SOC-Форум: кибербезопасность — продукт взаимодействия

22 ноября 2017 года в Москве при поддержке ФСБ России, ФСТЭК России и Банка России с размахом прошел SOC-Форум 2017 «Практика противодействия кибератакам и построения центров мониторинга ИБ». С самого начала проведения Форума в 2015 году количество участников, — а на этот раз их было свыше 1 700 — подтверждает, что затронутые на Форуме темы не просто актуальны, они требуют оперативного и конкретного решения.

В этом году обсуждались вопросы построения и эксплуатации SOCов, а также примеры обнаружения, предотвращения и анализа киберинцидентов. Особое внимание было уделено вопросам государственного регулирования.

SOC-Форум открыла пленарная дискуссия, модераторами которой выступили генеральный директор Solar Security Игорь Ляпунов и главный редактор сообщества BISA Олег Седов. Участниками обсуждения стали заместитель начальника 8 Центра ФСБ России Игорь Качалин, заместитель директора ФСТЭК России Виталий Лютиков, заместитель начальника ГУБиЗИ Банка России Артем Сычев, руководитель службы кибербезопасности Сбербанка Сергей Лебедь и заместитель генерального директора компании «Информзащита» Максим Темнов.

Выступая с приветственным словом, Игорь Ляпунов напомнил, что в России в этом году произошел ряд резонансных событий в сфере информационной безопасности. «Этот год стал принципиальным и поворотным, поскольку тема кибератак и киберугроз вышла на первый план и видна уже на уровне первых лиц государства. Драматически возросло напряжение на внешнем поле, где данная тема становится инструментом политического давления. Кроме того, в этом году по всему миру прокатилась волна массовых киберэпидемий *(WannaCry, Petya), которые затронули как частный бизнес, так и крупные корпорации. И, как мне кажется, Россия здесь неплохо выстояла»,* — отметил генеральный директор Solar Security.

Развивая начатую тему, заместитель начальника 8 Центра ФСБ России Игорь Качалин рассказал о тех изменениях, которые принёс принятый в июле 2017 года Федеральный закон N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Представитель ФСБ выразил надежду, что

«законы, которые будут приняты в ближайшее время, *поспособствуют тому, что безопасность станет более динамичным процессом».*

Заместитель начальника ГУБиЗИ Банка России Артем Сычев отметил, что отечественным кредитно-финансовым организациям удалось отразить массовые атаки вирусов-шифровальщиков. Однако трудности с обеспечением информационной безопасности в действительности сохраняются, и в этой ситуации SOCи являются реальным инструментом, способным помочь в борьбе с киберинцидентами.

Руководитель кибербезопасности Сбербанка Сергей Лебедь заявил, что работа современных SOC еще находится в процессе становления: «На сегодняшний день приходит только понимание того, что мы закладываем в *SOC*. Ещё не существует открытых процессов, подобных *ITSM, ITIL* в области ИБ и операционного управления безопасностью, поскольку мы пока не готовы. *П*ока мы пытаемся понять, *как управлять этим, что такое операционная безопасность, что такое управление на стратегическом уровне.* Современный *SOC, с точки зрения технологий, это набор информационных систем* (*SIEM, Threat Intelligence*-платформы), системы мониторинга и средства защиты. Однако пока они не связаны между собой, и главный вопрос состоит в том, как объединить все эти компоненты».

Свой подход к строительству коммерческого центра мониторинга описал заместитель директора компании «Информзащита» Максим Темнов. Он обратил внимание на необходимость развивать проактивный SOC, который обеспечит анализ потенциальных угроз, в том числе поступающих из анонимных сетей (вроде Tor, DarkNet) и других источников.

Заместитель директора ФСТЭК России Виталий Лютиков в ходе дискуссии затронул тему, которая оказывает прямое влияние на рынок ИБ-аутсорсинга, — введённое в начале текущего года лицензировании деятельности SOC. Он отметил, что ведомство в последнее время наблюдает рост количества коммерческих центров мониторинга, вследствие чего возникает необходимость законодательного регулирования данной сферы. «При подготовке лицензионных требований и условий мы максимально учли пожелания организаций, строящих подобные структуры», — подчеркнул Виталий Лютиков. Одним из следствий такого подхода стало то, что на данном этапе было решено не вводить лицензирование и аккредитацию ведомственных или корпоративных центров Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Как и ожидалось, построение и функционирование ГосСОПКА стало одной из главных тем SOC-Форума. Представитель ГУБиЗИ Банка России Артем Сычев рассказал, что взаимодействие Центробанка и ГосСОПКА позволяет «отследить первый выход злоумышленника и предупредить другие структуры». Благодаря этому достига-

ется высокая скорость реагирования на угрозы. Артем Сычев сообщил, что «в Центре мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) скорость обработки каждой угрозы в среднем составляет от 40 до 90 минут».

По словам Сергея Лебедя, специалисты Сбербанка «стали видеть все атаки в реальном времени, своевременно принимать решения. В качестве показателя эффективности могу сказать, что от компьютерных атак простои банка в этом году были ноль минут, то есть мы ни на секунду не прерывали деятельность банка вследствие различных атак... мы видели попытки атак на какие-то элементы нашей инфраструктуры, но не центральной». Однако препятствиями для укрепления информационной безопасности остаются нехватка информационного обмена с другими организациями и отсутствие единой структуры, которая взяла бы на себя руководящую роль при возникновении массированных кибератак. В ответ заместитель начальника ГУБиЗИ Банка России Артем Сычев предложил возложить эти функции на ГосСОПКА.

Говоря об обязательствах сторон по обеспечению безопасности конкретного объекта, участники напомнили о возможных санкциях вплоть до уголовной ответственности. Что касается ответственности регулятора, то, как подчеркнул Артем Сычев, она должна наступать только в том случае, если регулятор не предусмотрел одну из перспективных киберугроз.

Участники форума обсудили нынешнее состояние и перспективы международного информационного обмена. Заместитель начальника ГУБиЗИ Банка России Артем Сычев указал на существующие проблемы в данной сфере: «Уважаемые западные партнеры нас в информационном обмене не ждут, это тоже надо понимать. Причем они делают все, чтобы этот информационный обмен с нами был крайне скупой. Я не говорю за все отрасли, но могу сказать на примере финансовой: инициатива, которая есть со стороны РФ по формированию такого обмена, наталкивается на глухую стену непонимания. С другой стороны, мы имеем уже практически обязанность формирования единого информационного пространства, с точки зрения информационной безопасности в финансовой сфере, между государствами-членами Евразийского экономического сообщества, и эту работу мы будем делать. В рамках этой работы такой информационный обмен возможен, и от него тоже можно будет получить достаточно хороший результат».

Замначальника Центра ФСБ Игорь Качалин, в свою очередь, подытожил: «Сейчас все сосредоточены на строительстве крепостей для себя. Нужно объединяться для предотвращения атак. Сейчас мы на начальном этапе. Необходимо делиться своими проблемами, но не со всеми. В рамках федерального органа, отвечающего за создание и функционирование ГосСОПКА, *создается национальный координационный*

центр по компьютерным инцидентам, одна из функций которого — организация и регулирование вопросов обмена информации с иностранными партнерами. Это то окно, через которое мы можем выходить в мир», — заключил представитель ФСБ России.

Во время пресс-брифинга регуляторы и эксперты рассказали журналистам об последствиях использования социальной инженерии мошенниками, профильных программах в вузах по подготовке ИБ-специалистов, о факторах, влияющих на эффективность SOC.

В ходе тематических дискуссий компании-создатели центров мониторинга, ответственные за реализацию ГосСОПКА ведомства и разработчики методических рекомендаций рассказали о стоящих перед ними задачах, поделились опытом их решения и рассказали о дальнейших перспективах работы.

Дополнительный интерес участников Форума вызвали проходившие на протяжении всей встречи соревнования «SOC-Форум CTF». Постоянным вниманием представителей регуляторов, заказчиков и крупных игроков российского рынка решений и сервисов в области ИБ пользовалась демонстрационная зона. На стендах ведущих российских и мировых компаний демонстрировались решения по противодействию кибератакам, построению и эксплуатации центров мониторинга ИБ. Впервые были представлены стенды ФинЦЕРТ Банка России, ГосСОПКА ФСБ России и Базы данных угроз безопасности информации ФСТЭК России.

Как отметили организаторы, в этом году Форум в очередной раз побил все рекорды по количеству участников и значимости затронутых тем. За три года SOC-Forum успел стать тем местом, где собираются люди, формирующие будущее информационной безопасности в России.

Security Operations Center (SOC) представляет собой государственный или частный центр мониторинга информационной безопасности. SOC активно создаются сегодня во всем мире, в том числе в России. Главная задача SOC состоит в обнаружении угрозы компьютерных атак, высокотехнологичного мошенничества, кибершпионажа и утечек ценной информации, предотвращении и устранении их последствий.

Впервые SOC-Форум прошел в ноябре 2015 года в Москве. Более 500 ИБ-специалистов, работающих в российских банках, ИТ-компаниях, телеком-операторах, коммерческих предприятиях, государственных структурах обсудили вопросы укрепления сотрудничества между государственными и коммерческими SOC; проанализировали опыт внедрения центров мониторинга в ведущие российские компании; выделили наиболее перспективные технологии в киберсфере.

Сегодня SOC-Форум — единственная в России конференция, полностью посвящённая вопросам создания и эксплуатации центров мониторинга и реагирования на инциденты информационной безопасности. Организатором мероприятия третий год подряд выступает Медиа Группа «Авангард» и Закрытый клуб «SOC в России».