



Как изменился ландшафт информационных рисков и угроз для промышленных предприятий за последние три года, и как отреагировала на них ИБ-отрасль

Мухортов Юрий,
директор департамента специальных проектов
АО «ЭЛВИС-ПЛЮС»



**RISK
AHEAD**



ТОП-5 глобальных рисков

В 2014–2015 годах наиболее вероятны следующие риски:

1. Неравенство доходов.
2. Экстремальные погодные явления.
3. Безработица и частичная занятость.
4. Изменения климата.
5. Кибератаки.



ТОП-5 глобальных рисков

По степени возможного влияния наиболее разрушительной будет реализация следующих рисков:

1. Фискальный кризис.
2. Изменения климата.
3. Водный кризис.
4. Безработица и частичная занятость.
5. Коллапс критической информационной инфраструктуры и сетей.

Источник: Global Risks 2014, Ninth Edition published by the World Economic Forum





Ландшафт рисков для промышленных предприятий



Источник: Global Risks 2014, Ninth Edition published by the World Economic Forum



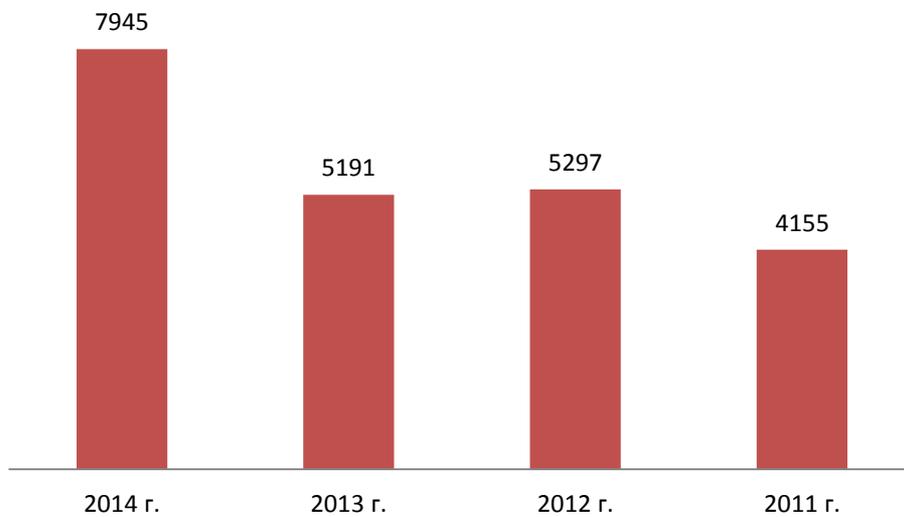
Наиболее быстрорастущие источники угроз ИБ в нефтегазовой сфере в процентах прироста по отношению к 2013 г.



Источник: PwC “Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015”



Общее количество уязвимостей



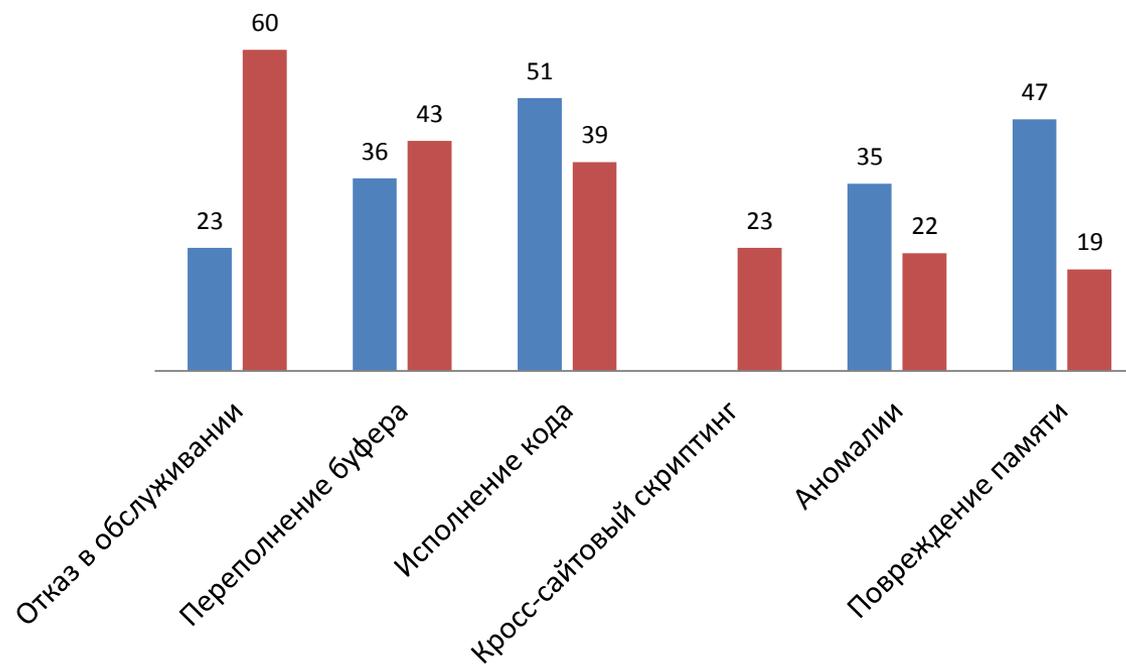
Источник: PwC “Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015”



Основные векторы атак

Процент организаций, подвергшихся хотя бы одной атаке указанных типов

■ 2013 г. ■ 2014 г.



Источник: Check Point 2015 security report



**Топ-5 приоритетных направлений ИБ в 2015 г.
по результатам исследования PwC
(опрошено почти 10 000 специалистов из более чем 150 стран)**

Предотвращение



Источник: PwC "Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015"

Обнаружение



Источник: PwC "Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015"

Защита



Источник: PwC "Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015"



Реагирование



Источник: PwC "Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security Survey 2015"

ТОП-тренды в сфере кибербезопасности

- Усиление государственного регулирования
- Инциденты кибербезопасности
- Изменения характера киберпреступности
- Мобильные устройства
- Безопасность персональных данных
- Утечки информации
- Облачные вычисления
- Социальные сети
- Проблема личных устройств (BYOD)



Что дает ИБ бизнесу?

Повышение
конкурентоспособности



Если бизнес-процесс напрямую не генерирует денежные потоки,
это еще не значит, что он не способствует росту бизнеса.

Что дает ИБ бизнесу?



О Компании

- Ведущий российский системный интегратор в сфере ИБ с отличной репутацией
- Почти 25 лет успешной работы на рынке ИБ
- Разработчик и производитель средств защиты информации

История



Лицензии и сертификаты

ЭЛВИС-ПЛЮС имеет все необходимые лицензии и сертификаты, позволяющие осуществлять деятельность в области защиты информации.

ФСТЭК

ФСБ

**Министерство
обороны РФ**





Наша команда

170

высококвалифицированных
сотрудников,
60% из которых это
специалисты технического
подразделения

Более 50

сертифицированных
специалистов

**8 кандидатов
наук**

10

аккредитованных
аудиторов

Сотрудники отмечены
15 наградами
Гостехкомиссии России
(ФСТЭК России)
«За заслуги в защите
информации»

Членство в Ассоциациях



Ассоциация защиты информации (АЗИ)



ЕВРААС (Научно-технический центр)



Ассоциация предприятий компьютерных и информационных технологий (АП КИТ)



ABISS (Сообщество пользователей стандартов по информационной безопасности)



Экспертиза

ЭЛВИС-ПЛЮС

аккредитована Роскомнадзором
для привлечения к проверкам
операторов ПДн, является органом
по аттестации ФСТЭК России, а также
регулярно привлекается к
подготовке законодательных
актов и нормативных
документов

Партнеры



Мы используем в своих проектах лучшие разработки мировых и отечественных производителей

и еще более 30 компаний-производителей программного и аппаратного обеспечения.



Продукты сетевой безопасности собственной разработки



Разрабатывается с 1996 г.

Ключевые преимущества VPN/FW «ЗАСТАВА»



- Высокий уровень масштабирования системы
- Централизованное иерархическое управление в режиме реального времени
- Низкая стоимость владения
- Разделение полномочий по управлению системой
- Высокая производительность и надежность системы
- Использование международных стандартов и протоколов сетевой защиты
- Поддержка механизмов качества обслуживания
- Гибкость поставки системы

Продукты сетевой безопасности собственной разработки



**БАЗОВЫЙ
ДОВЕРЕННЫЙ
МОДУЛЬ**

Новинка 2014 года



Карта услуг и решений Компании



ПРИВЕДЕНИЕ В СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

- Система защиты ИС персональных данных
- Система защиты АБС
- Система защиты ГИС
- Система защиты ИС коммерческих организаций
- Система защиты ИС платежной системы
- Система аттестация объектов автоматизации



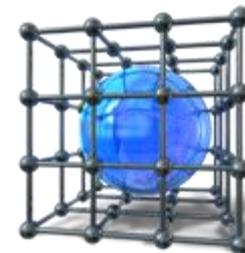
АУДИТ И КОНСАЛТИНГ

- Комплексный аудит
- Тесты на проникновение
- Анализ/оценка защищенности приложений
- Оценка соответствия требованиям законов и стандартов
- Технический аудит
- Аудит исходного кода приложений
- Обследование бизнес-процессов
- Разработка и реализация процессов управления ИБ



ОБЛАКА и ЦОДы

- Создание защищенных виртуальных рабочих мест VDI
- Защита периметра при использовании VDI
- Защищенный мобильный доступ
- Защита среды виртуализации серверов
- Антивирусная защита виртуальной среды
- Комплексная защита виртуальной среды
- Разграничение доступа к функциям управления виртуальной средой



УПРАВЛЕНИЕ ИБ

- Система создания Центра управления ИБ (SOC)
- Система мониторинга событий ИБ (SIEM)
- Система контроля действия пользователя и администраторов
- Система аудита защищенности и контроля соответствия
- Система анализа исходных кодов
- Система управления непрерывностью бизнеса
- Система автоматизации процессов управления ИБ
- Система визуализации и анализа рисков сетевой безопасности



УПРАВЛЕНИЕ ДОСТУПОМ

- Управление идентификационными данными пользователей
- Управление доступом к веб-приложениям
- Аудит и контроль полномочий пользователей
- Управление привилегированными учетными записями
- Защита от несанкционированного доступа
- Система аутентификации, авторизации и учета



СЕТЕВАЯ БЕЗОПАСНОСТЬ

- Система защищенного удаленного доступа для ИС
- Система защиты каналов связи распределенной ИС
- Система криптозащиты широкополосных каналов связи
- Система обнаружения и предотвращения вторжений
- Система защиты периметра нового поколения (NGFW)
- Система защиты от DDOS



ЗАЩИТА ПРИЛОЖЕНИЙ

- Удостоверяющий центр
- Криптопровайдеры
- Система защиты баз данных
- Система шифрования дисков и баз данных
- Система защиты ERP-систем на базе SAP
- Система предотвращения утечек данных (DLP)
- Система контроля и управления печатью
- Система безопасности мобильных устройств (MDM)
- Система противодействия мошенничеству (антифрод)



СОПРОВОЖДЕНИЕ И АУТСОРСИНГ

- Техническая поддержка продуктов защиты информации
- Техническая поддержка систем защиты информации
- Мониторинг систем защиты информации
- Аутсорсинг систем защиты информации





ЗАЩИТА АСУ ТП

- Оценка уровня кибербезопасности АСУ ТП
- Оценка требованиям регуляторов
- Создание комплексной системы защиты АСУ ТП и КВО
- Разработка ОРД для КВО



ЗАЩИТА ОТ ВРЕДОНОСНОГО КОДА

- Антивирусная защита
- Система защиты электронной почты
- Система контентной фильтрации веб-трафика
- Система защиты виртуальной инфраструктуры





Ваши вопросы?