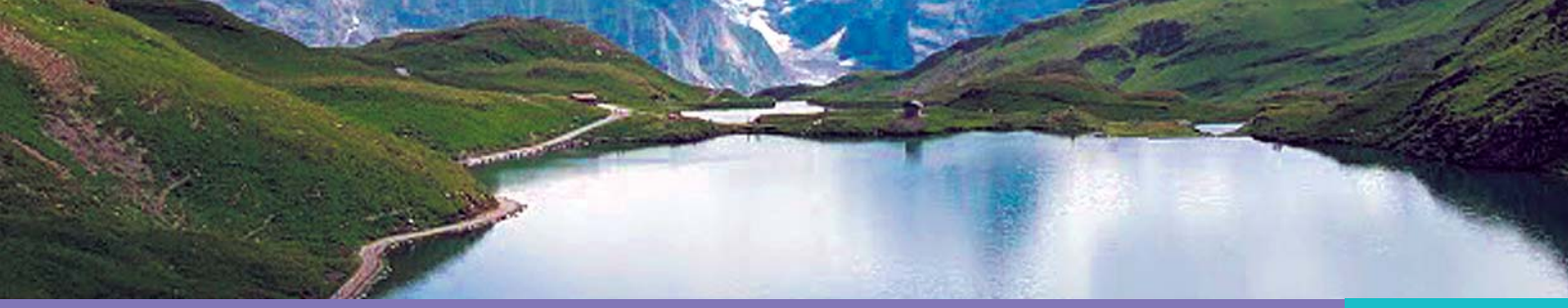

Модуль идентификаторов IDID в составе комплекса «Дозор-Джет»

ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В возможности современного комплекса для защиты от утечек информации «Дозор-Джет» входит мониторинг практически всех возможных каналов передачи данных. Даже в небольшой компании информационный поток очень велик, и в таких условиях очень важной задачей является качественный и быстрый анализ огромного количества собранной информации.

Модуль идентификаторов IDID, входящий в комплекс «Дозор-Джет», – одно из наиболее эффективных средств для проведения подобного анализа.

Модуль представляет собой удобный инструмент, обнаруживающий в потоке данных множество различных идентификаторов.

Идентификатор – это уникальная цифровая или буквенная последовательность, однозначно определяющая какой-либо объект. В частности, модуль идентификаторов IDID способен выявлять следующие типы идентификаторов:

финансовые	персональные данные	сетевые	Другие
• БИК • Visa • MasterCard • Diners Club • Laser • коды ОКАТО	• ИНН РФ • русские имена • номера российских паспортов • пенсионные карты (ПФ РФ СНИЛС)	• email • URL • samba shares • IP	• номера вагонов

Уникальной особенностью данного модуля является возможность обнаружения специфических русских идентификаторов (например, коды БИК, ОКАТО, ФИО, ИНН, номера российских паспортов, СНИЛС и т.д.).

В основе модуля – запатентованные алгоритмы. Сложные механизмы математических проверок и возможность анализа окружающего текста позволяют свести ложные срабатывания до минимума.

Политика работы модуля идентификаторов IDID гибко настраивается. Перечислим некоторые ее возможности:

- выбор поиска только нужного типа идентификаторов, что позволяет увеличить скорость обработки поискового запроса;
- учет количества уникальных идентификаторов. В рамках одного письма (документа, файла) один и тот же идентификатор может встречаться несколько раз. Данная опция позволяет считать все вхождения этого идентификатора за единичное появление идентификатора.

ЦЕНТР
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

- Настройка уровня строгости проверки:
  1. Проверка ключевых сумм, учет появления одного и того же идентификатора в рамках одного письма (файла, документа) несколько раз, проверка окружающего текста на наличие ключевых слов
  2. Проверка ключевых сумм и учет появления одного и того же идентификатора в рамках одного письма (файла, документа) несколько раз
  3. Проверка ключевых сумм

Модуль идентификаторов IDID взаимодействует с Системой анализа и архивирования «Дозор-Джет» (входит в состав комплекса «Дозор-Джет», может использоваться как самостоятельная система). В числе возможностей Системы обработка данных, собранных модулем идентификаторов, и осуществление заранее настроенных действий. Например, таким действием может быть отправка администратору безопасности уведомления об инциденте.

Отправка оповещений гибко настраивается под необходимые задачи администраторов безопасности. Например, в связи с особенностями работы компании, возможна ситуация, когда пересылка идентификаторов (номеров карт, ФИО и т.д.) – обычный рабочий процесс. В этом случае важно отличать рабочий процесс от возможной утечки идентификаторов, чтобы избежать ложных срабатываний и недопустимой утечки. Основываясь на регламентах работы подразделения, можно настроить отправку уведомлений следующим образом: при обнаружении в электронном письме более 5 различных номеров кредитных карт система автоматически отправит администратору безопасности оповещение с пометкой «Инцидент». Но в случае, если в письме один и тот же идентификатор встречается 5 и более раз, а другие идентификаторы отсутствуют или их количество менее четырех, отправка уведомления производиться не будет. Такое письмо будет помечено как содержащее идентификатор и помещено в архив.

С помощью модуля идентификаторов IDID администраторы безопасности могут легко отслеживать и контролировать пересылку идентификаторов, автоматически вычленяемую из огромного потока информации. Удобный интерфейс, гибкая настройка и запатентованные алгоритмы обеспечивают легкость решения этой задачи. Модуль позволяет избежать написания сложных регулярных выражений и пустой траты времени на рутинную обработку ложных срабатываний.

Jet infosystems

Россия, 127015, Москва
ул. Б. Новодмитровская, д. 14, стр. 1,
офисный Центр «Новодмитровский»
Тел.: +7 (495) 411-7601
Факс: +7 (495) 411-7602
E-mail: info@jet.msk.su
www.jet.msk.su