CNews
ИЗДАНИЕ О ВЫСОКИХ ТЕХНОЛОГИЯХ

# Спасибо регуляторам: рост на рынке ИБ сохранится

Издание: CNews.ru, 1 декабря 2018 г.

Спикер: Михаил Савельев, директор по развитию бизнеса «Информзащиты»

**Главными действующими лицами как на глобальном, так и на российским рынке ИБ в 2017-2018 гг. оказались регуляторы: в западных странах в центре внимания были меры по защите персональных данных, в то время как в РФ с января 2018 г. вступил в силу закон о защите критической инфраструктуры. Требования регуляторов необходимо выполнять, что ведет к росту бюджетов на информационную безопасность.**

Информационная безопасность давно превратилась в самостоятельную индустрию, значение которой для бизнеса не меньше чем ИТ-инфраструктуры, которую призваны защищать решения в сфере ИБ. Правильно развернуть ИТ-системы – это лишь половина задачи, далее необходимо обеспечить защиту ИТ-ландшафта от многочисленных угроз. Структура угроз постоянно меняется, это связано как с появлением новых технологий, которые скрывают в себе новые неизвестные ранее типы уязвимостей, так и с организационным развитием криминальных сообществ и гонкой кибервооружений между государствами (state-sponsored cyber attacks).

Таким образом, структура угроз остается весьма пестрой – это целевые атаки, вирусные эпидемии (WannaCry, NotPetya, Bad), фишинг и воровство конфиденциальных данных методами социальной инженерии, утечки данных через сотрудников организаций. При этом заказчики проявляют все больший интерес к проактивной защите, то есть предотвращению атак, а не ликвидации их последствий: «Фокус смещается от «построения заборов» к мониторингу, к более тщательному планированию действий по восстановлению работоспособности систем», – констатирует **Михаил Савельев**, директор по развитию компании «Информзащита». При этом заказчики становятся более прагматичными: «Если нет четкой формулировки выгоды от продукта – ему просто нет места. Нести необоснованные издержки никто не готов», – говорит собеседник CNews.

Тем не менее, расходы на ИБ растут быстрее, чем рынок ИТ в целом. Согласно прогнозу Gartner, глобальные траты на информационную безопасность в 2018 г. вырастут на 12,4% и достигнут $114 млрд (3% от общих глобальных затрат на ИТ). Около половины всех расходов приходятся на услуги в области безопасности, причем особенно высокими темпами будут расти услуги класс security-as-a-service, предполагают аналитики американской компании. Среди программного обеспечения, развертываемого на стороне заказчика, наибольшим спросом пользуются решения в области сетевой безопасности ($10,9 млрд в 2017 г.) и продукты для защиты инфраструктуры (infrastructure protection, $12,6 млрд), а наиболее быстро растущим сегментом являются средства защиты облаков (прогнозируемый рост в 2018 г. – 64%).

**Структура глобальных расходов на ИБ, в млрд $**

| тип решений | 2 017 | 2 018 | | 2 019 | |
|---|---|---|---|---|---|
| Защита приложений | 2 434 | 2 742 | +13% | 3 003 | +10% |
| Защита облаков | 185 | 304 | +64% | 459 | +51% |
| Защита данных | 2 563 | 3 063 | +20% | 3 524 | +15% |
| Управление учетными данными (Identity Access Management) | 8 823 | 9 768 | +11% | 10 578 | +8% |
| Защита инфраструктуры (infrastructure protection) | 12 583 | 14 106 | +12% | 15 337 | +9% |
| Управление рисками (Integrated Risk Management) | 3 949 | 4 347 | +10% | 4 712 | +8% |
| Сетевая безопасность | 10 911 | 12 427 | +14% | 13 321 | +7% |
| другое ПО в области безопасности | 1 832 | 2 079 | +13% | 2 285 | +10% |
| ИБ-услуги | 52 315 | 58 920 | +13% | 64 237 | +9% |
| розничный/потребительский софт (consumer security software) | 5 948 | 6 395 | +8% | 6 661 | +4% |
| **Итого** | **101 544** | **114 152** | **+12%** | **124 116** | **+9%** |

*Источник: Gartner, 2018*

**Персональные данные – новая «валюта» цифрового мира**

По мнению аналитиков Gartner, ключевым фактором рост расходов на ИБ становится защита персональных данных, не менее 10% ИБ-расходов будет связано именно с этим направлением. В частности, спросом будут пользоваться решения в области предупреждения утечек данных (data loss prevention, DLP), управления учетными данными – IAM (Identity and Access Management), а также IGA (Identity Governance and Administration).

Внимание к защите ПДн было привлечено скандалом вокруг компании Cambridge Analytica, которая незаконно собирала данные пользователей Facebook для использования в предвыборных кампаниях в различных странах мира. Кроме того, в мае 2018 г. в Европе вступил в силу общий регламент по защите данных (General Data Protection Regulation, GDPR), который ужесточил требования по защите ПДн. Выполнение новых требований регулятора потребует дополнительных расходов со стороны международных ИТ-компаний.

С точки зрения пользователя идеальной защитой было бы полностью отказаться от публикации о себе каких-либо данных в сети. «Известны случаи, когда владельцы новых автомобилей выставляли фотографию в социальной сети, а через короткий промежуток времени машину угоняли. Другой пример – когда человек выставляет фото из отпуска с геотегом, а в этот момент совершается кража из его квартиры», – рассказывает **Мария Воронова**, директор по консалтингу Infowatch.

Данные о пользователях и их активности – «новая валюта в мире интернет-бизнеса», утверждает **Андрей Янкин**, заместитель директора центра информационной безопасности компании «Инфосистемы Джет»: «Чаще всего возможности пользователей по защите своих данных крайне ограничены. Можно лишь несколько сократить их передачу недоверенным обработчикам. Поэтому обеспечение приемлемой защиты такой информации (далеко не всегда относимой к персональным данным) – задача в первую очередь регуляторов».

**Во сколько обойдется защита критической инфраструктуры?**

В России как и в Европе 2017-2018 гг были отмечены активной деятельностью регуляторов. С 1 января 2018 г. вступил в силу 187-ФЗ – закон «О безопасности критической информационной инфраструктуры РФ», согласно которому в России должна быть создана централизованная система по обнаружению, предупреждению и ликвидации атак на критическую информационную инфраструктуру (КИИ). К элементам КИИ относятся инфо-телекоммуникационные системы, которые обеспечивают работу предприятий тяжелой промышленности, транспорта, энергетики, здравоохранения, финансового сектора и т.д. Компании, работающие в данных отраслях, должны составить перечень объектов КИИ и передать их во ФСТЭК.

За координацию мер по защите КИИ будет отвечать ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации компьютерных атак. К данной системе должны будут подключиться все операторы КИИ, чтобы предоставлять информацию об инцидентах. Территориально ГосСОПКА представляет распределенную сеть центров по обеспечению безопасности, общее руководство которой осуществляет Национальный координационный центр по компьютерным инцидентам (НЦКИ).

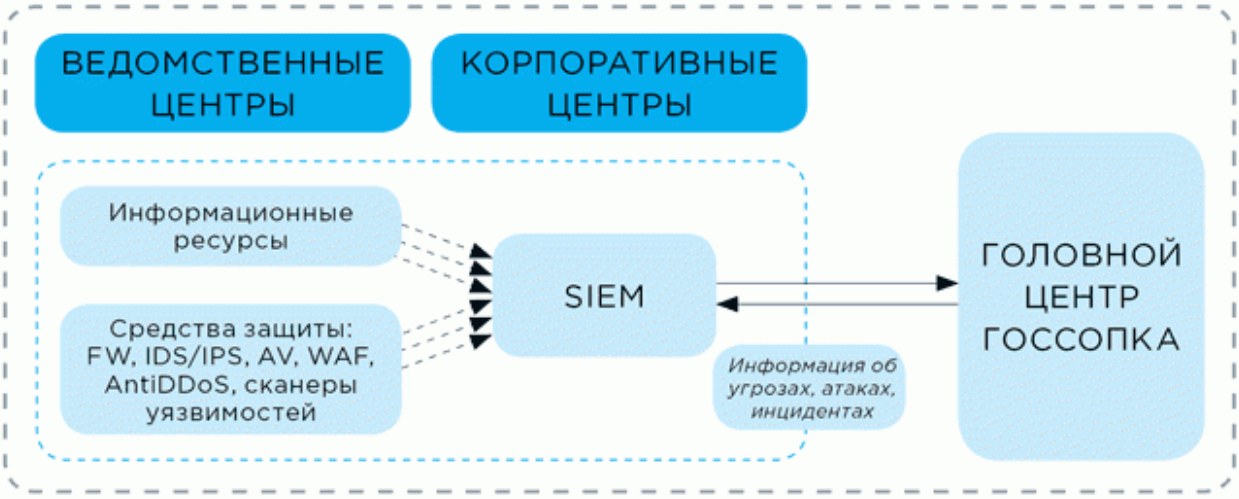
**Рис. 1. Иерархическая структура ГосСОПКА**


*Источник: «Инфосистемы Джет», 2017*

Реализация требований регулятора потребует инвестиций со стороны операторов критической инфраструктуры: «Наибольшее количество новых проектов в части информационной безопасности мы отмечаем именно в области защиты КИИ.

Они охватывают большое число объектов, к которым требования по ИБ ранее внутри организаций не предъявлялись. Определенно, требования по защите КИИ и подключению к ГосСОПКА породили новый специфический сегмент рынка. Мы видим перераспределение ИБ-бюджетов в этом направлении, но еще чаще речь идет о выделении дополнительного финансирования», – рассказывает **Андрей Янкин**.

**Рис. 2. Взаимодействие в рамках ГосСОПКА**




*Источник: «Инфосистемы Джет», 2017*

Технически есть два способа подключения к ГосСОПКА – создание собственного центра или подключение к аутсорсинговому центру внешнего оператора. Многие крупные организации уже сейчас располагают собственными центрами управлениями событиями ИБ (SoC, Security Operation Center). Модернизация SoC под требования ГосСОПКА зависит от наличия уже внедренных решений: «По идее, существующие SOC могут быть с успехом модернизированы для взаимодействия с ГосСОПКА, и это не потребует больших финансовых вливаний. Затраты на модернизацию существующей инфраструктуры SOC зависят от входящих в него элементов. В качестве стартовой точки отсчета для оценки можно назвать бюджет 5 миллионов рублей», – утверждает **Евгения Наумова**, руководитель отдела корпоративных продаж «Лаборатории Касперского».

«В данном случае регулятор подошел к проблематике достаточно взвешенно, так что, если вы успели отстроить собственный SOC, то потребуются только косметические изменения, – полагает **Михаил Савельев**. – А вот если в вашей компании только запланировали его построить, то это достаточно затратная процедура. Учитывать необходимо как стоимость инструментария для построения SOC, так и стоимость содержания обязательного персонала». По его словам, затраты на такую систему составляют десятки миллионов рублей в год.

Подробнее: http://clc.am/yI_tLg