Информационная безопасность для начинающих, где взять ресурс

ОБО МНЕ

- Хантемиров Наиль Равильевич
  Начальник управления по защите коммерческой тайны
  и информационной безопасности
  ПАО «Уралмашзавод»

Необходимо определить, куда ты попал, вариантов не очень много:

- Служба безопасности (DLP, OSINT, Forensic)
- Дирекция по информационным технологиям (СА , ЭЦП, Антивирус)
- Служба внутреннего аудита (Нормативная документация, комплаенс)
- Прямое подчинение руководителю

DLP

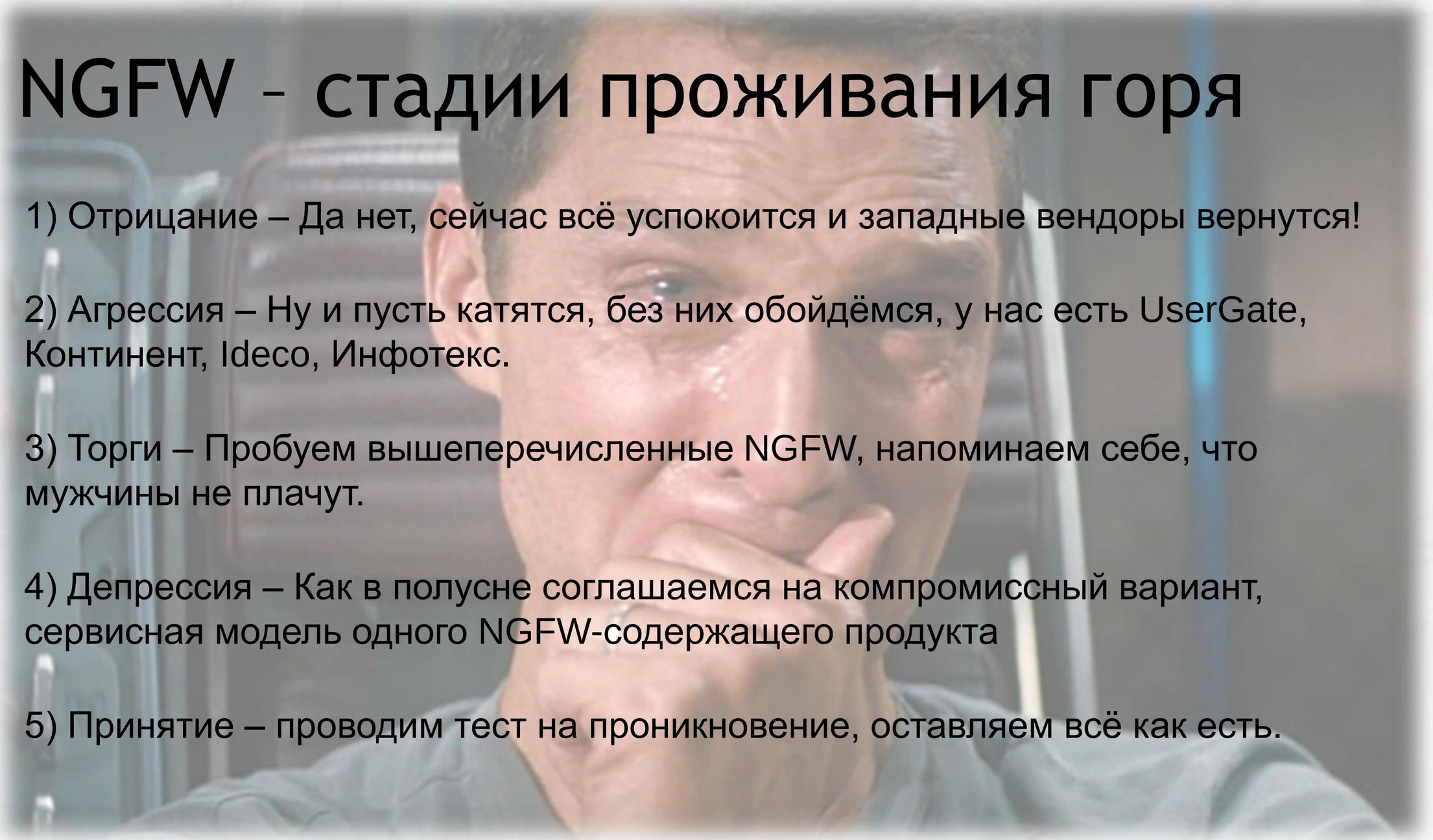
20% - выявление утечки чувствительной информации,
80% - поиск внутренних вредителей

Кейс: Менеджер по закупкам высылает конкурентный лист на почту одному из участников торгов ООО «Рога и копыта»:

- Нарушение регламента;
- Необходимость проверить данного менеджера на аналогичные случаи.

- Необходимо разобраться работает ли ООО «РиК» с какими-то ещё менеджерами или только с этим?
- Выяснить обороты у ООО «РиК», согласно СПАРКу?
- Поднять данные, как проходили остальные тендерные процедуры с участием ООО «РиК»?
- Выяснить, кто работает в ООО «РиК», как они аффилированы с менеджером?
- Проверить в социальных сетях связи менеджера с выявленными работниками ООО «РиК».
- Сравнить тендерную документацию с отгрузочными накладными, всё ли нам отгрузили, что обещали.
- Сравнить отгрузочные накладные с оприходованием на склад, совпало ли количество отгруженного по документам с тем, что принято физически.

NGFW – стадии проживания горя



1) Отрицание – Да нет, сейчас всё успокоится и западные вендоры вернутся!

2) Агрессия – Ну и пусть катятся, без них обойдёмся, у нас есть UserGate, Континент, Ideco, Инфотекс.

3) Торги – Пробуем вышеперечисленные NGFW, напоминаем себе, что мужчины не плачут.

4) Депрессия – Как в полусне соглашаемся на компромиссный вариант, сервисная модель одного NGFW-содержащего продукта

5) Принятие – проводим тест на проникновение, оставляем всё как есть.

СОПКА

- Бесплатно
- Реально выявленные заражения
- Аргумент в спорах

Универсальные комбайны

2FA – необходимо защитить вторым фактором удалённые подключения через RDG 300-500 пользователей.

	VPN и VDI	Linux	Windows	Облачные приложения (SAML)	API (Web)
Telegram	✓	✓	✓	✓	✓
[illegible]	✓	✓	✓	✓	✓
SMS или звонок	✓	✓	✓	✓	✓
[illegible]	✓	✓		✓	✓
U2F / FIDO токены				✓	✓
Биометрия				✓	✓

Молодой развивающийся продукт, который только выходит на рынок

Плюсы:

- Цена в 4 раза ниже, чем у многофункциональных конкурентов;
- Индивидуальный подход;
- Внедрение большинства пожеланий.

Минусы:

- Детские болезни, баги.

Ключевой момент – техническая поддержка

Awareness

- ✓ 15 курсов по теме ИБ в SCORM формате с интерактивными элементами, из них 3 курса в виде игры;
- ✓ Фишинговый модуль (3 вида атак, с возможностью прикрепления вложений, выбора домена отправителя и страницы переадресации, маркерами для максимальной персонализации письма);
- ✓ Возможность имитации фишинговой атаки с использованием USB-накопителей;
- ✓ Синхронизация с несколькими экземплярами AD;
- ✓ Модуль автоматизации (Расширенный мастер создания правил);
- ✓ Отчеты;
- ✓ Использование встроенной и внешней СДО;
- ✓ Набор готовых шаблонов и форм для тестовых фишинговых рассылок;
- ✓ Брендирование курсов, СДО, аналитического отчета по брендбуку Заказчика;
- ✓ Базовая кастомизация курсов;
- ✓ Разработка коннектора к внешней СДО;
- ✓ Техническая поддержка.

Awareness

Всего	Выдержали	Открыли	Эффективность
361	322	38	10,80%
357	298	59	16,53%
361	242	116	32,96%

Новости не из приятных. У нашего коллеги сгорела квартира. Вся семья живет у родственников. Руководство Компании организовало сбор гуманитарной помощи (спальные принадлежности, посуда, канцтовары - у коллеги двое детей школьного возраста - и т.д. Примерный список вещей представлен ниже) и денег, чтобы смогли сделать хотя бы минимальный ремонт после пожара и вернуться домой. Кто сколько может, никакой принудиловки. Просто всегда следует помнить, что любой из нас может оказаться в схожих обстоятельствах.
Реквизиты для сбора средств, контакты для сбора вещей и примерный список того, что может понадобиться, см. ниже. Если Вы предпочитаете помочь вещами, убедительная просьба, чтобы они были новыми.

По инициативе Службы крови РФ ФМБА России, поддержанной Министерством обороны РФ, мы присоединяемся к акции «Сдавайте кровь – делитесь жизнью». В течение месяца на нашей территории будет работать мобильный пункт приёма крови. Объём забора крови в каждом конкретном случае зависит от актуальной потребности в определённых группах крови. Кровь наиболее востребованных групп сдаётся в объёме 550 мл, остальных – 450 мл. К наиболее востребованным на данный момент относятся: AB (IV) Rh-, Rh+; 0 (I) Rh-; B (III) Rh-; A (II) Rh+.
Донация является обязательной. Подумайте о том, что именно ваша кровь может спасти чью-то жизнь…

На данный момент у вас насчитывается **пропуск двух рабочих дней** без уважительной причины.
Во вложении доступен табель учёта рабочего времени.
Необходимо подтвердить информацию о количестве отработанных дней в предыдущем месяце.
Если есть больничный или командировочный лист, то предоставить их в ответном письме в виде скана.
Ответ нужно предоставить до конца рабочего дня, иначе заработная плата за этот месяц будет перерассчитана в сторону уменьшения, исходя из текущих данных.

Полнодисковое шифрование

Касперский для бизнеса - Расширенный

Мобильная форензика

Мобильный криминалист Эксперт

Дополнительные источники ресурсности

Вендоры

Системные интеграторы

Управляющие компании

Стажёры

Не сдавайтесь -
стройтесь

Готов ответить
на ваши вопросы

E-mail: N.Khantemirov@uralmash.ru