ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БИЗНЕСА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / DLP-система «СёрчИнформ КИБ»

ЭКОНОМИКА

Дополнительная информация по кейсу

КРАТКОЕ ОПИСАНИЕ РЕШЕНИЯ

Решение представляет собой – DLP-систему (Data Leak Prevention) для предотвращения утечек информации и корпоративного мошенничества. Контролирует максимальное число каналов связи, облачных хранилищ, устройств (принтеров, оборудования, подключаемого по USB, Bluetooth, RDP и др.) и активность пользователей за ПК. Система анализирует поступающие данные с помощью мощных поисковых механизмов, которые работают со всеми видами конфиденциальной информации, в т.ч. аудио, видео и графикой. Автоматизирует контроль и ускоряет реакцию на инцидент. Решение позволяет:

- Защищать конфиденциальные данные от утечек и неправомерного доступа.
- Выявлять факты корпоративного мошенничества и нарушения дисциплины.
- Контролировать средства удаленного управления и виртуализации.
- Блокировать нежелательные действия пользователей с чувствительной информацией

SEARCHINFORM
INFORMATION SECURITY

УСЛОВИЯ РЕАЛИЗАЦИИ И ИСПОЛЬЗУЕМЫЕ ДАННЫЕ

Для внедрения требуется: серверное оборудование (за исключением внедрения в облаке); лицензии серверных ОС и СУБД.

В помощь заказчикам вендор предоставляет техническое задание к закупке необходимых компонентов.

Финансово-экономическая модель: Для госзаказчиков доступна закупка по 44-ФЗ и 223-ФЗ, для коммерческих компаний – на общих условиях. Основная модель – приобретение бессрочных лицензий и ежегодной технической поддержки (техническое обслуживание, обновления, доработки, обучение работе с ПО, консультации). Доступно внедрение по сервисной модели: в облаке, по подписке на период, в формате аутсорсинга.

Данные: заказчика, предоставляемые в рамках реализации проекта

ПРОБЛЕМНАЯ СИТУАЦИЯ

- Утечки информации (встречалось в 44% компаний в 2022 г.)*: торговля персональными данными, «пробив», промышленный шпионаж, работа на конкурентов, случайные «сливы» корпоративной информации в открытый доступ
- Корпоративное мошенничество (в 32 % компаний): боковые схемы, откаты, взятки, воровство, саботаж
- Нерациональное использование рабочего времени (в 34% компаний): игры, онлайн-шопинг, просмотр кино и сериалов, сторонняя занятость в рабочее время
- Внешние атаки через сотрудников (в 14% компаний): фишинг, социальная инженерия, BEC-атаки (атаки с подменой корпоративных email-адресов), вирусные заражения, компрометация рабочих аккаунтов
- Расходы на внедрение и обслуживание защитного ПО (в т.ч. человеческих ресурсов - рабочего времени специалистов ИБ)

*по данным исследования «СёрчИнформ» об уровне информационной безопасности российских компаний, 2022 г.

СТОИМОСТЬ И СРОКИ

От 4 часов

От 3 до 31 тыс. руб.
(за 1 бессрочную лицензию продукта для контроля 1 пользователя / ПК)

РЕЗУЛЬТАТЫ ЦИФРОВИЗАЦИИ

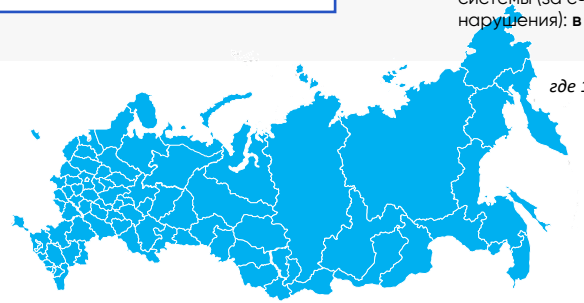
- Снижение количества свершившихся (непредотвращенных) утечек информации: **95%***
- Снижение количества фиксируемых попыток мошенничества: инциденты данной группы встречаются на **60%** реже
- Повышение дисциплины и эффективности работы сотрудников: инциденты, связанные с нарушением трудовой дисциплины, встречаются на **35%** реже
- Повышение ИБ-грамотности сотрудников, за счет осведомленности об угрозах и действующих правилах безопасности: случайные инциденты, инциденты «по незнанию» и пр. встречаются на **75%** реже
- Экономия до **25%** на ПО и оборудовании для работы системы (по сравнению с конкурентами) за счет технологических и архитектурных решений. Окупаемость системы (за счет снижения финансового ущерба от инцидентов ИБ, компенсаций за нарушения): **в течение 1 года**

**субъективные оценки клиентов «СёрчИнформ», где 100% - среднее суммарное кол-во инцидентов ИБ, зафиксированных системой*

Сергей Ожегов

Генеральный директор
ООО «СёрчИнформ»

order@searchinform.ru



ОПЫТ РЕАЛИЗАЦИИ

Решения «СёрчИнформ» внедрены во всех регионах РФ.