УДК 004

Ибрагимова А.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

АКТУАЛЬНОСТЬ ПРИМЕНЕНИЯ СИСТЕМ КЛАССА DECEPTION ДЛЯ ЗАЩИТЫ ПРЕДПРИЯТИЯ ОТ СОВРЕМЕННЫХ КИБЕРУГРОЗ

Аннотация. В статье раскрыты особенности комплексной системы защиты информации с применением систем класса Deception. Рассматриваются и анализируются принципы работы данной системы, выделяются преимущества систем класса Deception.

Ключевые слова: информация, система защиты информации, Deception, виртуальные ловушки, эмулированная инфраструктура.

Современные информационные системы (ИС) каждый день сталкиваются с новыми и все более сложными атаками на систему безопасности. Зачастую такие атаки могут оказаться даже незамеченными, т. к. в системах могут применяться неактуальные средства и методы защиты информации, которые не зафиксируют сам факт атаки. В связи с этим особо актуальными становятся новые подходы к управлению рисками информационной безопасности (ИБ), которые имеют возможность опознавать кибератаки на ранних стадиях и предотвращать их дальнейшее воздействие на систему.

Ежегодно поставщики средств защиты информации (СЗИ) представляют клиентам обновленные и все более совершенные средства и инструменты для обеспечения информационной безопасности. Одним из таких инновационных решений является технология Deception - DDP (Distributed Deception Platform), относительно недавно появившаяся на рынке, но уже успевшая привлечь внимание специалистов в области защиты информации. Такие системы создают виртуальные приманки и имитируют слабые места (уязвимости), которые отвлекают внимание

злоумышленников. Это позволяет быстро обнаруживать попытки несанкционированного доступа в систему и снижать потенциальный ущерб от реализации угроз нарушения информационной безопасности [1].

Системы Deception, также называемые системами дезинформации или платформами обмана, представляют собой специализированное программное обеспечение, разработанное для создания ложных целей и сетей, предназначенных для привлечения потенциальных злоумышленников и выявления их тактик. Функционирование этих систем осуществляется путем развертывания фиктивных узлов, сервисов и данных, имитирующих настоящие активы компании, тем самым создавая привлекательные цели для злоумышленников.

Если рассматривать принцип работы Deception, то эта технология основывается на имитации информационной инфраструктуры, которая вводит в заблуждение злоумышленника относительно подлинности и конфигурации информационных ресурсов компании. После внедрения системы класса Deception, инфраструктура организации структурируется в виде двух уровней:

1. Первый уровень – это существующая инфраструктура организации.
2. Второй уровень – это имитированная среда, включающая в себя ловушки и приманки, размещенные на реальных устройствах. Любая активность злоумышленника в отношении этих ловушек немедленно раскрывает его присутствие, отправляя уведомление специалистам по защите информации.

Основными этапами работы Deception-систем являются:

1. Создание виртуальных ловушек: развертывание поддельных серверов, компьютеров, IoT-устройств и т.д., которые неотличимы от настоящих и служат для привлечения внимания злоумышленников.
2. Выявление отклонений: система регистрирует любое взаимодействие с созданными системой ресурсами, что позволяет обнаружить активность злоумышленников.
3. Получение информации об угрозах: анализ действий злоумышленников на виртуальных ловушках предоставляет ценные сведения о применяемых методах, инструментах и тактике нападающего, позволяя проактивно реагировать на угрозы ИБ.
4. Взаимодействие с системой безопасности: данные, полученные с помощью Deception-систем, интегрируются с основными инструментами мониторинга безопасности, обеспечивая комплексную защиту информации.

Система Deception обеспечивает точную регистрацию событий активации виртуальных ловушек и практически любых взаимодействий с созданной имитированной средой [2]. Это дает возможность определить весь путь злоумышленника и провести связь между его действиями с другими событиями, которые происходят в инфраструктуре. В случае обнаружения попыток НСД к основным ресурсам компании, центр

управления безопасностью (SOC) может оперативно предпринять шаги для их изоляции, блокировки подозрительной активности и даже имитировать дальнейшие действия злоумышленника, чтобы отвлечь его внимание от реальных целей.

Таким образом, система Deception не ограничивается только констатацией факта несанкционированного доступа в ИТ-инфрастуктуре, а предоставляет возможности для активного противодействия, обеспечивая анализ всех действий злоумышленника.

Преимуществами систем класса Deception являются:

– раннее предупреждение угроз безопасности на этапе вторжения в систему задолго до того, как атака достигнет критически важных активов, обнаружение подготовительных стадий сетевых атак;

– минимизация ущерба от атаки за счет раннего реагирования;

– обман злоумышленника путем создания ложных целей;

– повышение эффективности защитных мер безопасности информации путем анализа поведения злоумышленников и выявления новых методов атак.

Для успешного внедрения решений класса Deception необходима тщательная настройка имитируемой конфигурации. Поскольку каждая организация имеет уникальные особенности инфраструктуры, система должна быть адаптирована именно под конкретные условия эксплуатации [3]. Это позволит построить более эффективную систему для введения злоумышленника в заблуждение. Также необходима регулярная проверка работоспособности для своевременного обновления конфигураций и мониторинга. Это позволяет избежать уменьшения эффективности механизмов защиты информации.

Кроме того, системы Deception позволяют провести интеграцию с существующими системами мониторинга и управления инцидентами (SIEM, SOC) организации. Инструменты Deception могут стать частью общей экосистемы безопасности информации, эффективно дополняя традиционные меры защиты (антивирусные программы, межсетевые экраны), применяемые в организации.

Использование систем класса Deception способствует созданию дополнительного слоя защиты, повышая устойчивость организации перед современными киберугрозами. Таким образом, внедрение систем класса Deception становится важным элементом современной стратегии кибербезопасности, способствующим повышению защищенности информационных ресурсов предприятия.

Список использованных источников:

1. Вавилин Я.А. Информационные технологии в управлении качеством и защита информации: учебное пособие для вузов / Я.А. Вавилин, В.Г. Солдатов, И.Г. Манкевич. Санкт-Петербург: Лань, 2025. 196 с.

Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/447242 (дата обращения: 18.04.2025).

2. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. 6-е изд., стер. СПб.: Лань, 2025. 124 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book /445250 (дата обращения: 18.04.2025).

3. Тумбинская М.В. Защита информации на предприятии: учебное пособие для вузов / М.В. Тумбинская, М.В. Петровский. 2-е изд., стер. Санкт-Петербург: Лань, 2025. 184 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book /463043 (дата обращения: 18.04.2025).

Ibragimova A.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

THE RELEVANCE OF USING DECEPTION CLASS SYSTEMS TO PROTECT ENTERPRISES FROM MODERN CYBER THREATS

Abstract. The article reveals the features of a comprehensive information protection system using Deception class systems. The principles of operation of this system are considered and analyzed, the advantages of Deception class systems are highlighted.

Keywords: information, rights, information protection, information protection system, Deception, virtual traps, emulated infrastructure.