# JSOC Security flash report Q1 2015

Отчет **JSOC Security flash report Q1 2015** основан на данных, полученных в коммерческом центре мониторинга и реагирования JSOC за первый квартал 2015 года.

Отчет предназначен для информирования служб ИТ и ИБ о текущем ландшафте угроз и основных трендах.

## Оглавление



## Ключевые выводы

01 Компаниям следует обратить пристальное внимание на обеспечение безопасности веб-приложений: на их долю приходится 41,2 % всех внешних атак

02 В очередной раз подтверждена гипотеза о том, что внешние злоумышленники часто и целенаправленно атакуют в ночное время (доля критичных внешних инцидентов ночью составляет 45,2 %)

03 Утечки информации продолжают оставаться самой часто реализуемой (30,3 %) и критичной, однако, не единственной внутренней угрозой

# Методология

## Общие положения

«Статистика угроз» является сводным материалом и результатом анализа инцидентов, выявленных командой JSOC как в рамках оказания своих регулярных услуг мониторинга и реагирования на инциденты, так и консультативно-аналитической поддержки компаний российского рынка. Деление инцидентов по категориям и типам угроз основано на внутренней классификации и методологии самого JSOC. Отчет является только информативным материалом и не претендует на то, что приведенные данные полностью отражают все угрозы российского рынка. Команда JSOC постоянно работает над улучшением объема и качества собираемой и анализируемой информации.

## Сводная статистика за отчетный период

- Всего за первый квартал 2015 года в JSOC было зафиксировано **34 743** события с подозрением на инцидент.
- Доля критичных инцидентов составила **8,4 %** от общего числа.
- Среднее время принятия инцидента в работу специалистом JSOC с момента выявления составило **15,5 минуты**. Среднее время на подготовку и предоставление аналитической справки об инциденте и рекомендаций клиенту JSOC по критичным инцидентам составило **24,5 минуты** и **86 минут** по всем остальным.
- Соблюдение клиентских SLA за первый квартал составило **98,3 %**.
- **54,2 %** исследуемых событий зафиксировано при помощи основных сервисов инфраструктуры и базовой безопасности: межсетевые экраны и сетевое оборудование, VPN, AD, почтовые серверы, базовые средства защиты (антивирусы, прокси-серверы, IPS).
- При этом стоит отметить, что оставшиеся инциденты (**45,8 %**), выявляемые при помощи сложных интеллектуальных средств защиты или анализа событий бизнес-систем, несут гораздо больший объем информации и критичность для информационной и экономической безопасности клиента. Информация по данным инцидентам позволяет глубже и полнее видеть картину защищенности компании и своевременно предотвращать критичные, таргетированные инциденты.

## Классификация инцидентов по критичности

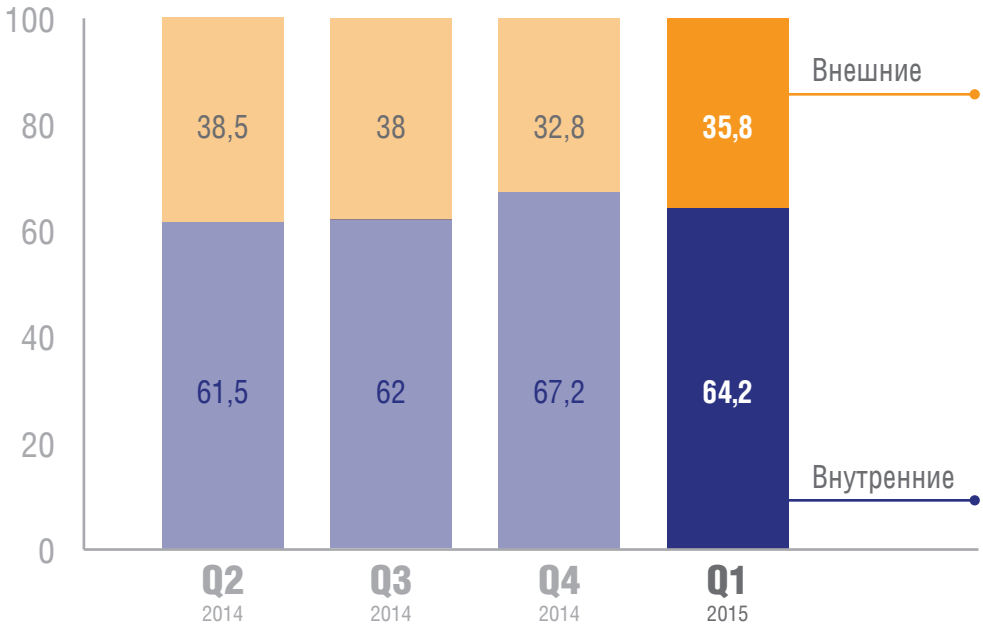
Основным критерием при классификации инцидентов по критичности является воздействие инцидента на ключевые бизнес-процессы и данные заказчика.

Инцидент считается критичным, если в его результате возможны и высоковероятны следующие события:

- длительное прерывание (более получаса) или остановка функционирования систем и сервисов клиента, относящихся к категориям Business и Mission Critical;
- повреждение, потеря или компрометация критичной информации и учетных записей, включая сведения, относящиеся к персональным данным, коммерческой и банковской тайнам;
- прямые финансовые потери в результате действий внутренних сотрудников или киберпреступников суммой более 1 млн рублей.

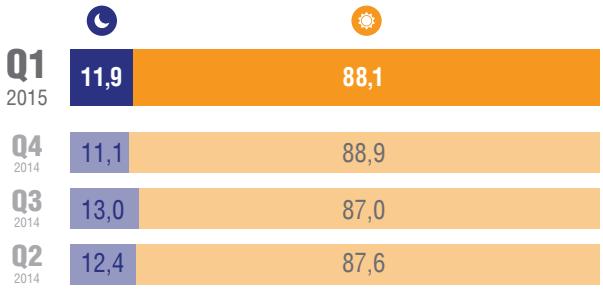
# Общие показатели по инцидентам

## Распределение инцидентов по внешним и внутренним[1] в %-ном соотношении от общего числа:

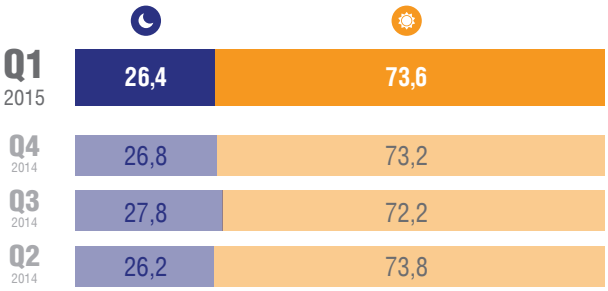



## Распределение количества инцидентов по времени суток

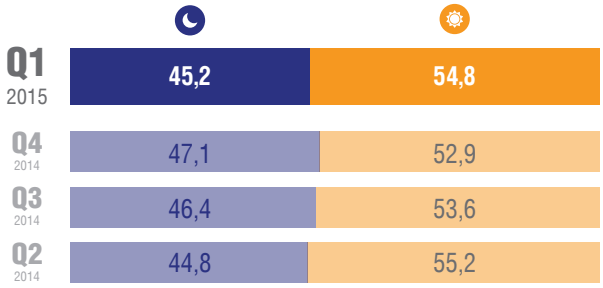
Общее распределение по времени суток (в %)




Распределение по критичным инцидентам (в %)




Распределение по критичным внешним инцидентам (в %)




Ночь
С 21:00 до 08:00 по времени расположения офиса заказчика

День
С 08:00 до 21:00 по времени расположения офиса заказчика

В первом квартале 2015 года ситуация по распределению инцидентов по времени суток не претерпела существенных изменений. Это позволяет говорить о том, что эти показатели будут стабильны в среднесрочной перспективе.

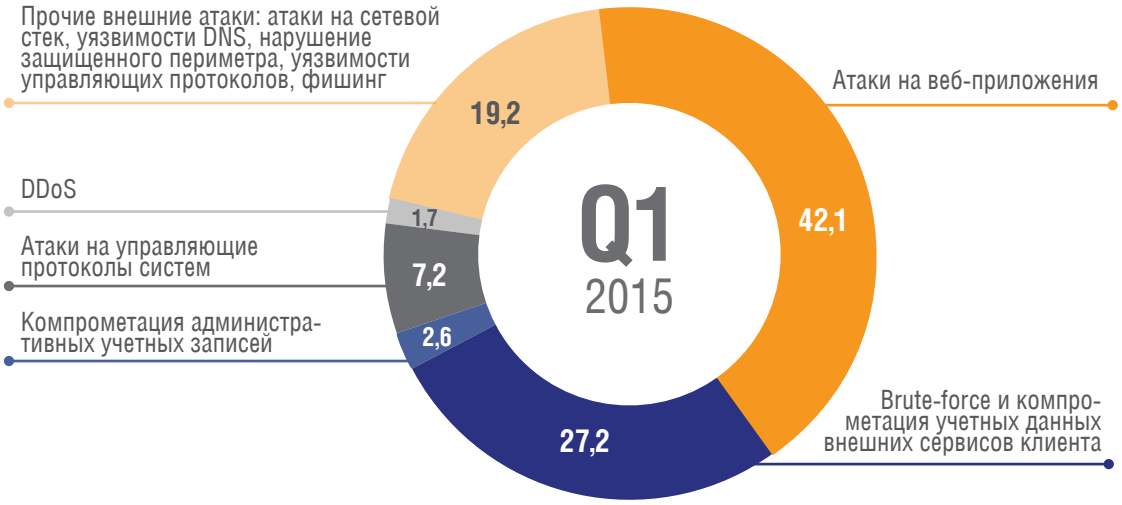
[1] К внутренним пользователям-инициаторам инцидента относятся все пользователи с возможностью доступа в локальную сеть без преодоления периметра, в том числе подрядчики и контрагенты

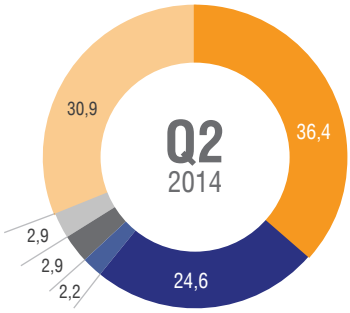
# Внешние инциденты

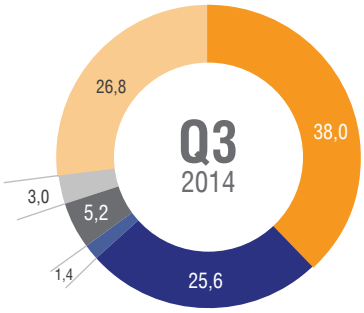
В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия лиц, не являющихся внутренними пользователями клиента.

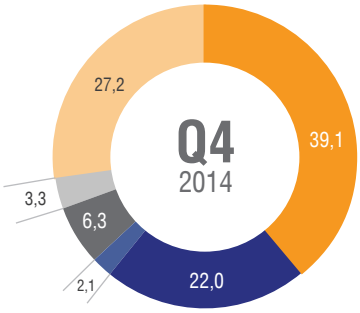
«Простые атаки», а именно действия, которые можно явно классифицировать как деятельность автоматизированных систем (бот-сетей), не приводящие к реальным инцидентам информационной безопасности: сканирование сетей, неуспешная эксплуатация уязвимостей и подборы паролей – из отчета исключены.

## **Направления атак** в %-ном соотношении от общего числа:




## Особенности внешних инцидентов в первом квартале 2015 г.

- Продолжается рост атак на уровень веб-приложения, в том числе благодаря по-прежнему актуальным уязвимостям Shellshock и уязвимости в http.sys. По оценке аналитиков JSOC, рост атак на веб-приложения уже является устойчивой тенденцией. Связано это с тем, что в последнее время наблюдается увеличение публично доступной информации по уязвимостям веб-приложений, при этом на самих веб-приложениях эти уязвимости устраняются недостаточно быстро.
- Зафиксирован существенный рост количества атак, направленных на компрометацию учетных данных внешних сервисов. Прежде всего компрометация касается массовых онлайн-сервисов, в том числе интернет-банкинга и онлайн-ритейла.
- Снижение доли «прочих внешних атак» предположительно связано с усилением базовой защищенности клиентов JSOC и может не отражать общую тенденции в целом по России.

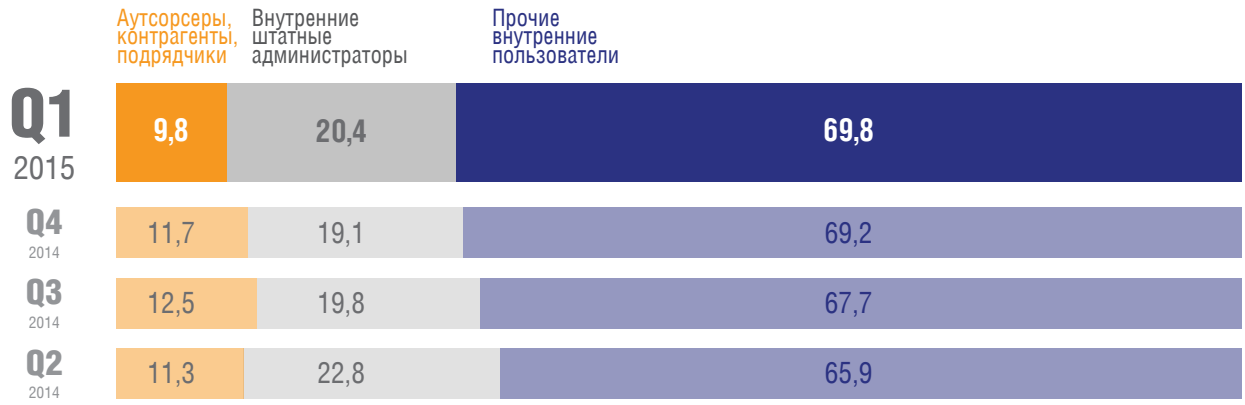

info@solarsecurity.ru
+7 (499) 755-0770

# Внутренние инциденты

В рамках данной части отчета рассматриваются инциденты, инициаторами и причиной которых становились действия внутренних сотрудников клиентов JSOC: халатность в соблюдении политик информационной безопасности или их прямое нарушение, утечки информации, компрометация или передача учетных данных сотрудников к внутренним системам, злонамеренные и незлонамеренные воздействия на бизнес-процессы и функционирование систем клиента.

## Направления атак в %-ном соотношении от общего числа:


## Инициаторы внутренних инцидентов в %-ном соотношении от общего числа:



# Внутренние инциденты

## Распределение инцидентов по каналам утечек в %-ном соотношении от общего числа:


## Особенности внутренних инцидентов в первом квартале 2015 г.

- Существенный рост компрометации учетных данных наблюдается среди сотрудников финансовых подразделений компаний: расчетные центры, казначейство и т.д. Возможная причина – более пристальное внимание злоумышленников к прямым финансовым потокам и возможности быстрой монетизации инцидента.
- В очередной раз зафиксировано снижение доли нарушения политик доступа в Интернет. Предположительно это связано с тем, что в компаниях стали осознавать этот риск и закрывать его техническими и организационными мерами. По оценке экспертов JSOC, количество и доля таких инцидентов будут постепенно снижаться.
- Уменьшение доли утечек конфиденциальных данных, вероятно, связано со снижением деловой активности в первом квартале года. Также после резкого всплеска в четвертом квартале доля утечек будет стремиться к своему «обычному» значению в связи со стабилизацией экономической ситуации.
- Большой интерес с точки зрения утечек стала представлять информация об инфраструктуре (схемы сетей и особенности работы информационных систем). Вероятно, она используется для планирования и подготовки последующих атак и мошеннических схем.

# JSOC

**JSOC –** первый в России коммерческий центр мониторинга и реагирования на инциденты ИБ, являющийся провайдером сервисов безопасности (MSSP).

На всех этапах мониторинга и реагирования на инциденты ИБ JSOC обеспечивает защиту клиентских данных. Обеспечение безопасности реализовано как на физическом, так и на информационном уровне с помощью средств разграничения доступа, аудита работы специалистов JSOC, контроля целостности и защиты данных при передаче. JSOC сертифицирован по требованиям PCI DSS, что подтверждает зрелость процессов обеспечения безопасности.

Уже более десятка клиентов получают аутсорсинговые услуги JSOC. Сервис по мониторингу инцидентов был запущен в 2013 году, став первым подобным коммерческим центром в России. Сейчас в штате JSOC более 30 специалистов дежурной смены, аналитиков и экспертов, которые обрабатывают более 100 000 событий с подозрением на инциденты в год.

## Сервисы JSOC

- Мониторинг инцидентов
- Контроль защищенности
- Противодействие кибепреступности
- Эксплуатация систем ИБ
- Анализ кода приложений
- Анти-DDoS
- Защита web-приложений

## О компании Solar Security

Solar Security – это команда, создающая продукты и сервисы, позволяющие выстроить вертикаль управления и мониторинга ИБ, начиная с низкоуровневых инцидентов и заканчивая системами стратегической аналитики и ситуационными центрами по информационной безопасности.

Solar Security – это команда с двадцатилетним опытом разработки продуктов и собственная исследовательская лаборатория по анализу и прогнозированию инцидентов информационной безопасности. Наши знания позволяют гарантировать нашим клиентам уверенность в контроле над ситуацией в постоянно меняющемся мире внутренних и внешних киберугроз.

Solar Security – это продукты и сервисы, удобные в использовании и простые в восприятии. Они упрощают работу сотрудников ИБ, повышая их эффективность. Мы делаем технологии доступными руководителям и сотрудникам подразделений информационной безопасности, позволяя им выбрать удобный канал доставки в виде сервиса, приложения и комплексной системы.