ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ OSINT ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лукашевич Е.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Супрун Ф.Н.

Аннотация. На протяжении последних десятилетий значительно увеличивается количество информационных атак. В современном мире конфиденциальность данных и стабильность функционирования информационной системы являются необходимым условием бесперебойной и конкурентоспособной деятельности. В связи с этим стремительными темпами развивается противодействие угрозам информационной безопасности. В статье представлены способы применения технологии разведки данных из открытых источников (OSINT) для выявления угроз информационной безопасности.

В условиях новой реальности стабильно увеличивается количество кибератак. Злоумышленники находят все более сложные и неуловимые способы информационного воздействия с целью кражи или уничтожения данных, внедрение вредоносного кода или программного обеспечения.

Наиболее распространёнными видами угроз информационной безопасности являются следующие:

– DDoS (Distributed Denial of Service) – атака, направленная на перегрузку сети или конкретного сервера большим количеством запросов. DDoS-атаки приводят к временной недоступности инфраструктуры.

– Фишинг — мошенническая практика, когда киберпреступники выдают себя за надежные источники для получения личной информации.

– SQL-инъекции — метод атаки, при котором злоумышленники внедряют SQL-код в запросы к базе данных для получения доступа к данным, содержащимся в этой БД.

– Социальная инженерия — манипуляции людьми с целью получения личной информации или выполнения определенных действий. Например, злоумышленник может различными способами втираться в доверие к жертве, ведя с ней переписку в социальных сетях или мессенджерах.

– Advanced Persistent Threat (APT) — продолжительная и хорошо подготовленная целенаправленная кибератака. В отличие от DDoS, APT — комплексная киберугроза, сочетающая различные способы атак на корпоративную инфраструктуру [1].

Исходя из этого возникает необходимость поиска эффективных способов противодействия. Проблема многих систем информационной безопасности в том, что они направленны на противостояние возникающим угрозам, а не на выявление уже существующих уязвимостей для их устранения. Одним из наиболее эффективных методов такого противодействия является OSINT.

OSINT (Open Source Intelligence, разведка на основе открытых источников) — это методика сбора данных из открытых источников информации, таких как публичные базы данных, интернет-сайты, медиа и социальные сети. Эти данные анализируются для получения сведений, которые могут быть использованы в аналитических, разведывательных и стратегических целях [2].

Использование методов разведки из открытых источников позволяет проанализировать структуру сети и базы данных, обнаружить важную коммерческую информации в открытом доступе, тем самым устранить бреши в системе защиты.

Сервисы Shoodan и Censys позволяют обнаружить открытые порты, устаревшие протоколы защиты и неверные конфигурационные настройки сети.

Публичные репозитории исходного кода. Такие платформы, как GitHub, GitLab и Bitbucket, нередко становятся источником утечек конфиденциальной информации вследствие ошибочной публикации учетных данных.

Также активно развивается использование социальной инженерии. Злоумышленники используют публикации в социальных сетях для составления психологического портрета, тем самым находя точки воздействия для достижения своих целей. Использование технологии OSINT позволяет обнаружить в открытых источниках подобную информацию и обучить не оставлять информационные следы, которые могут быть использованы для совершения информационной атаки.

Таким образом применение технологии OSINT позволяет эффективно выявлять уязвимости в информационной безопасности. Методы сбора данных из открытых источников дают возможность оперативно обнаружить риски укреплению информационной безопасности и повышению устойчивости к внешним и внутренним рискам.

Список использованных источников:

1. Академия Selectel [Электронный ресурс]. – Электронные данные. – Режим доступа: https://selectel.ru/blog/security-threats/. – Дата доступа: 25.03.2026.

2. RTM Group [Электронный ресурс]. – Электронные данные. – Режим доступа: https://rtmtech.ru/articles/dlya-chego-nuzhen-osint/. – Дата доступа: 25.03.2026.