Аналитическое чтение тезисов с лекции 2 (от 16 фев 2015)

Мартынов Семён

9 марта 2015 г.

Селеста Лин Пол, известный эксперт в области дизайна и юзабилити, а также член совета KDE e.V. в своём отчёте по человекоориентированному изучению Сетевых Операционных центров (СОЦ) публикует те методики и приёмы, которые, по её мнению, могут помочь будущим исследователям этой области.

Она начинает с того, что перечисляет те сложности, с которыми сталкивается человек, исследующий сетевую безопасность с точки зрения работы людей, и главным из них является сложность сбора информации, т.к. специалисты, занимающиеся сетевой аналитикой, постоянно перегружены задачами и у них нет времени отвлекаться от своей работы. Тем не менее, растет общее понимание, что в компьютерной безопасности человеческий фактор превалирует над технологией, так что подобные исследования необходимы.

Своё исследование она проводила в крупном правительственном Сетевом Центре, занимавшемся обеспечением защиты крупной правительственной сети. Работа в центре строилось по принципу 24/7 и делилась на две смены (дневную и ночную). Доступ в подобные организации строго ограничен, и для проведения исследования требовалось приглашение кого-либо из Центра или партнерской организации.

В виду особенностей изучаемой среды, автору требовались гибкие методы работы с минимальным влиянием на саму среду. Интервью, полевые исследования и распределение карточек длилось более 12 месяцев.

Первые **интервью** были проведены с целью понимания работы Сетевого Операционного центра ещё до визита на объект. Базовую информацию (границы ответственности, используемые средства, общая организация) могла быть получена от человека, имевшего достаточный опыт работы в центре. Эти темы хорошо подходят для первой встречи с новым человеком, хотя и не являются самым эффективным способом потратить время интервьюируемого специалиста.

Семь интервью были проведены в людьми, имевшими опыт работы в СОЦ. Интервью содержали открытые вопросы чтобы не ограничивать экспертов. Продолжительность каждого интервью была от 45 минут до полутора часов. Последние три интервью были с людьми, которые на тот момент работали в центре в должности начальника смены. Это те люди, кто выполнял операционные задачи и принимал решения в течение смены. Среди трёх интервьюируемых нашёлся человек заинтересовавшийся исследованием, и

обеспечивший автору доступ на объект. Проведённые интервью позволили составить понимание целей и методов работы операционных центров а так же получить базовые знания до погружения в эту среду.

Примерно 30 часов были посвящены **наблюдению**. Оно проводилось один раз в месяц по 2 – 4 часа. Как правило, наблюдение проводилось в ночное время, т.к. дневные смены очень заняты другими посетителями и встречами. Ночные смены тише, и иногда предоставляют возможность общения с аналитиком при минимальном влиянии на работу.

Наблюдение включало следующие активности:

- Ежедневные операции, включая совместную работу и коммуникации между аналитиками и менеджерами
- Плановые встреча, летучки и технические демонстрации
- Тренировочные упражнения, изображающие различные события

Распределение карточек является методом, позволяющим человеку выстроить связи между объектами, и построить ментальную модель обсуждаемой области. Автор задавала вопрос и просила аналитиков и менеджеров разбить карточки на группы по применяемым для решения этого вопроса методам. Когда участник заканчивал, он описывал каждую группу и объяснял свой выбор.

Аналитики и менеджеры получали удовольствие от участия в этом эксперименте. После недели работы, они ощутили себя частью исследования. Некоторые участники отметили, что задача с карточками подтолкнула их к общим размышлениям о той области, к которой они были хорошо знакомы.

Результаты работы с карточками легли в основу другого исследования по анализу работы процессов и позволили выявить, что аналитики и менеджеры считают наиболее важным в своей работе.

В итоге, автор заключает, что Сетевые Операционные центры являются средой с высокой степенью взаимодействия сотрудников. Хотя каждый аналитик имеет свою зону ответственности, общая работа строится на командном принципе. Наиболее применяемым методом распространения информации является вербальное общение. Обычной ситуацией является когда аналитик подходит к столу другого аналитика, или несколько человек собираются вместе для обсуждения какого-либо вопроса, даже если каждый из них видит на своём мониторе одну и туже картинку. Наиболее важная информация может распространяться по внутренней телефонной связи. Менее приоритетная информация фиксировалась в виде каких либо артефактов, которые можно было передать следующей смене.

Подобная система создаёт трудности для обмена данными между сменами. Использование тикетов и отчётов о событиях не позволяет передать контекст ситуации. Наиболее эффективно подобные данные хранятся в "капитанском журнале который ведёт начальник смены. Но реальная возможность ведения таких записей сильно связана с тем, на сколько напряженная выдалась смена.