



КОЛЛАБОРАЦИЯ РОССИЙСКИХ РЕШЕНИЙ

Архиватора ARZip и DLP-системы InfoWatch Traffic Monitor
в частном учреждении «Цифрум»

Решение проблемы утечек конфиденциальной информации через защищенные паролем архивы

Компания ARinteg – ведущий системный интегратор на российском рынке информационной безопасности*

- Обеспечиваем защиту информационных ресурсов, оказываем экспертно-аналитические, технические, консалтинговые услуги, развиваем собственные разработки
- С 1996 года выполняем подбор, проектирование, поставку программных и аппаратных решений. Помогаем оперативно внедрять, обеспечиваем техническую поддержку
- Работаем с лидирующими российскими вендорами
- Используем как готовые системы и технологии, так и разрабатываем персональные решения под задачи заказчика

* рейтинг Snews 2023 г.

InfoWatch – ведущий российский разработчик решений для обеспечения информационной безопасности крупного бизнеса и государственных организаций



Признанный эксперт и лидер рынка DLP-систем России и СНГ, InfoWatch успешно развил свои решения в направлении всесторонней защиты данных

Подтверждением экспертизы и технологического преимущества InfoWatch являются более 4000 проектов для коммерческих и государственных организаций в двадцати странах мира



ARZip – первое и единственное в Реестре отечественного ПО решение, которое **совмещает в себе возможности для работы с файловыми архивами с функциональностью противодействия утечкам данных** благодаря совместной работе с наиболее распространенными российскими DLP-системами

The screenshot shows the website 'reestr.digital.gov.ru' with a search for 'Архиватор'. The search results table is as follows:

Наименование	Правообладатель / Производитель	Дата включения в реестр	№ реестровой записи
Архиватор ByteFuse	ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "КЛАУД БЭЙС СТЭЙШН"	07.04.2020	6457
Архиватор ARZip	Общество с ограниченной ответственностью "ARinteg"	05.12.2022	15721
Программный комплекс "Специализированный архиватор электронных сообщений" версия 6	Российская Федерация	14.06.2022	13931

Below the table, there is a section 'Информация об уязвимостях' with a green checkmark and the text: 'Сведения об уязвимостях в Банке данных угроз безопасности информации не обнаружены'.

Уникальность ARZip

ARZip позволяет, благодаря интеграции по API с DLP, **автоматизировать проверку запароленных архивов, тем самым предупредить утечки данных через них.**

Эффективность сжатия данных ARZip на уровне лучших мировых решений благодаря современным алгоритмам



ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№15721 от 05.12.2022 г.



Архиватор ARZip поможет:

повысить
кибербезопасность

рационально
использовать
ресурсы

автоматизировать
проверку архивов

Работает на ОС

- Windows
- Linux Debian
- Astra Linux
- Alt Linux
- RED OS

Распаковывает

- .zip
- .rar
- .7z
- .tar
- .tar.gz
- .arj

Упаковывает

- .zip
- .7z
- .tar
- .tar.gz



**ВКЛЮЧЕН В РЕЕСТР
ОТЕЧЕСТВЕННОГО ПО
№10340 от 21.04.2021 г.**

**и относится к сфере
искусственного
интеллекта**



**INFOWATCH
TRAFFIC MONITOR**

- Разрабатывается в России с 2007 года
- Поддерживает отечественные операционные системы и СУДБ
- Сертифицирована ФСТЭК России, ФСБ и Министерством Обороны

InfoWatch Traffic Monitor – DLP-система нового поколения. С использованием технологий машинного обучения предотвращает утечки конфиденциальной информации, прогнозирует риски и повышает уровень автоматизации работы службы ИБ

Продвинутое технологии анализа не только по контенту, но и с учетом контекста

- 39 программных технологий и патентов, не имеющих аналогов на рынке
- Точно идентифицируем объекты защиты меньше ложных срабатываний
- Категоризируем 100% данных по смыслу документа с помощью ML и т.д.

Универсальные технологии перехвата

- Контроль любых облачных хранилищ
- Перехват передачи файлов независимо от протокола приложения
- Контроль потребляемой информации из критических приложений и т.д.

Возможности для расследований и аналитики, которым нет аналогов на рынке

- Центр расследований – единый интерфейс для работы с событиями DLP, персонами, файлами, рисками и аналитикой из «одного окна»
- Переключение между разными срезами данных с сохранением контекста
- Исследуем коммуникации людей и пути перемещения документов с помощью интерактивного графа связей на 50 000 узлов и т.д.

Интеграция решений ARinteg и InfoWatch

Пилотное внедрение успешной коллаборации российских решений ARZip с DLP-системой InfoWatch Traffic Monitor провели весной 2024 г. в частном учреждении «Цифрум»

Защищенные паролем архивы – распространенные каналы утечек конфиденциальной информации.

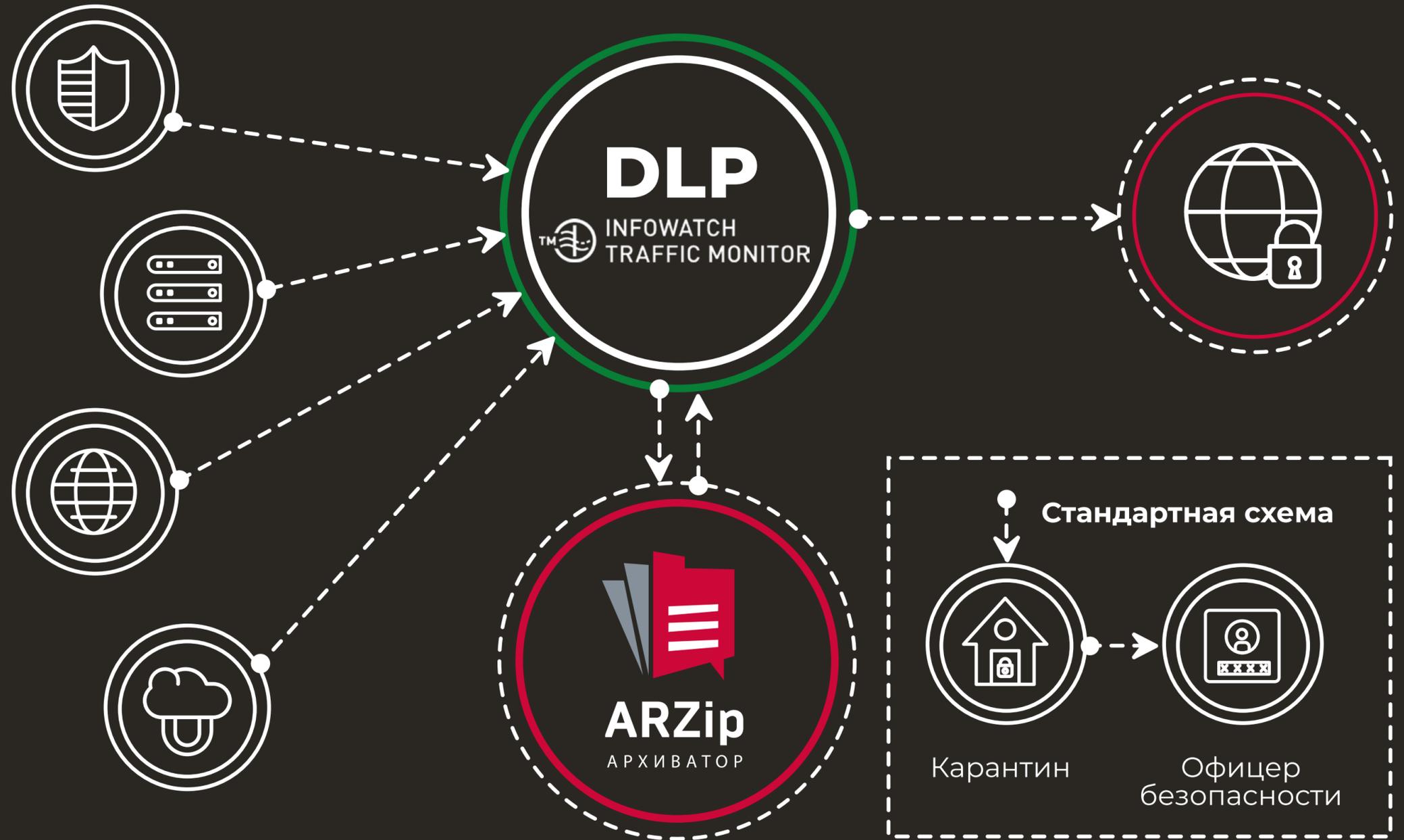
Совместное использование решений ARZip и InfoWatch Traffic Monitor – одно из предлагаемых нами вариантов, как можно закрыть потенциальный риск, обеспечив возможность контролировать архивы в автоматическом режиме, и сократить операционные затраты на обработку подобных инцидентов

Интеграция ARZip и InfoWatch Traffic Monitor



Рекомендуем **принять ARZip**
в качестве **корпоративного стандарта**

Автоматизированная работа DLP
с запароленными архивами
позволит уйти от ручного разбора
карантинных файлов



Интеграция ARZip и DLP InfoWatch Traffic Monitor представляет решение по чтению зашифрованных архивов

Если архив без пароля – ARZip просто его распаковывает

Если архив зашифрован ARZip, из файла считывается его ID и по нему запрашивается пароль на сервере-паролей

Получив обратно пароль, ARZip распаковывает архив в доступную Traffic Monitor папку

Traffic Monitor проверяет содержимое архива по установленным правилам



Процесс работы с архивными файлами становится автоматизированным, нет необходимости задействовать офицеров безопасности или отправлять автоматический запрос сотруднику предоставить пароль

Пример интеграции

Создание нового архива

1 Шаг Параметры 2 Шаг Файлы 3 Шаг Дополнительно

Описание

Пароль для шифрованного архива

Что архивируем? Рабочие файлы (pdf, docx, xlsx)

Назад Создать архив

Сбросить

Создание архива с паролем ARZip

```
astra@astra: ~/Tools
[clap_builder::parser::validator]Validator::validate_required: is_exclusive_pres
ent=false
[clap_builder::parser::arg_matcher]ArgMatcher::get_global_values: global_arg_vec
=[]
root
User { username: "root",
Попробуем запускиться на порту 8081
008be0154c967a8db067743e2f90a4ec ← 1
Archive id: 008be0154c967a8db067743e2f90a4ec ← 2
Password: ***** ← 3
```

1. Информация (ID архива и пароль) передаётся между ARZip и сервером паролей в зашифрованном виде. Используется собственный алгоритм шифрования
2. Запрос пароля по ID файла
3. Получение пароля

The screenshot displays the InfoWatch Traffic Monitor Enterprise web interface. The browser address bar shows the URL: `https://10.70.240.74/events?QUERY=1&SELECTED_OBJECT_ID=27171`. The interface includes a navigation menu with options like "Сводка", "События", "Отчеты", "Технологии", "Объекты защиты", "Персоны", "Политики", "Списки", and "Управление".

The main content area is divided into two sections:

- События за текущий день**: A list of events for the current day. The first event (ID: 27171) is highlighted. It shows details such as "Отправители" (администратор@exchange), "Компьютер" (exchange), "Веб-ресурс" (cloud.prod.arinteg.ru), and "Описание" (cloud.prod.arinteg.ru : отправка сообщения).
- Event ID: 27171 details**: A detailed view of the selected event. It includes a table of metadata:

Отправители	администратор@exchange
Компьютер	exchange exchange fe80::bdb5:4089:ed08:4d90%12
Веб-ресурс	cloud.prod.arinteg.ru
Политики	Система безопасности
Объекты защиты	Охрана организации

Below the table, there is a download link for a file named "Some%20tips%20for%20protecting... (6 KB)".

The main text of the event details is a document snippet with the following content:

сооружения, например крепостная стена, ров с водой и перекинутый через него подъемный мост. И если применяемые для защиты периметра средства с течением времени видоизменялись, вбирая в себя новые достижения инженерной мысли, то функции, выполняемые системой, в целом остались неизменными:

 - сдерживание или запугивание;
 - обнаружение **нарушителя**;
 - увеличение времени преодоления **нарушителем** систем защиты (задержка);
 - физическое **задержание нарушителя**.

Последнее во многом зависит от правильной организации **служб безопасности** и обучения их личного состава.

Проектирование систем защиты периметров требует использования комплексного подхода, предполагающего наличие в их составе пассивного ограждения и системы сигнализации: первое затрудняет и замедляет проникновение постороннего, а второе обеспечивает его обнаружение. Следует также отметить, что

срабатывания. Последние со временем начинают раздражать обслуживающий персонал, что в конечном итоге может привести к игнорированию всех сигналов, в том числе и истинных. Поэтому системы сигнализации желательно дополнять средствами телевизионного наблюдения, которые позволяют проверить обоснованность тревожного сигнала. Достоинства систем телевизионного наблюдения не исчерпываются возможностью обнаружения действий **нарушителя** — не менее важна постоянная или выборочная фиксация (например, на видеопленку) происходящих на объекте событий.

Основные характеристики периметровых средств сигнализации

Обычно выделяются следующие характеристики периметровых средств сигнализации [1].

1. Уязвимость системы. Данный параметр определяет возможность преодоления рубежа без возникновения сигнала тревоги, в том числе с использованием специальных методов и

InfoWatch Traffic Monitor перехватил запароленный архив, провел анализ контента и подсветил характерные признаки защищаемой конфиденциальной информации

Пилотное внедрение и тестирование ARZip в частном учреждении «Цифрум»

- Установка проведена силами группы ИБ и представителями компании ARinteg
- На АРМ администратора ИБ развернут сервер паролей
- В фокус-группу вошли 3 АРМа блока безопасности и 1 АРМ группы ИТ



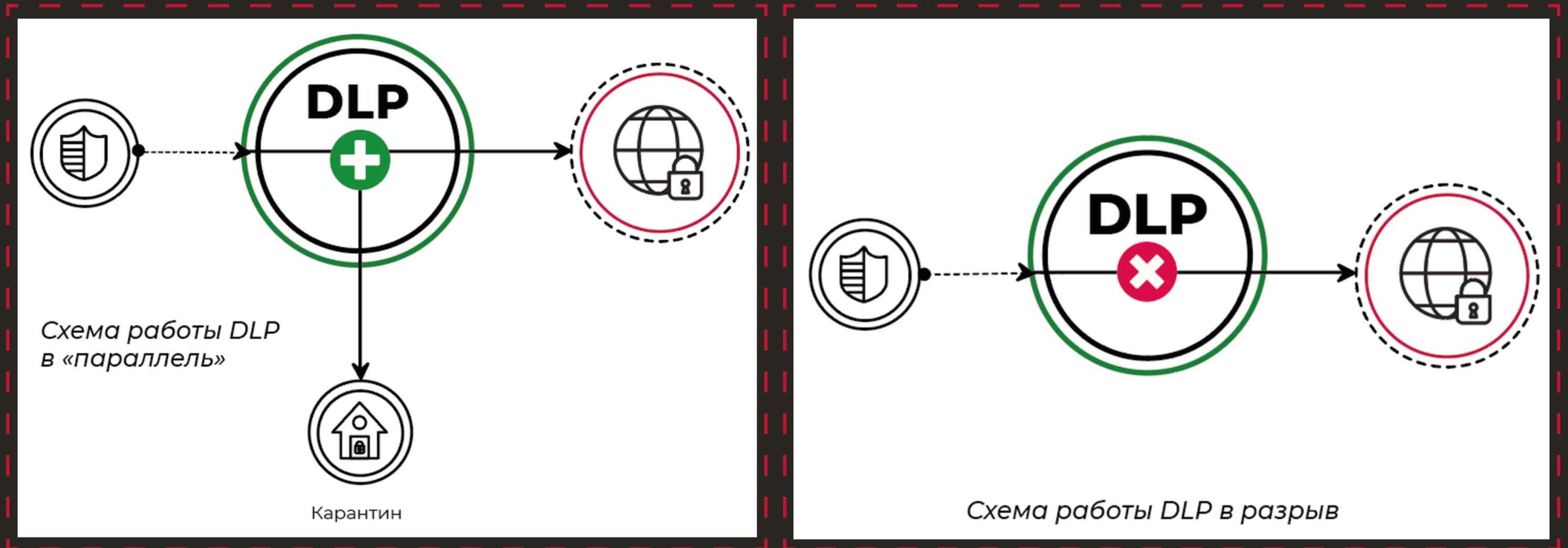
Плюсы внедрения

Для работников безопасности чтение и проверка содержимого запароленного архива не представляет сложностей. Любой запароленный архив прозрачен, по сути, являясь обычным читаемым вложением

Выводы

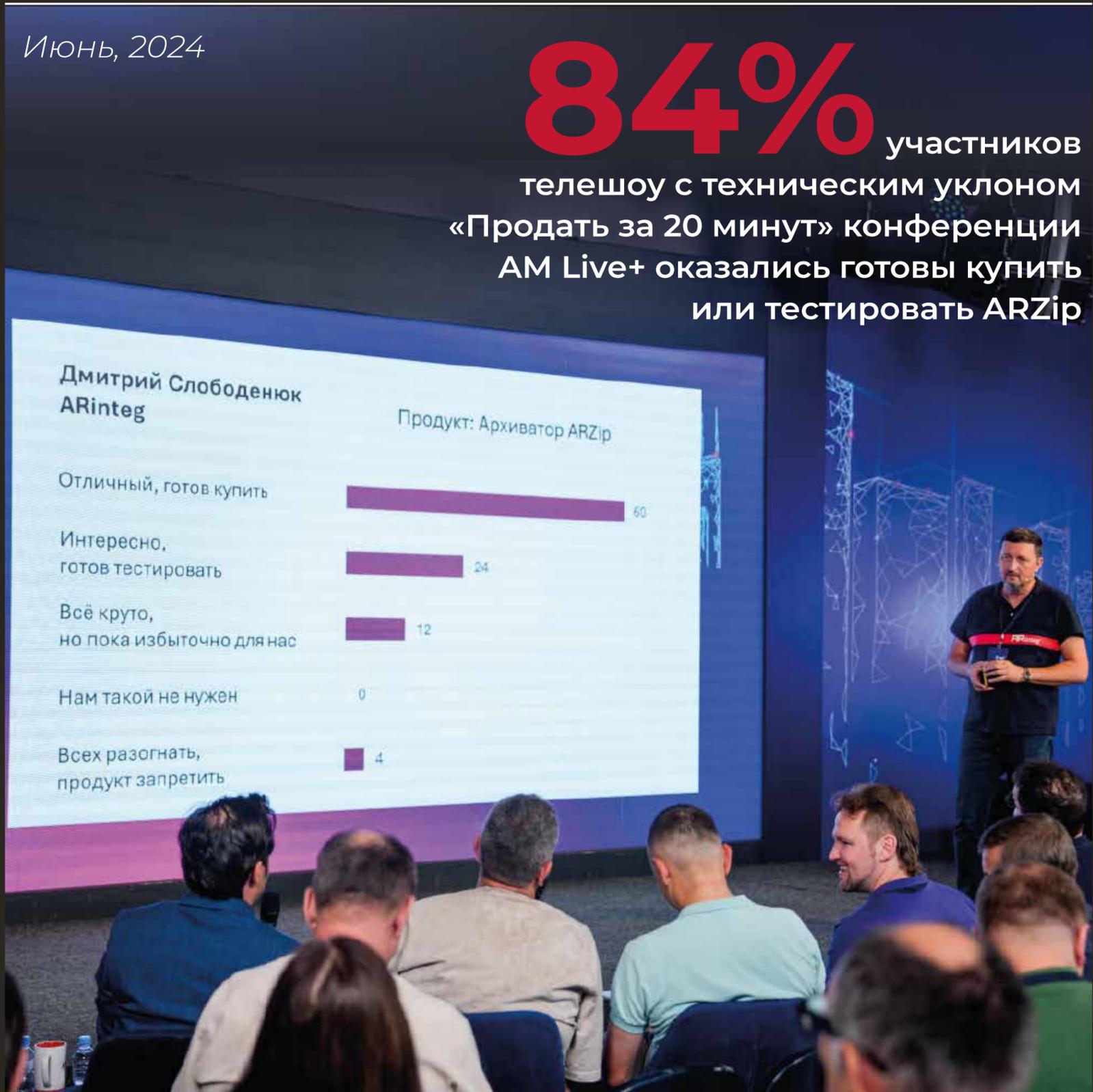
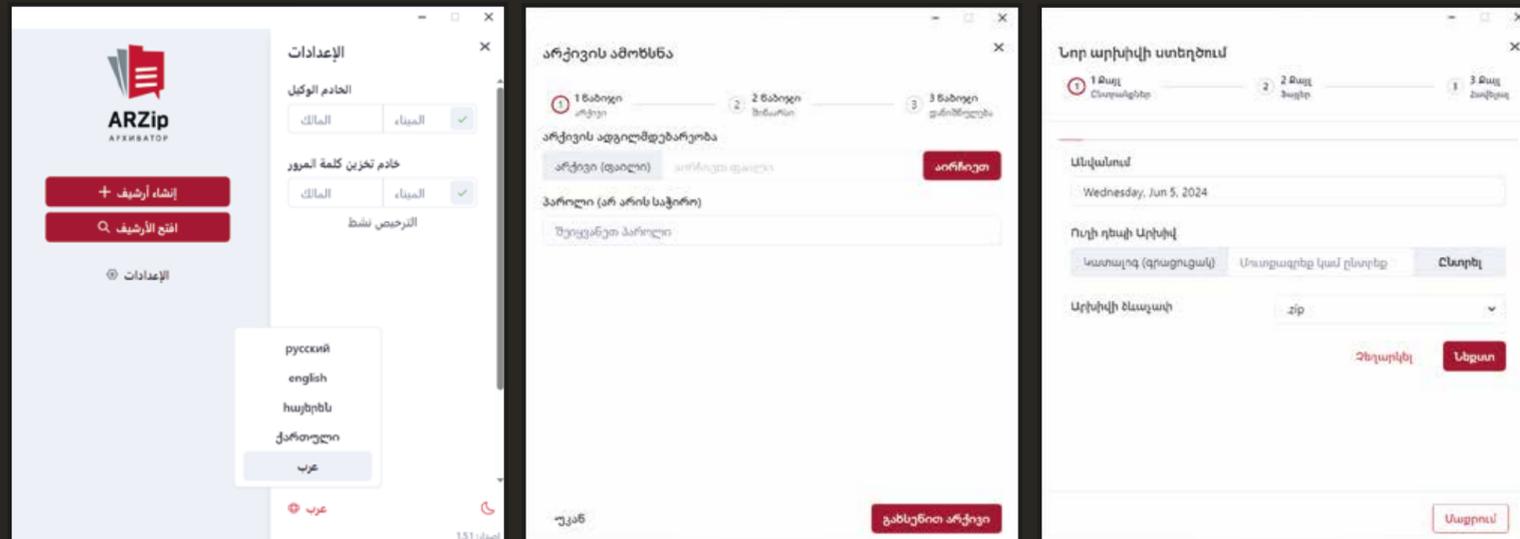
- Тестирование считаем успешным
- При внедрении программного комплекса требуется внесение изменений в ЛНА о применении в качестве программы для архивирования файлов и директорий программы ARZip
- Решение о приобретении программного комплекса ARZip руководством блока безопасности принято

Схема работы DLP в «параллель» и разрыв

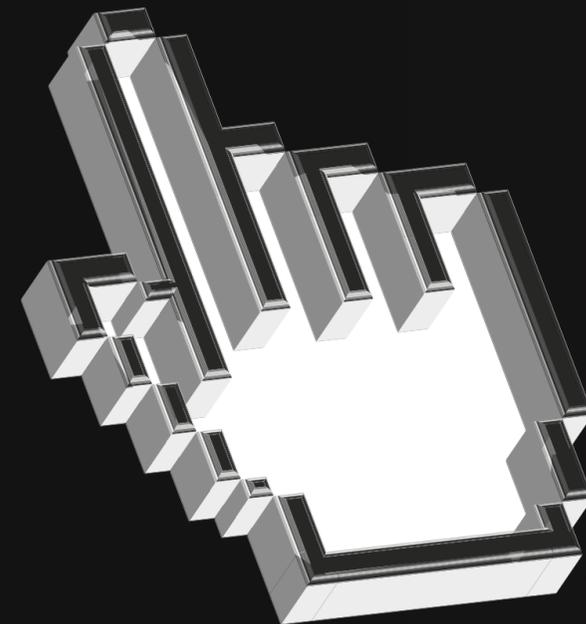


Использование ARZip способствует тому, что все большее число компаний устанавливают DLP «в разрыв», а не в «параллель», тем самым позволяя DLP-системе сразу блокировать передачу конфиденциальной информации за пределы организации

ARZip мультиязычен



ARinteg продолжает **расширять**
функциональность архиватора ARZip
и интегрировать его с другими
распространенными отечественными
DLP-системами



Российские СМИ про ARZip

NBJ НАЦИОНАЛЬНЫЙ
БАНКОВСКИЙ ЖУРНАЛ

РБК

conews

TADVISER
Государство. Бизнес. Технологии

2024/03/06 17:06:28

Как ARZip позволяет автоматизировать проверку архивов и повысить кибербезопасность организации

Компании уязвимы архивами. Но выход есть: ARZip — уникальное решение для работы с запароленными архивами.

Запароленный архив — крепкий орешек для специалистов по информационной безопасности компаний с точки зрения процедур, связанных с предотвращением утечек.

Сжатый и защищенный паролем файл, как правило, не позволяет DLP-системе заглянуть внутрь такого архива. А значит, с ним за периметр организации может уйти чувствительная информация.

Однако, команда ARinteg нашла решение этой проблемы, создав программу-архиватор ARZip для работы с запароленными архивами, которая уже внесена в реестр отечественного ПО под №15721.

Содержание Свернуть

- Уникальность ARZip
- Кто и почему защищает архивы паролями
- Как быстро ARZip окупается

Аналитика и комментарии
20 августа 2024

Проблема утечек конфиденциальной информации через защищенные паролем архивы нашла решение: архиватор ARZip научил DLP «видеть архивы насквозь»



Пилотное внедрение такой интеграции успешно прошло в частном учреждении «Цифрум», входящем в структуру ГК «Росатом», и сейчас оно продолжает развивать этот проект.

«Мы можем интегрировать архиватор ARZip по API с любой DLP-системой. Уникальность нашего совместного проекта с InfoWatch заключается в том, что данная интеграция двусторонняя, решение доставляется заказчику уже «в коробке». Более того, сегодня мы обсуждаем с коллегами дальнейшие возможности коллаборации», — прокомментировал коммерческий директор ARinteg Дмитрий Слободенюк.

ВАШ ГАРАНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

НАШИ КОНТАКТЫ

 +7 (495) 221-21-41

 sales@ARinteg.ru



www.ARinteg.ru



t.me/ARinteg



vk.com/ARinteglife