От «бумажной» безопасности к реальной защите

ЕГОР КОЖЕМЯКА

ДИРЕКТОР ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU

Что происходит после закупки СЗИ?

Требования регуляторов

Модель угроз

Меры защиты информации

Закупка сертифицированных СЗИ

?

Есть такое мнение

Сертифицированные решения:

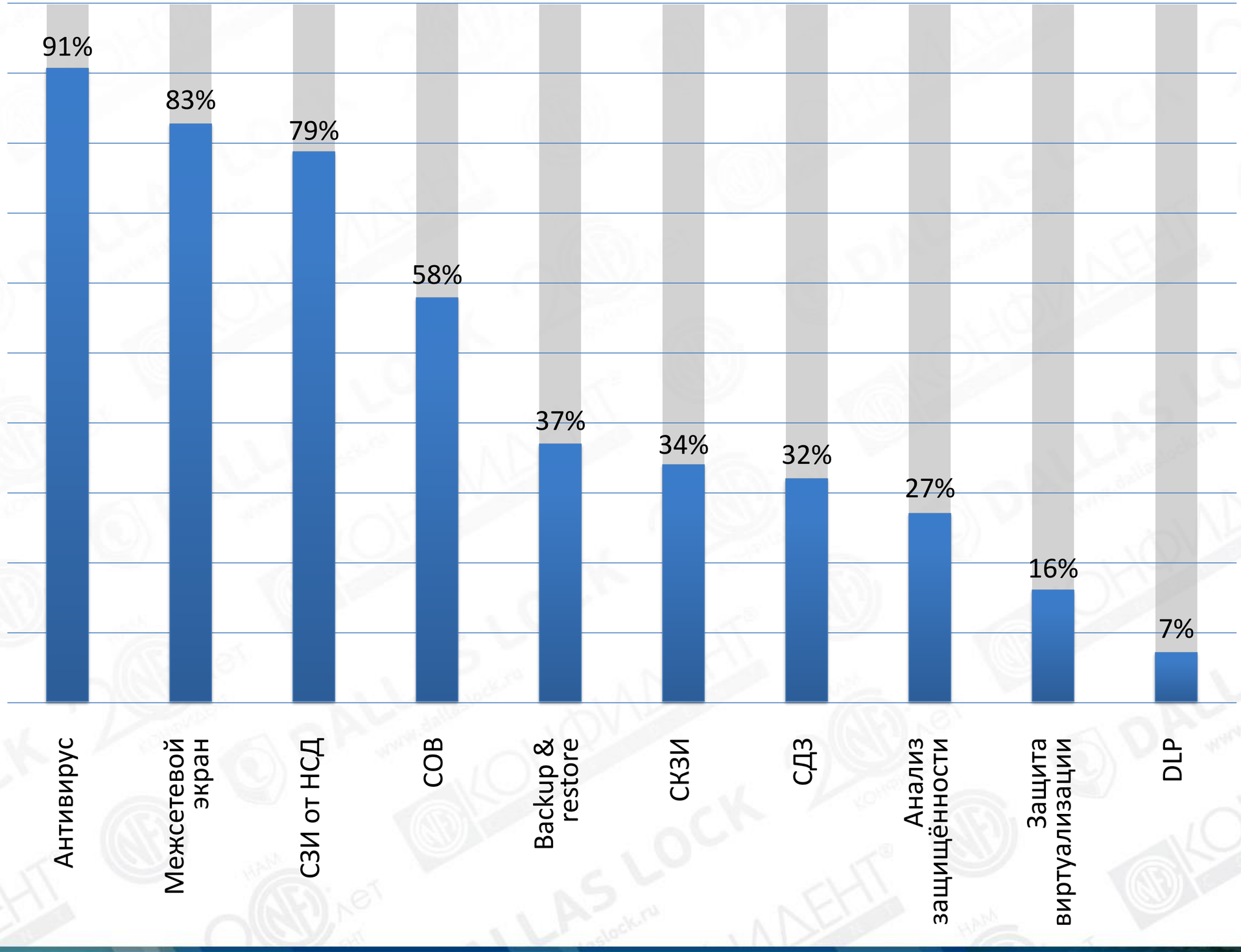
- СЗИ от НСД
- СДЗ
- МЭ
- СКЗИ
- другие

Нужно приобрести, чтобы соблюсти требования

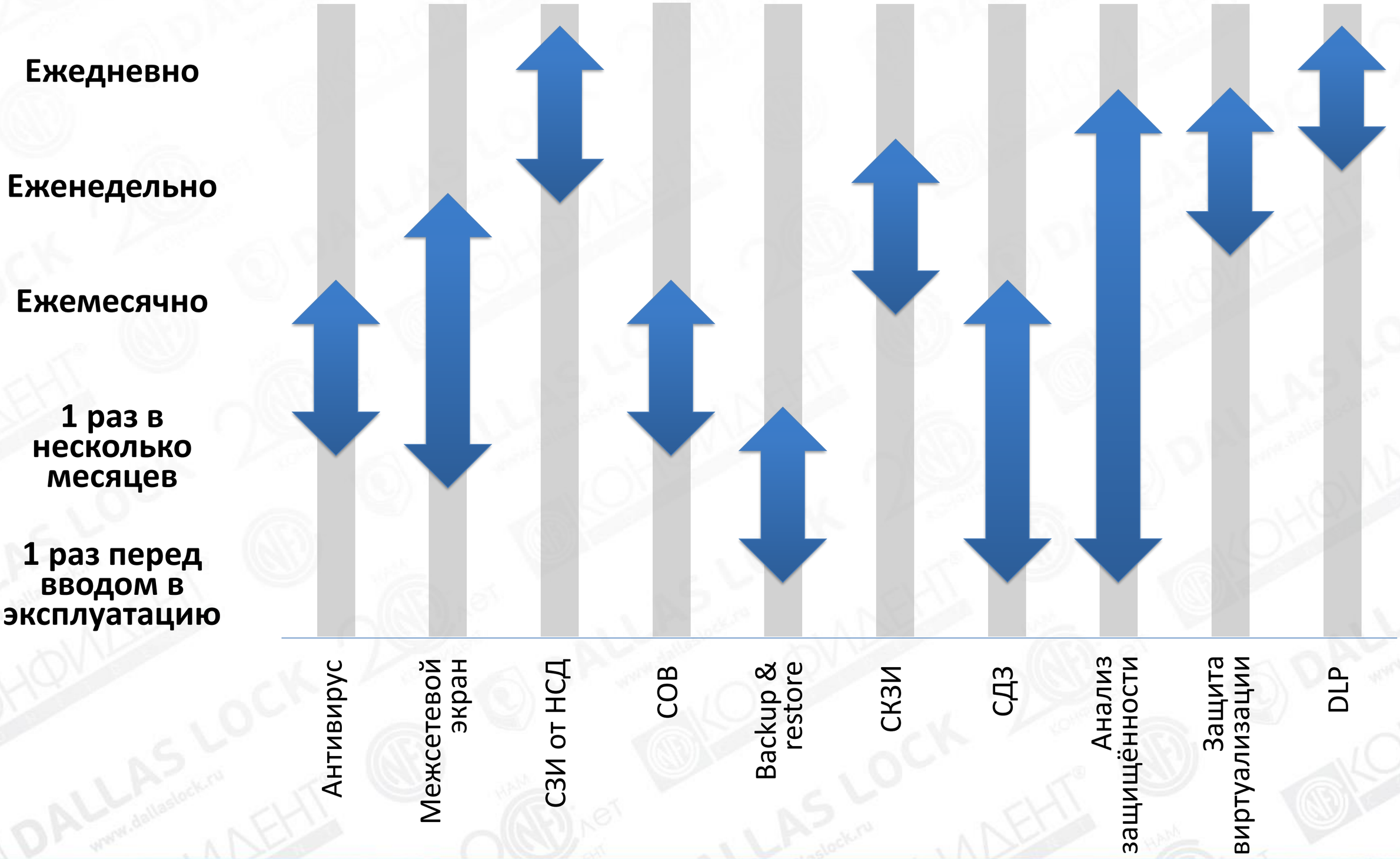
- Антивирус
- NGFW
- SandBox
- DLP
- SIEM
- EDR

Нужно приобрести, чтобы защитить информацию

Какого набора СЗИ достаточно в большинстве случаев для защиты информационной системы



Как часто на объектах заказчиков производится настройка этих СЗИ



Лабораторные исследования

	Без СЗИ	СЗИ НСД 1	СЗИ НСД 2
Без СЗИ	25	10	10
Антивирус 1	19	10	10
Антивирус 2	20	10	10

Количество существующих уязвимостей в ИС на базе Linux

Некоторые соображения

- Принцип действия антивирусов и СЗИ от НСД отличается. Они дополняют друг друга.
- СЗИ от НСД зачастую модифицируют или подменяют ядро ОС. Это касается как наиболее популярных Linux-дистрибутивов, так и отечественных ОС. Например, Dallas Lock Linux заменяет ядро ОС на то, которое проверили специалисты по защите информации, включая вендора, испытательную лабораторию и **некоторые другие организации**.

Поиск уязвимостей

Релиз продукта, фиксация программного кода

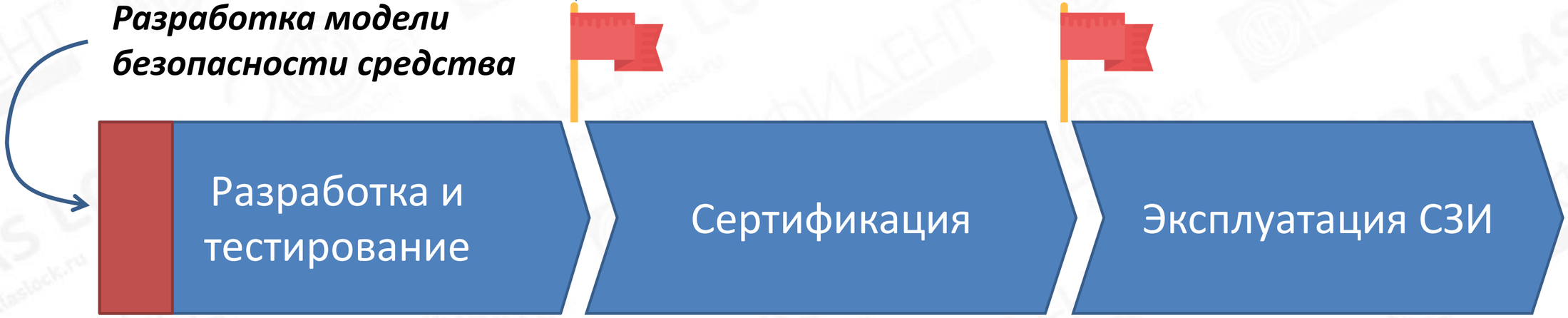
Статический и динамический анализ, Fuzzing-тестирование

Разработка модели безопасности средства

Анализ уязвимостей в системе сертификации ФСТЭК России

Получение сертификата соответствия

Выявление уязвимостей по программе Bug Bounty



Испытательная лаборатория

Независимые исследователи

Поиск уязвимостей

Релиз продукта, фиксация программного кода

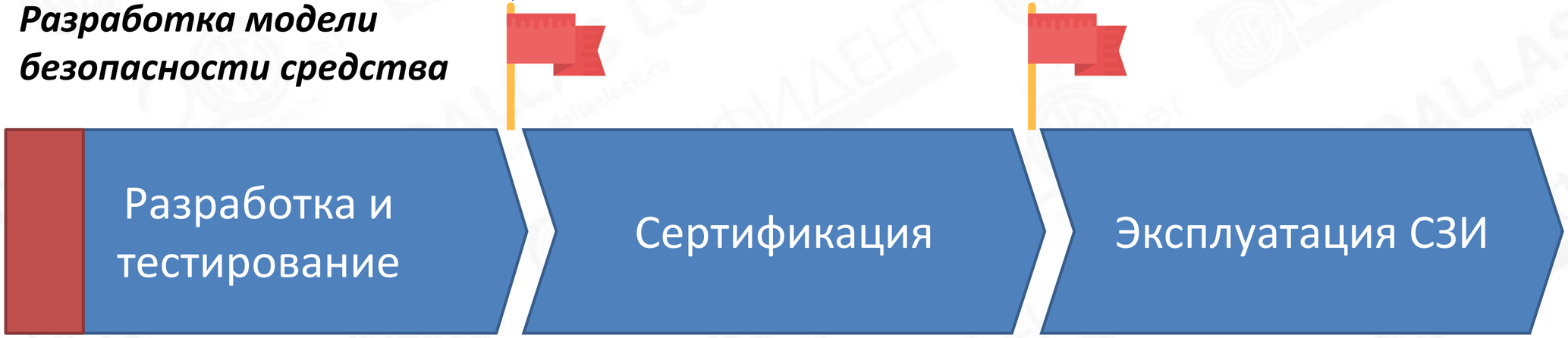
Статический и динамический анализ, Fuzzing-тестирование,

Разработка модели безопасности средства

Анализ уязвимостей в системе сертификации ФСТЭК России

Получение сертификата соответствия

Выявление уязвимостей по программе Bug Bounty



Подрядная организация

Испытательная лаборатория

Независимые исследователи

Поиск уязвимостей

- Продукты становятся сложнее, функциональность постоянно развивается
- Чем больше функций, тем потенциально больше уязвимостей

Привлечение независимой подрядной организации позволило ещё на этапе разработки выявить уязвимости в новой функциональности

Распространённое мнение

«СЗИ от НСД обладают только той функциональностью, которую определяют требования Регулятора»

Функциональность СЗИ от НСД

- ☐ Авторизация до загрузки ОС
- ☑ Контроль целостности до и после загрузки ОС
- ☑ Защита от НСД
- ☐ Контроль подключения носителей и переноса информации
- ☑ Персональный межсетевой экран
- ☑ Обнаружение и предотвращение вторжений
- ☐ Безопасная среда («песочница»)
- ☐ Инвентаризация ПО
- ☐ Защита виртуализованных сред
- ☐ Резервное копирование и восстановление
- ☐ Интеграция с другими системами (SIEM, контроль защищённости)
- ☑ Журналирование всех событий

Примерно так воспринимают СЗИ от НСД

Функциональность СЗИ от НСД

Централизованное управление, профессиональные сервисы

- ☑ Авторизация до загрузки ОС
- ☑ Контроль целостности до и после загрузки ОС
- ☑ Защита от НСД
- ☑ Контроль подключения носителей и переноса информации
- ☑ Персональный межсетевой экран
- ☑ Обнаружение и предотвращение вторжений
- ☑ Безопасная среда («песочница»)
- ☑ Инвентаризация ПО
- ☑ Защита виртуализованных сред
- ☑ Резервное копирование и восстановление
- ☑ Интеграция с другими системами (SIEM, контроль защищённости)
- ☑ Журналирование всех событий

Примерно так обстоят дела на самом деле

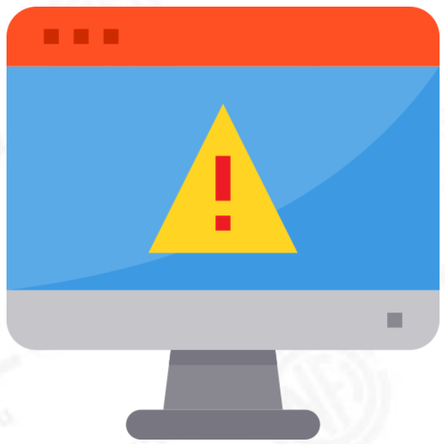
Взаимодействие пользователя с ТП

Администратор ИБ
(конечный пользователь)

запросы

решения проблем

Техническая
поддержка



типовые решения

все запросы

Шаг 1. Журнал ТС в составе СЗИ

Администратор ИБ
(конечный пользователь)

запросы

решения проблем

Техническая
поддержка

типовые решения

все запросы

решения проблем,
важные новости и уведомления

Шаг 1. Журнал ТС в составе СЗИ

Dallas Lock 8.0-C, Admin, 0 (Открытые данные), метка не выбрана (СБ: WIN10V1909) Демо-версия.

Состояние | Учетные записи домена | Параметры безопасности домена | Контроль ресурсов домена | СКН | РК | МЭ | СОВ | Журнал СБ | Администрирование на СБ

Журнал СБ | Журнал ТС — Категории

Обновить | Настроить | Экспорт... — Действия

Объекты DL

Windows | Linux | СДЗ | Общее

- Сервер безопасности (WIN10V1909)
  - Default
    - Default
  - Group
    - TORWIN7ULTX64
    - WIN10V1909

Время	Тип	Номер заявки	Источник	Комментарий
2019-10-25 12:00:00	Информационный		dallasl	
2019-10-20 12:00:00	Важный		dallasl	
2019-09-24 12:00:00	Обновление		dallasl	
2019-09-02 12:00:00	Важный		dallasl	
2019-08-16 09:03:55	Техподдержка	1032475	"Антон	
2019-08-15 17:15:33	Техподдержка	1032475	"Антон	
2019-08-15 17:02:18	Техподдержка	1032475	"Антон	
2019-08-15 16:57:49	Техподдержка	1032475	"Антон	
2019-08-15 16:56:53	Техподдержка	1032475	"Антон	
2019-08-15 16:50:54	Техподдержка	1032475	"Антон	
2019-08-15 16:48:19	Техподдержка	1032475	"Антон	
2019-08-08 17:10:02	Техподдержка	1032376	"Антон	
2019-08-08 17:06:20	Техподдержка	1032376	"Антон	
2019-08-08 17:02:29	Техподдержка	1032376	"Антон	
2019-08-08 16:51:42	Техподдержка	1032376	"Антон	
2019-08-08 16:40:21	Техподдержка	1032376	Технич	
2019-08-08 16:20:10	Техподдержка	1032376	"Антон	
2019-04-23 00:00:00	Информационный		dallaslo	СЗИ Dallas Lock 8.0, СЗ...
2019-03-20 00:00:00	Информационный		dallaslo	19 ноября 2019 года О...

Настройка

Выбор типа получаемых сообщений

- [x] Важный
- [x] Техподдержка
- [x] Информационный
- [x] Обновление

Выбор отображаемых сообщений

0 | все записи (все записи / первые записи / последние записи)

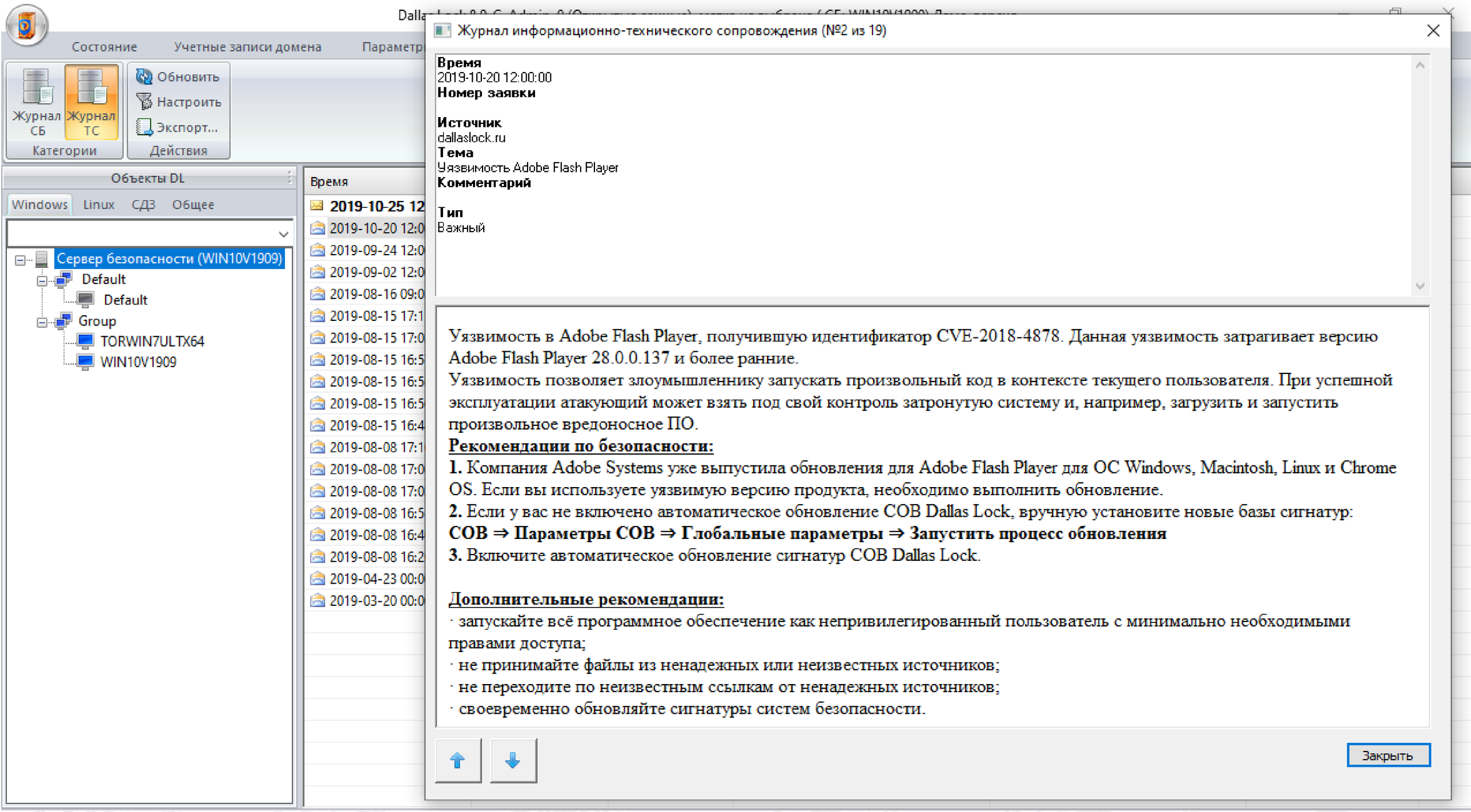
- [ ] Фильтр по времени

С: 19.12.2019 15:47:12

По: 19.12.2019 15:47:12

OK | Отмена

Шаг 1. Журнал ТС в составе СЗИ



Позиция Регулятора

«Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» утверждены приказом ФСТЭК России от 30 июля 2018 г. №131

Приказ зарегистрирован Минюстом России 14 ноября 2018 г. No 52686, вступил в силу с 1 августа 2018 г., применяется при проведении сертификационных испытаний с 1 мая 2019 г.

Позиция Регулятора

Обновление средства должно предусматривать:

- информирование потребителей средства о выпуске обновлений;
- обеспечение возможности получения обновления средства способами, обеспечивающими его целостность.
- в случае получения обновления средства по сетям связи средство должно получать такие обновления с информационного ресурса заявителя;
- при доведении обновлений средства до потребителей должны обеспечиваться подлинность и целостность обновлений за счет применения электронной цифровой подписи.
- доведение информации о выпуске обновлений средства должно осуществляться до каждого потребителя сертифицированного средства путем отправки сообщений на электронные адреса потребителей или за счет применения компонента средства, обеспечивающего доведение указанной информации до потребителя автоматически.

Шаг 2. Помощь в идентификации инцидентов

Администратор ИБ
(конечный пользователь)

запросы, инциденты

решения проблем

Техническая
поддержка

сообщение об инциденте

***решения проблем,
важные новости и уведомления***

типовые решения

все запросы

Шаг 3. Превентивное реагирование

угрозы

запросы, инциденты

решения проблем

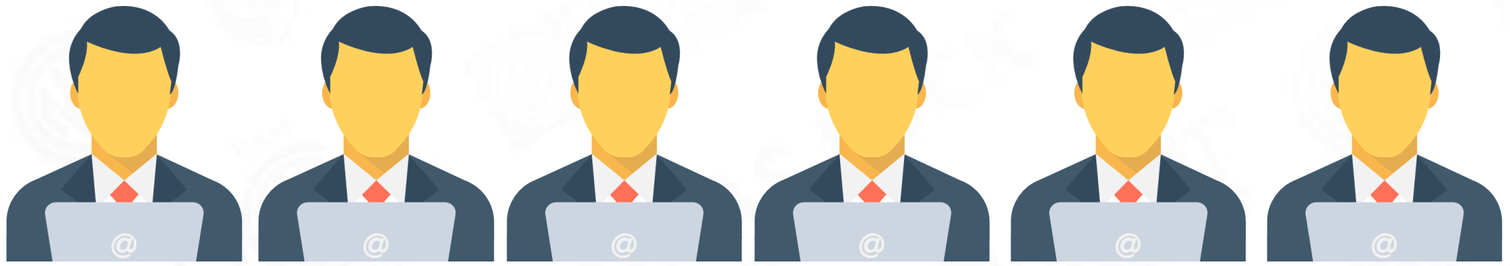
Техническая поддержка

типовые решения

все запросы

превентивное реагирование на инциденты

Синергетический эффект

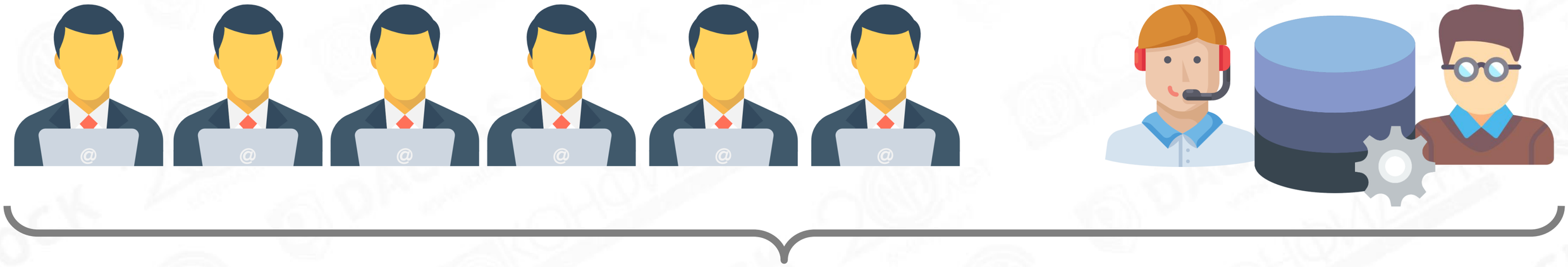


десятки тысяч специалистов по всей России

27-летний опыт вендора и стендовая база

- Получают необходимые знания от вендора.
- Учатся друг у друга.
- Решают проблемы до их возникновения.
- Точно идентифицируют инциденты.
- Понимают, за что платят деньги.

Синергетический эффект



Профессиональное сообщество производителя и потребителей, совместно решающее задачи по защите информации

Спасибо за внимание!

ЕГОР КОЖЕМЯКА

ДИРЕКТОР ЦЕНТРА ЗАЩИТЫ ИНФОРМАЦИИ
ГК «КОНФИДЕНТ»

E-MAIL: ISC@CONFIDENT.RU

WEB: WWW.DALLASLOCK.RU