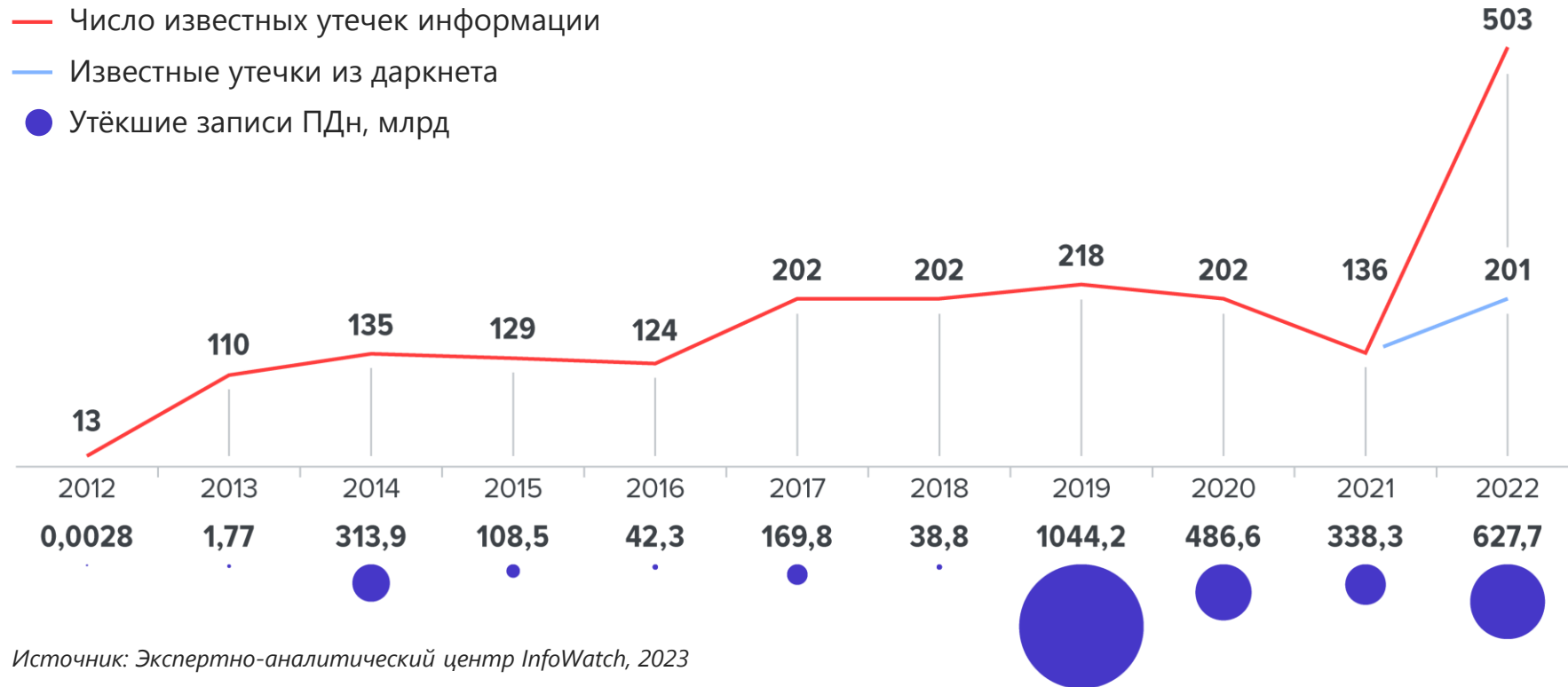


ЗАЩИТА ПЕРСОНАЛЬНЫХ ОТ УТЕЧЕК

КЕЙС

Успешный проект InfoWatch
в крупном российском банке

Лавинообразный рост утечек информации и ПДн в финансовом секторе: мир, 2022



Источник: Экспертно-аналитический центр InfoWatch, 2023

Статистика экспертно-аналитического центра InfoWatch фиксирует рост утечек: мир, H1 2023



в **2,4** раза
больше утечек
информации



+19,4% —
рост доли утечек
коммерческой тайны

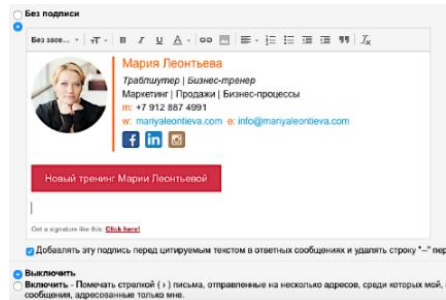


18,3 млрд
записей ПДн
скомпрометировано

На практике идентифицировать утечку персданных крайне сложно

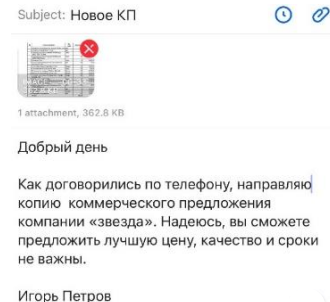
Для защиты от утечек компании используют DLP-системы*, но не все они одинаково эффективно справляются с поставленной задачей

Подпись к письму часто содержит персональные данные и может ошибочно распознаваться обычной DLP-системой как угроза



Ущерб — 0 руб.
ложная тревога

Настоящая утечка КП конкуренту теряется в рядовой переписке в рамках рутинных бизнес-задач



Ущерб — 300 млн. руб.

* Data Loss Prevention — система предотвращения утечек информации

Принцип работы InfoWatch Traffic Monitor фундаментально отличается от традиционных DLP

Традиционные DLP-системы на рынке определяют персональные данные по контенту

- ФИО
- Номер карты
- Номер паспорта
- Электронный адрес



Они «засоряют» внимание службы безопасности множеством ложных срабатываний

DLP-система InfoWatch Traffic Monitor определяет персональные данные по контексту

- Банковская выписка может быть отправлена владельцу карты или постороннему лицу
- Конфиденциальные данные — **подрядчику, с которым подписано NDA, или конкуренту**
- Спецпредложение по кредитной ставке — **не тому клиенту**



Динамическая настройка системы — и точное выявление угроз

task_detail_id	line1	line2	line3	line4	line5	server...	start_time	end_time	exec_number
3e1fa646-3f...	Резервное копи...	Создать резер...	Базы данных В...	Тип: Полная	Добавить к существующему	SERVER-1C	2010-12-23 04:...	2010-12-23 04:...	ALL
25bc3654-a2...	Восстановить н...	Перестроить н...	Базы данных В...	Объект: Таблицы и пред...	Исходный обмен свободно...	SERVER-1C	2010-12-23 23:...	2010-12-23 23:...	ALL
533d3d00-35...	Восстановить н...	Перестроить н...	Базы данных В...	Объект: Таблицы и пред...	Исходный обмен свободно...	SERVER-1C	2010-12-24 23:...	2010-12-24 23:...	ALL
e13fd11c-f0e...	Резервное копи...	Создать резер...	Базы данных В...	Тип: Полная	Добавить к суш				
95e9f00e-37...	Обновить стат...	Обновить стат...	Базы данных В...	Объект: Таблицы и пред...	Все собранная с				
5116e450-e1...	Восстановить н...	Перестроить н...	Базы данных В...	Объект: Таблицы и пред...	Исходный обмен				
1e3219fc-19...	Обновить стат...	Обновить стат...	Базы данных В...	Объект: Таблицы и пред...	Все собранная с				
45e833cc-01...	Реорганизация ...	Реорганизоват...	Базы данных В...	Объект: Таблицы и пред...	Сжатие базово				
45e833cc-01...	Обновить стат...	Обновить стат...	Базы данных В...	Объект: Таблицы и пред...	Все собранная с				
1904af39-92...	Восстановить н...	Перестроить н...	Базы данных В...	Объект: Таблицы и пред...	Исходный обмен				
25bc3654-a2...	Обновить стат...	Обновить стат...	Базы данных В...	Объект: Таблицы и пред...	Все собранная статистика	SERVER-1C	2010-12-23 23:...	2010-12-23 23:...	ALL
533d3d00-35...	Реорганизация ...	Реорганизоват...	Базы данных В...	Объект: Таблицы и пред...	Сжатие базово: объектов	SERVER-1C	2010-12-24 23:...	2010-12-24 23:...	ALL
95e9f00e-37...	Восстановить н...	Перестроить н...	Базы данных В...	Объект: Таблицы и пред...	Исходный обмен свободно...	SERVER-1C	2010-12-25 23:...	2010-12-25 23:...	ALL
e08a281b-0c...	Реорганизация ...	Реорганизоват...	Базы данных В...	Объект: Таблицы и пред...	Сжатие базово: объектов	SERVER-1C	2010-12-27 23:...	2010-12-27 23:...	ALL
e08a281b-0c...	Обновить стат...	Обновить стат...	Базы данных В...	Объект: Таблицы и пред...	Все собранная статистика	SERVER-1C	2010-12-27 23:...	2010-12-27 23:...	ALL
25bc3654-a2...	Реорганизация ...	Реорганизоват...	Базы данных В...	Объект: Таблицы и пред...	Сжатие базово: объектов	SERVER-1C	2010-12-23 23:...	2010-12-23 23:...	ALL
402aad63-e3...	Резервное копи...	Создать резер...	Базы данных В...	Тип: Полная	Добавить к существующему	SERVER-1C	2010-12-24 04:...	2010-12-24 04:...	ALL
533d3d00-35...	Обновить стат...	Обновить стат...	Базы данных В...	Объект: Таблицы и пред...	Все собранная статистика	SERVER-1C	2010-12-24 23:...	2010-12-24 23:...	ALL

Смирнова Мария
ул. Пришвина, 10, кв. 99
+79857733378

- Контролируем движение конкретных данных, а не просто доступ к базе
- Защищаем актуальные данные — динамическое обновление данных при обновлении в ИС

ЗАПАТЕНТОВАНО

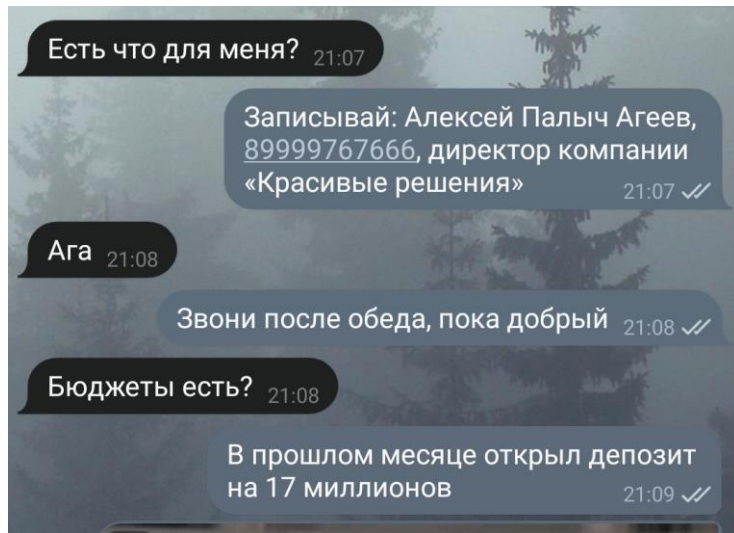
Для каждой защищаемой сущности (ПДн, база клиентов, поставщиков, сотрудников) несколько критериев срабатывания — например, комбинации полей и объём переданных данных.

2 Проверка и контроль движения конкретных данных, а не доступа к БД

task_detail_id	line1	line2	line3	line4	line5	server...	start_time	end_time	exec_number
3e1fa646-3f...	Резервное копи...	Создать резер...	Базы данных: В...	Тип: Полная	Добавить к существующему	SERVER-1C	2010-12-23 04:...	2010-12-23 04:...	ALL
25bc3654-a2...	Восстановить н...	Перестроить н...	Базы данных: В...	Объект: Таблицы и пред...	Исходный обмен свободно...	SERVER-1C	2010-12-23 23:...	2010-12-23 23:...	ALL
533d3d00-36...	Восстановить н...	Перестроить н...	Базы данных: В...	Объект: Таблицы и пред...	Исходный обмен свободно...	SERVER-1C	2010-12-24 23:...	2010-12-24 23:...	ALL
e13fd11cc-f0e...	Резервное копи...	Создать резер...	Базы данных: В...	Тип: Полная	Добавить к суш				
95e9f00e-37...	Обновить стат...	Обновить стат...	Базы данных: В...	Объект: Таблицы и пред...	Все собранная с				
5116d450-a1...	Восстановить н...	Перестроить н...	Базы данных: В...	Объект: Таблицы и пред...	Исходный обмен				
1a3219fc-19...	Обновить стат...	Обновить стат...	Базы данных: В...	Объект: Таблицы и пред...	Все собранная с				
45e833cc-01...	Реорганизация ...	Реорганизоват...	Базы данных: В...	Объект: Таблицы и пред...	Сжатие большо				
45e833cc-01...	Обновить стат...	Обновить стат...	Базы данных: В...	Объект: Таблицы и пред...	Все собранная с				
1904af39-92...	Восстановить н...	Перестроить н...	Базы данных: В...	Объект: Таблицы и пред...	Исходный обмен				
25bc3654-a2...	Обновить стат...	Обновить стат...	Базы данных: В...	Объект: Таблицы и пред...	Все собранная статистика	SERVER-1C	2010-12-23 23:...	2010-12-23 23:...	ALL
533d3d00-36...	Реорганизация ...	Реорганизоват...	Базы данных: В...	Объект: Таблицы и пред...	Сжатие большо: объектов	SERVER-1C	2010-12-24 23:...	2010-12-24 23:...	ALL
95e9f00e-37...	Восстановить н...	Перестроить н...	Базы данных: В...	Объект: Таблицы и пред...	Исходный обмен свободно...	SERVER-1C	2010-12-25 23:...	2010-12-25 23:...	ALL
e08a291b-0c...	Реорганизация ...	Реорганизоват...	Базы данных: В...	Объект: Таблицы и пред...	Сжатие большо: объектов	SERVER-1C	2010-12-27 23:...	2010-12-27 23:...	ALL
e08a291b-0c...	Обновить стат...	Обновить стат...	Базы данных: В...	Объект: Таблицы и пред...	Все собранная статистика	SERVER-1C	2010-12-27 23:...	2010-12-27 23:...	ALL
25bc3654-a2...	Реорганизация ...	Реорганизоват...	Базы данных: В...	Объект: Таблицы и пред...	Сжатие большо: объектов	SERVER-1C	2010-12-23 23:...	2010-12-23 23:...	ALL
402aad63-e3...	Резервное копи...	Создать резер...	Базы данных: В...	Тип: Полная	Добавить к существующему	SERVER-1C	2010-12-24 04:...	2010-12-24 04:...	ALL
533d3d00-36...	Обновить стат...	Обновить стат...	Базы данных: В...	Объект: Таблицы и пред...	Все собранная статистика	SERVER-1C	2010-12-24 23:...	2010-12-24 23:...	ALL

Агеев Алексей Павлович
ООО «Красивые решения»
89999767666

Блокируем передачу клиентских данных постороннему лицу с новой функцией — проверка допустимости получателя.



3 Автоматическая проверка легитимного получателя

ИС, где хранятся данные	→ Письмо с выгрузкой по счёту	→ DLP-система
124. Иван Иванов, ivanov@mail.ru	Уважаемый Иван Иванов! Ваша выписка по счёту №...	ivanov@mail.ru ✓ →
3555. Пётр Сидоров, sidorov@yandex.ru	Уважаемый Сергей Собянин! Ваша выписка по счёту №...	sidorov@yandex.ru ✗ →

Система проверила, что выгрузка о состоянии счета принадлежит Ивану Иванову, его адрес электронной почты совпадает с тем, на который пытаются отправить данные.

отправка легитимна и разрешена

Система проверила, что выгрузка о состоянии счета принадлежит Сергею Собянину, но его адрес электронной почты не совпадает с тем, на который пытаются отправить данные.

отправка нелегитимна и заблокирована

Проект внедрения решения по защите ПДн в финансовой организации



О клиенте*

- 3 000+ сотрудников
- 20+ лет на рынке
- 100 000 записей клиентов
- В CRM-системе хранятся миллионы персональных данных клиентов



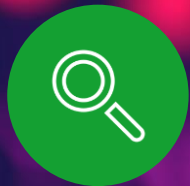
Задачи

- Как защитить ПДн в CRM-системе от злоумышленника?
- Как быть уверенным, что 4 000 выписок о состоянии счёта, отправленные ВИП-клиенту, точно принадлежат ему?



Защитить

все выгрузки из базы данных, где содержится чувствительные данные (CRM и другие ИС)



Проверить

принадлежность конкретной порции персональных данных отправителю до отправки



Блокировать

отправку письма с важными данными на e-mail, который не соответствует электронному адресу клиента в ИС

Итоги внедрения DLP нового поколения InfoWatch Traffic Monitor для защиты ПДн

- Защищены выгрузки из баз и ИС, где содержатся ПДн
 - Система определяет легитимность отправки порции ПДн конкретному получателю
 - Всегда актуальные данные: при обновлении данных в CRM-системе автоматически обновляется информация в DLP InfoWatch Traffic Monitor
 - Поиск для каждого сообщения составляет не более 1/10 сек
-
- Персональные данные Банка надёжно защищены благодаря уникальной запатентованной разработке InfoWatch
 - Защищённость повысилась на >70%
 - Количество инцидентов снизилось в ~3,5 раз

О компании InfoWatch



20

лет на рынке
информационной
безопасности



+30%

инвестиций
в разработку
и НИОКР
ежегодно



500+

сотрудников
в компании



28

патентов
на технологии



700+

клиентов
в финансовой
орасли



135+

аналитических
отчётов в год



100+

технологических
партнёров



5000+

обученных
специалистов ИБ



Наталья Касперская

Президент и основной владелец
ГК InfoWatch. Соучредитель
и генеральный директор
«Лаборатории Касперского».
Руководитель рабочей группы
«Информационная безопасность»
национальной программы
«Цифровая экономика РФ»

САМЫЕ СВЕЖИЕ НАГРАДЫ,

которые получили продукты InfoWatch

TADVISER
Государство. Бизнес. Технологии

«Лучшее ИБ-решение»

TAdviser, 2021

CNews

«Инновация года в ИБ»

CNews FORUM Кейсы, 2022