



Кибер угрозы, как защитить свои данные

Руководитель департамента автоматизации
Чудин Андрей



ФГИС «Меркурий»

С 1 января 2018 все грузы, подконтрольные Госветнадзору, подлежат обязательной электронной сертификации в Федеральной государственной информационной системе «Меркурий», которая отслеживает их на протяжении всего жизненного цикла: от сырья до готового продукта на полке конкретного магазина

Для кого сертификация обязательна



Мясокомбинаты



Птицефабрики



Производители морепродуктов



Молочные заводы



Дистрибьюторы



Торговые сети



Для оптовой и розничной торговли

- Не нужно хранить бумажные ВСД
- Через портал «Меркурий» можно легко найти ВСД, в системе хранятся три года
- С 01.01.2018 поставщики не обязаны предоставлять бумажный документ, а смогут указать 32-значный код или QR код
- Гашение входящих ВСД
- Оформление возвратов через ВетИС



Поддержка в 1С

- Планируется реализовать интеграцию с ВетИС в части оптовой и розничной торговли в типовых конфигурациях:
 - ERP управление предприятием
 - Комплексная автоматизация 2.0
 - Управление торговлей 11
 - Розница
- Срок выхода 1-й квартал 2018 г.
- Для полноценной интеграции в ВетИС в информационной базе должен вестись полноценный партионный учет

НАШИ НАПРАВЛЕНИЯ:



Внедрение
и сопровождение



Веб-студия



Электронные
подписи



Отчетность
через интернет



Учебный
центр

НАШИ ПРОЕКТЫ:



Решения
для общепита



ЕГАИС



54-ФЗ:
онлайн-кассы



Маркировка
меха



Автоматизация
медицины



Кибер угрозы, как защитить свои данные

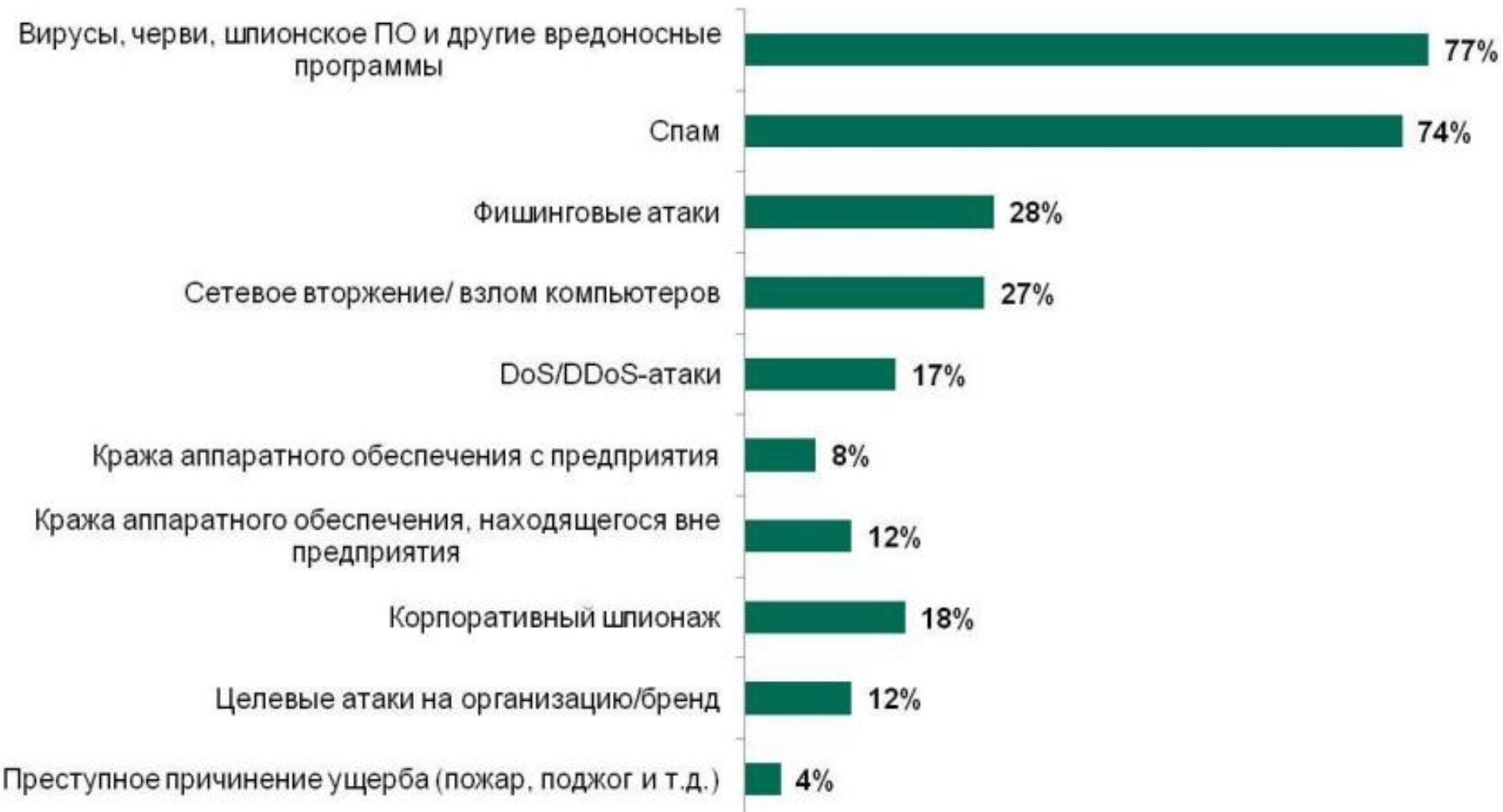


9 из 10 компаний сталкиваются с внешними киберугрозами

- За последний год 91% компаний в мире сталкивались с угрозами информационной безопасности.
- В России этот показатель еще выше – 96%.
- 50% вирусных атак закончилась потерей данных



Типы внешних угроз, с которыми сталкивались Российские компании





Антивирусная защита

- 31% компаний в России внедрили антивирусную защиту (Великобритания – 92%, США – 82%)
- 44% российских компаний считают киберугрозы одним из главных бизнес- рисков
- В большинстве компаний популярен реактивный подход к IT-безопасности. Компании начинают вкладывать деньги в систему защиты после того, как инцидент уже произошел.



Внешние угрозы

- Вирусы / блокираторы / шифровальщики
- Спам
- Удаленный взлом
- Фишинг / подмена данных
- Хищение мобильных устройств

95%

всех киберинцидентов
вызваны человеческими
ошибками





Защита от вирусов и шифровальщиков



Ежедневный архив данных

- Облако (Яндекс.Диск, Google drive, DropBox)
- 1С:Облачный архив
- Выделенный компьютер для резервного копирования
- Внешний жесткий диск
- Флэшка





Внимание к открываемым файлам

«exe», «vbs» и «scr»



Сетевая защита

- Своевременное обновление Windows
- Настройка доступа из интернет к рабочим местам сотрудников
- Открытый доступ в интернет (социальные сети, развлекательные порталы и т.д.)





Антивирус





Обучение сотрудников!

- Обучение сотрудников основам информационной безопасности
- Правила обработки электронной почты и подозрительных файлов





Отчетность

Онлайн-
касса

ЕГАИС

Клиент-
банк

ШУБаИС

1С

ЭЛН

ВетИС





Нужна консультация?

Отмечайте в анкетах

Звоните +7 (3902) 306-119

Спасибо за внимание!