# Аналитическое чтение тезисов с пленарных заседаний ACM CCS'13-14

Александр Сухинин

2 июня 2015 г.

**The Science, Engineering and Business of Cyber Security**

Данный фрагмент состоит из двух частей: введения и краткой биографии автора. Во введении автор благодарит за оказанную возможность составить данный обзор и возможность выразить свою точку зрения. Далее, в статье говорится о двойственном положении компьютерных наук по сравнению с точными и о том, что данные технологии находятся на стыке трех областей: инженерии, бизнеса и точных наук. При этом, задача обеспечения безопасности компьютерных систем вносит ряд особенностей в данную область.

Автор считает, что текущий потребительский рынок приведет общество к относительно низкому уровню гарантии безопасности. Это связано с тем, что средний пользователь всегда предпочитает большее удобство использования, оттесняя риски безопасности на второй план. При этом, сохраняется необходимость повышения безопасности таких систем, пусть и по неестественным причинам. При этом, отмечается, что проблема вторжения со стороны крупного бизнеса или правительств может оказаться гораздо большей проблемой, чем преступления.

В статье также говориться о беспокойстве множества людей касательно угрозы кибер-терроризма или кибер-войны. Департамент защиты США считает киберпространство местом, которое также будет сопровождаться войнами.

Биография:

Ravi Sandhu является исполнительным директором кибербезопасности Техасского университета в San Antonio. Обладает степенями BTech и ATech. Участник IEEE, ACM и AAAS, обладатель наград IEEE, ACM, NSA и NIST. Автор более 235 статей, которые набрали более 6 тысяч цитирований. Считается лучшим специалистом по защите информации не связанным с криптографией. Со- основатель TriCipher. Изобретатель 29 запатентованных технологий защиты информации.

**The Science, Engineering and Business of Cyber Security**

Успех интернет технологий превзошел все возможные ожидания. На сегодняшний день веб-технологии затрагивают все аспекты нашей жизни, от общества до экономики. С другой стороны, также возрастает зависимость общества от таких технологий. Даже короткое отсутствие доступа в интернет может оказать негативное влияние на государство, экономику и социальные операции. Ухудшает положение также и то, что изначально

интернет не разрабатывался для высокой доступности и защиты. Многие недавние улучшения, предложенные для совершенствования защиты были отклонены из-за текущей архитектуры. Другой актуальной проблемой является необходимость авторизации на разных уровнях, от маршутизации и DNS до доменов для TLS. Текущая модель PKI не масштабируется, так как рядовые пользователи не способны оценить уровень доверия к CA в их браузерах. Эти проблемы важны для разработки интерната нового поколения, который бы обеспечивал защиту, доступность и приватность изначально. Для того, чтобы исключить все указанные ограничения архитектуры; изучить и построить сети нового поколения.

Биография автора: Adrian Perrig - профессор компьютерных наук в Швейцарском федеральном институте технологий. Получил докторскую степень в университете Беркли. Обладатель награды NSF CAREER и ACM SIGSAC. Работник IBM и Sloan research.

**The Cyber Arms Race**

Изначально интернет появился как общее глобальное свободное пространство. Однако в последствии политики осознали пользу этих технологий, особенно для наблюдения за гражданами. Эта проблема получила широкую огласку после утечек информации из PRISM благодаря Сноудену. При этом, PRISM - это не система наблюдения за подозрительными лицами, а система наблюдения за всеми. Данная предназначена для создания досье на каждого. Такие досье строятся на основе активности пользователя в сети.

При этом, спецслужбы США имеют полное законное право для слежения за приезжими. И это не звучит не слишком страшно, до тех пор, пока не осознаешь, что до 96% населения попадает под эту категорию.

После утечек информации, правительство США попыталось оправдаться говоря, что данная система предназначена для борьбы с терроризмом. Однако дальнейшие утечки касательно слежения за европейским комитетом и Великобритании, что несколько не укладывается в их объяснения.

Другим объяснением, которое можно было услышать от спецслужб США - это то, что подобную слежку ведут все. Однако в этом вопросе США имеет неоспоримое преимущество, так как большинство технологий и сервисов произведено именно в США.

К сожалению, на практике оказывается слишком сложным отказ от таких сервисов как Google, Facebook, Dropbox, Amazon, Windows, Skype и т.п. Таким образом встает вопрос, если ты не делаешь ничего запретного должен ли ты беспокоиться об этом? Ответ автора состоит в том, что ему нечего скрывать, но и, в частности, нет никакого желания делиться информацией со спецслужбами. И если есть необходимость в наличии "большого брата то автор предпочитает в этом случае своего, а не иностранного. И когда люди спрашивают его, должны ли они беспокоиться по поводу PRISM, автор говорит, что нужно быть в ярости. Нельзя просто принимать такое повсеместное наблюдение.

Прогресс в компьютерных технологиях сделал возможным наблюдение и сбор информации. Однако также из-за этого появилась и возможность утечки информации.