.5120/12197-8136

7. Bilinski, M., Gabrys, R. 9th International Conference on Decision and Game Theory for Security, Volume 11199 LNCS, 2018, pp. 115-126. DOI: dx.doi.org/10.1007/978-3-030-01554-1_7

8. Bringer M.L., Chelmecki C.A International Journal of Computer Network and Information Security, Volume 4, 2012, № 10, pp. 63 DOI: dx.doi.org/10.5815/ijcnis.2012.10.07

9. Ochiai H. Expert Systems with Applications, Volume 201, 1 September 2022, P. 117073. DOI: doi.org/10.1016/j.eswa.2022.117073

10. Neal C. 16th International Conference on Network and System Security, 2022, pp. 155-169. DOI: dx.doi.org/10.1007/978-3-031-23020-2_9

11. Yuan J., Yang H., Kong Y. Future Internet, Volume 15, 2023, № 4, pp. 127. DOI: doi.org/10.3390/fi15040127

12. Lim C., Budiarto E., Hobert K. 1st IEEE International Conference on Cryptography, Informatics, and Cybersecurity, 2023, pp. 139-144. DOI: doi.org/10.1109/ICoCICs58778.2023.10276639

13. Pedersen J.M. 38th Annual Computer Security Applications Conference, 2022, pp. 742-755. DOI: doi.org/10.1145/3564625.3564645

14. Salimova H.R. Central Asian Research Journal for Interdisciplinary Studies, Volume 2, Issue 5, 2022, pp. 479-486.

15. Yamin M.M., Katt B. Computers & Security, Volume 122, 2022, pp. 102892, DOI: doi.org/10.1016/j.cose.2022.102892

16. Liu G., Ou X., Singhal A., Tabari A.Z. 19ep IFIP International Conference on Digital Forensics, 2023, pp. 73-90. DOI: dx.doi.org/10.1007/978-3-031-42991-0_5

17. Eng S., How K.C., Zhu Y. Conference on Science, Engineering and Technology, 2023, pp. 587-598.

18. Alissa K., Alqahtani M., Faiz T., Alyas T. Mobile Information Systems, 2022, pp. 1-13. DOI: doi.org/10.1155/2022/2600712

19. Konkin Ju.V., VII Mezhdunarodnyj nauchno-tehnicheskij forum STNO-2024. Sbornik trudov. V. 3, pp. 167-171. EDN: UZZJOA.

20. Javadpour A. Cluster Computing, February Volume 26, Issue 1, 2023, pp. 367-384 DOI: doi.org/10.1007/s10586-022-03621-3

21. Tihonov A.M. Izvestija Instituta Inzhenernoj Fiziki, 2024, №3, pp. 65-71 EDN: QSVNKO

22. Sokolovskij S.P. Informatika: problemy, metodologija, tehnologii, Sbornik materialov XIX mezhdunarodnoj nauchno-metodicheskoj konferencii, 2019, pp. 639-643. EDN: ZFDMBF

23. Yuan J., Yang H., Kong Y. Future Internet, Volume 15, 2023, № 4, pp. 127. DOI: doi.org/10.3390/fi15040127

24. «Deception technology use to grow in 2024 and proliferate in 2025» URL: csoonline.com/article/1246065/deception-technology-use-to-grow-in-2024-and-proliferate-in-2025.html

25. Javadpour A., Taleb T., Ja'Fari F. Computers & Security, Volume 140, 2024, №103792, DOI: doi.org/10.1016/j.cose.2024.103792

26. Onyekware U. Journal of Information Security, 2021, pp. 250-269. DOI: doi.org/10.4236/jis.2021.124014

27. Zhang Li, Thing L. Computers & Security, Volume 106, 2021, P. 102288, DOI: doi.org/10.1016/j.cose.2021.102288.

Дата поступления: 8.05.2025

Дата публикации: 26.06.2025