Тенденции инцидентов информационной безопасности в Республике Казахстан

Государственная техническая служба

Profit Government Day

Жакупов Жанат
zh_zhakupov@kz-cert.kz

Основные направления деятельности Предприятия






1	Служба реагирования на компьютерные инциденты KZ-CERT
2	Центр мониторинга защиты е-правительства
3	Услуги по сопровождению единого шлюза доступа к Интернету для ГО РК
4	Испытание объектов информатизации на соответствие требованиям информационной безопасности
5	Аттестационное обследование информационных систем на соответствие требованиям информационной безопасности

Перечень планируемых услуг

7	Защита от DDoS-атак
8	Техническое исследование вредоносного программного обеспечения
9	Исследование мошеннических действий (antifraud)

СЛУЖБА РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

KZ-CERT

Главная миссия – снижение уровня угроз информационной безопасности для пользователей казахстанского сегмента Интернета

KZ-CERT обеспечивает сбор и анализ информации по компьютерным инцидентам, консультативную и техническую поддержку пользователям в предотвращении угроз информационной безопасности

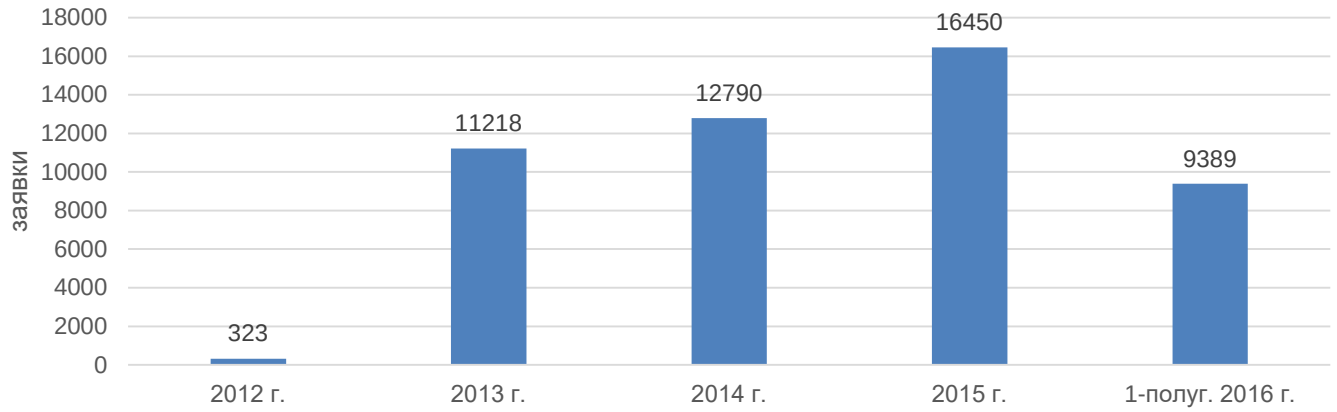
KZ-CERT обеспечивает взаимодействие с Интернет-сообществом по вопросам выявления и разрешения компьютерных инцидентов, а также выработки мер по предотвращению предполагаемых инцидентов в дальнейшем

Обеспечение надежного, доверительного центра обращений пользователей Интернета в случае возникновения инцидентов информационной безопасности

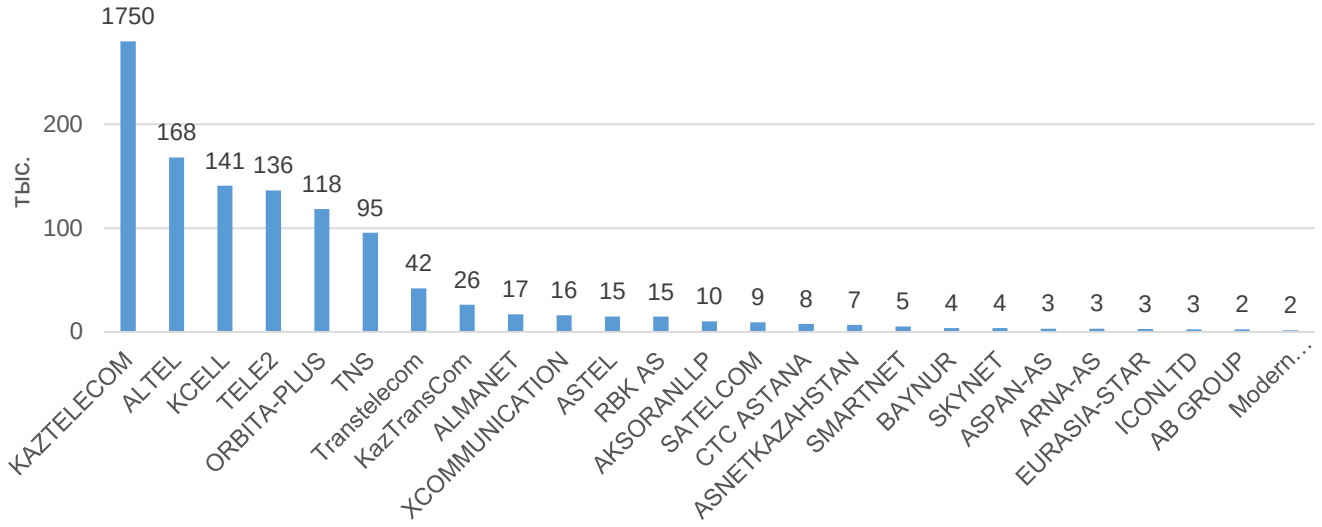
Направления деятельности KZ-CERT

Направления деятельности служб CERT	*Текущая деятельность*	*Перспективные направления*
Сервисы реагирования	▪ Оповещение и Предупреждение об инцидентах ▪ Обработка инцидентов ▪ Координация реагирования на инциденты ▪ Обработка и оповещение об уязвимостях ▪ Анализ уязвимостей, координация реагирования на уязвимости	▪ Реагирование на инциденты на месте ▪ Поддержка жертвы после инцидента
Профилактические услуги	▪ Объявления на интернет-ресурсе kz-cert.kz о текущих угрозах и шагах, предпринимаемых для борьбы с ними, а также о тенденциях в области ИБ ▪ Слежение за развитием технологий	▪ Распространение информации о системах безопасности ▪ Обнаружение вторжения посредством анализа журналов систем обнаружения вторжений ▪ Анализ и оценка систем безопасности
Обработка артефактов (вредоносное ПО)	▪ Анализ вредоносного ПО ▪ Реакция на артефакты	▪ Координация реагирования на артефакты
Управление качеством систем безопасности	▪ Консультирование по вопросам безопасности ▪ Повышение осведомлённости ▪ Обучение / Тренинги	▪ Анализ рисков и угроз ИБ

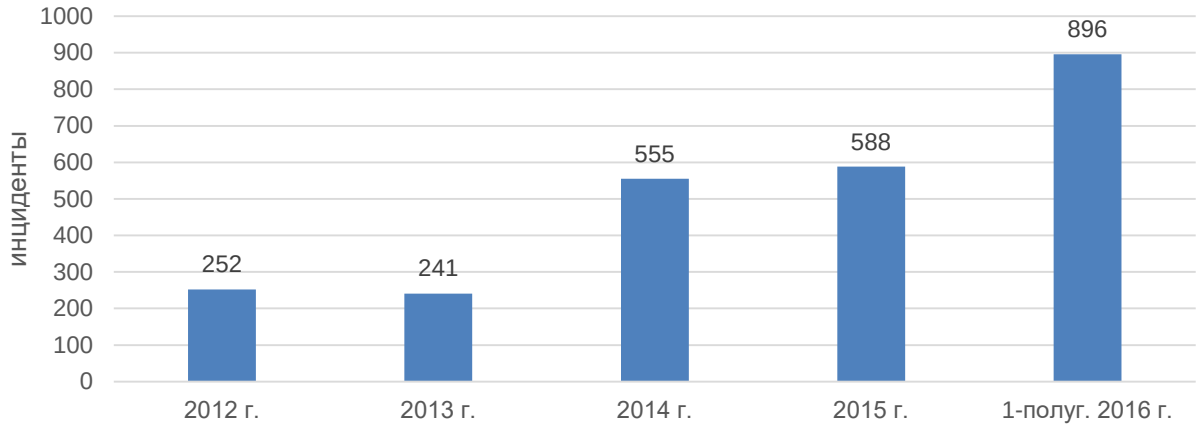
БОТНЕТЫ



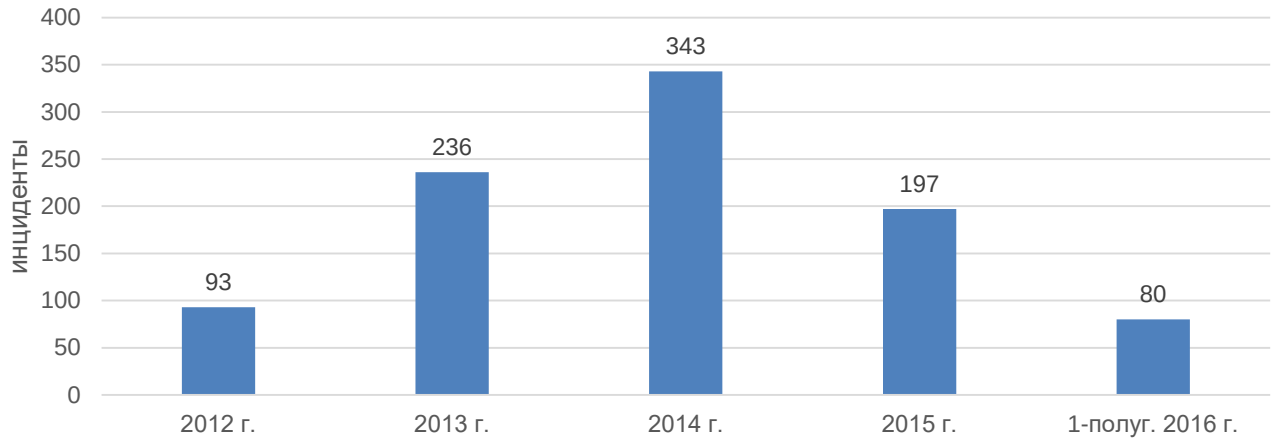
Распределение инцидентов по провайдерам

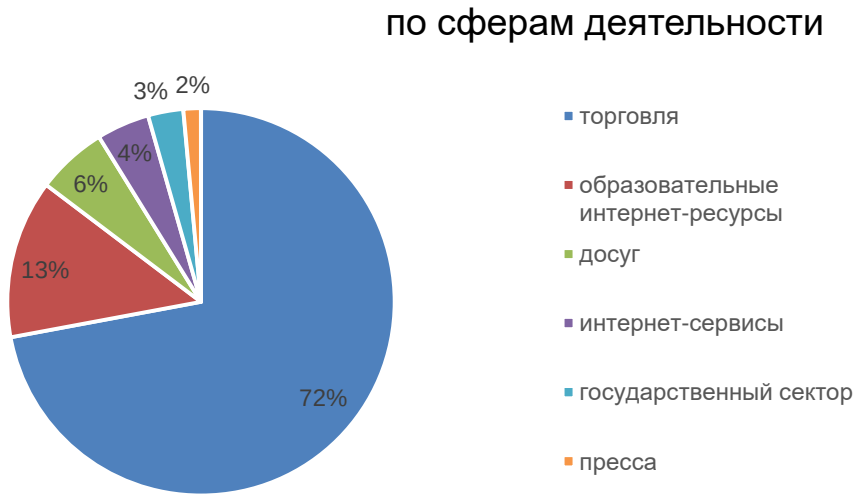


ВЗЛОМЫ ИНТЕРНЕТ-РЕСУРСОВ

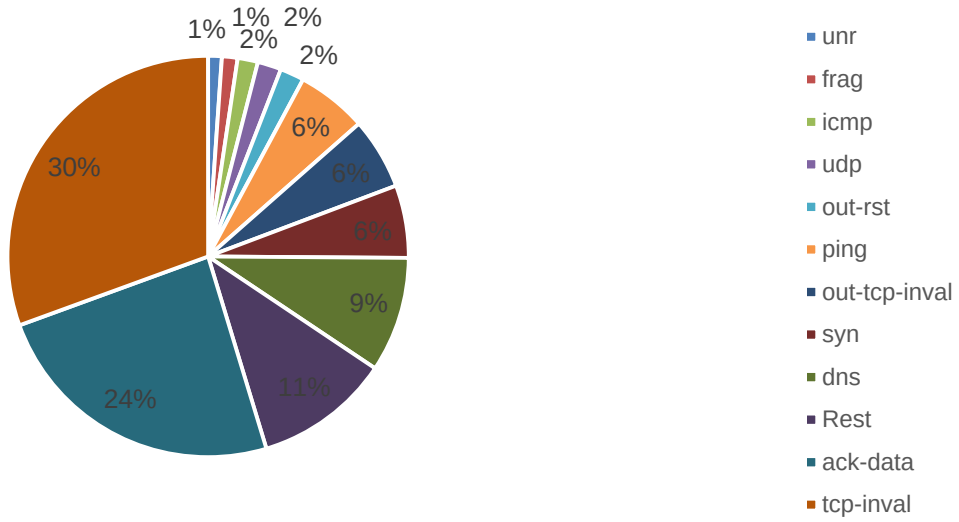


ФИШИНГ

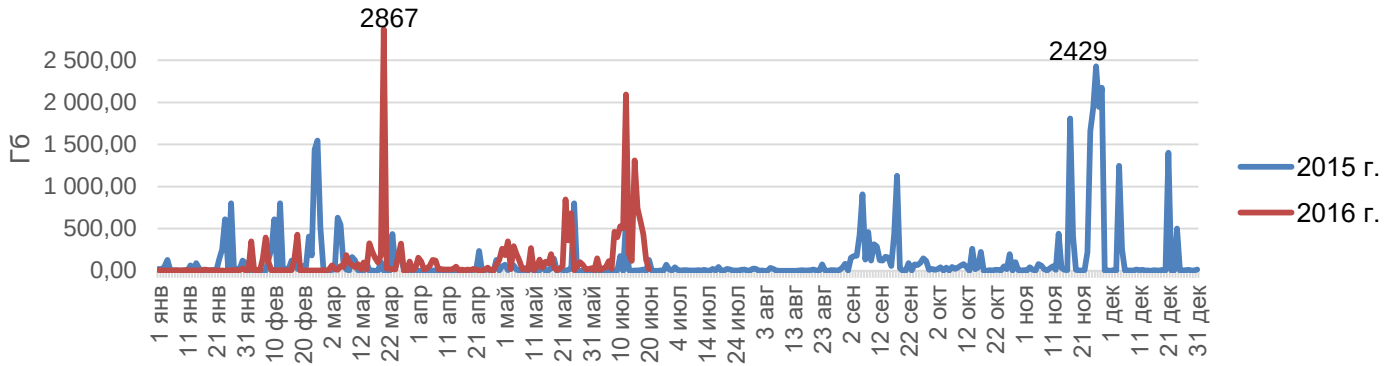

400
350
300
250
200
150
100
50
0
инциденты
93
236
343
197
80
2012 г.
2013 г.
2014 г.
2015 г.
1-полуг. 2016 г.


по сферам деятельности
3%
2%
4%
6%
13%
72%
торговля
образовательные интернет-ресурсы
досуг
интернет-сервисы
государственный сектор
пресса

DDOS

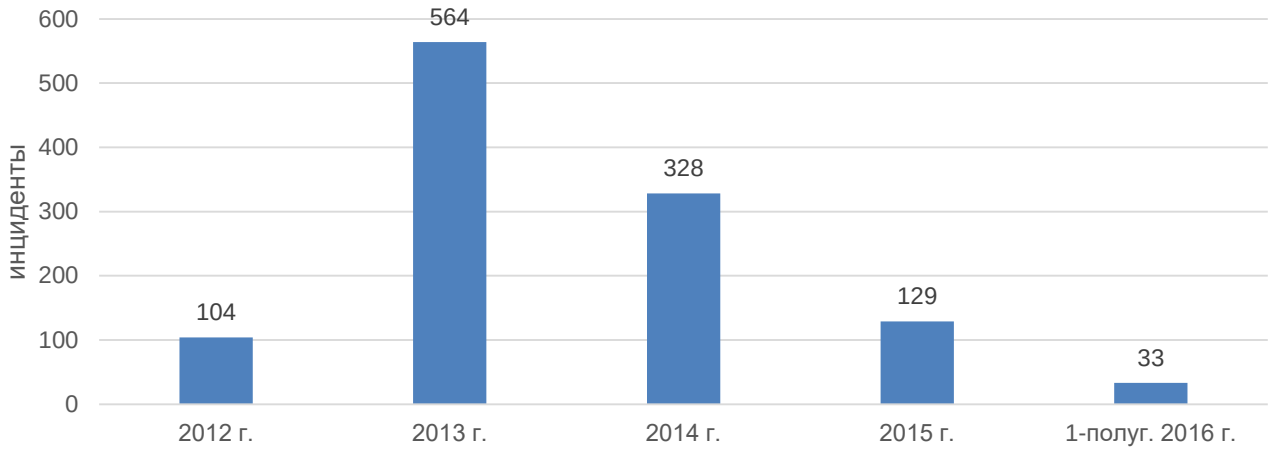


Сетевые протокола



Отраженный вредоносный трафик по дням, Гб

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ



Распространение вредоносного программного обеспечения

В 2016 г. наблюдалась высокая активность (57%) вирусов-блокировщиков, вымогающих деньги у пользователей якобы от лица правоохранительных органов РК и вирусов-шифровальщиков, таких как Vault. В 2015 г. этот показатель был 41%.

Зафиксировано и проанализировано несколько компонентов шпионских целевых атак.

СТАТИСТИКА

В 2016 г. направлено **10 816** писем-уведомлений и рекомендаций, в том числе:
316 государственным органам и организациям РК

862 оповещения об инцидентах Службам CERT, владельцам и провайдерам интернет-ресурсов других стран.

Статистика по оповещению зарубежных стран

Внешние проблемы

- Большое количество угроз ИБ. Число уникальных вредоносных образцов, создаваемых в сутки (в мире) - более 200 000
- Активное развитие ИКТ в Казахстане в числе лидеров по доле зараженных вредоносными программами устройств (по данным антивирусных компаний)
- Высокий уровень распространения в Казахстане специфических видов угроз - целевых атак

Пути решения

- Создание групп реагирования на компьютерные инциденты у операторов связи, хостинг-провайдеров, в предприятиях критической инфраструктуры, в банках второго уровня и других частных компаниях
- Обучение и подготовка квалифицированных кадров
- Обмен опытом с зарубежными профильными организациями

kz-cert.kz

Подробная информация о деятельности KZ-CERT

Свежие новости и статьи из области информационной безопасности на казахском, русском и английском языках

Возможность отправить заявку о компьютерном инциденте в KZ-CERT

Сервис по проверке интернет-ресурсов на наличие вредоносного ПО

KZ-CERT на KazTube, YouTube, Kivvi

С целью повышения общего уровня грамотности и культуры населения Республики Казахстан в области информационной безопасности разработаны информационные и обучающие видеоролики, размещенные на популярных видеохостингах

KZ-CERT в социальных сетях

На официальных страницах Службы KZ-CERT в социальных сетях можно ознакомиться с новостями компьютерной безопасности и задать вопрос специалистам Службы