# Лекция № 9. Аннотированный перевод статьи

## Cybersecurity, tech infrastructure requires international trust

### SUMMARY

Researchers use the field of incident response to shed light on how experts — and nations — can more effectively combat cyber-warfare when they foster trust and transcend politics.

### FULL STORY

In new research published in the journal Technology and Culture, Rebecca Slayton, professor of science and technology studies at Cornell University, uses the field of incident response to shed light on how experts — and nations — can more effectively combat cyberwarfare when they foster trust and transcend politics.

"People often think of infrastructure as a set of technologies just sitting there, but in fact they're living technologies — socio-technical systems that are constantly being maintained by people, and trust is central to that," Slayton said.

Most experts agree that state-sponsored hackers in Russia are trying to use the internet to infiltrate the U.S. electrical grid and sabotage elections, yet internet security teams in the U.S. and Europe actively seek to cooperate with their Russian counterparts, focusing on the issues where they can establish mutual trust.

"Even though they recognize that there are actors in the shadows in those countries whom they don't trust, they have a shared goal of keeping the infrastructure running," Slayton said.

The field of incident response began after the internet was struck by "an attack from within" in November 1988. A self-replicating program — a "worm" — infected thousands of connected computers, causing them to stop processing and communicating normally.

Although computer scientists realized that the connected nature of the internet required international cooperation, global participation in these efforts was initially limited. But that began to change in the early 1990s, with the formation of the Forum of Incident Response and Security Teams (FIRST), which remains the leading global organization of security experts.

"Teams in the U.S. and in Europe very much want to cooperate with teams in Russia, and they see that as a way of having influence they might otherwise not have in that space," Slayton said.

Previous research on the history of computer and network security focused largely on development of new technology, rather than repair or maintenance. However, Slayton wrote in the new paper "Trusting Infrastructure: The Emergence of Computer Security and Incident Response, 1989-2005," that without the efforts of incident responders, the internet as we know it wouldn't exist.

"It's one thing to come up with a new algorithm or a new technique for, say, intrusion detection, but actually making it work and operate requires people to implement and maintain it on an ongoing basis," Slayton said. "It's nice to think some innovative technology will fix everything. But in practice, people have to keep things up to date, particularly when you're dealing with an intelligent adversary. You have to stay ahead of that."

The research was supported by the National Science Foundation.

*Source:* [*https://www.sciencedaily.com/releases/2020/04/200413132754.htm*](https://www.sciencedaily.com/releases/2020/04/200413132754.htm)

## List of unknown words

|  |  |
| --- | --- |
| Word | Translation |
| The field of incident response | Сфера деятельности по реагированию на инциденты |
| Shed | Пролить |
| Foster | Способствовать |
| Transcend | Превосходить |
| Infiltrate | Проникать |
| Mutual | Взаимное |
| Struck | Поражён |
| Otherwise | Иначе |
| Adversary | Противник |

## Annotation in Russian

Люди часто думают об инфраструктуре как о наборе технологий. Но на самом деле это живые технологии — социально-технические системы, которые постоянно поддерживаются людьми, и доверие является центральным элементом этого. Большинство экспертов сходятся во мнении, что спонсируемые государством хакеры в России пытаются использовать интернет для проникновения в американскую электросеть и саботажа выборов. Однако команды по интернет-безопасности в США и Европе активно стремятся к сотрудничеству со своими российскими коллегами, сосредотачиваясь на вопросах, где они могут установить взаимное доверие, ведь им нужно поддерживать инфраструктуру в рабочем состоянии. Сфера деятельности по реагированию на инциденты началась после того, как в ноябре 1988 года в интернете была совершена «атака изнутри», из-за которой тысячи компьютеров прекратили обработку данных и нормальное общение. В начале 1990-х годов был образован Forum of Incident Response and Security Teams (FIRST), который остается ведущей глобальной организацией экспертов по безопасности. Предыдущие исследования истории компьютерной и сетевой безопасности были в основном сосредоточены на разработке новых технологий, а не на ремонте или обслуживании. Слейтон говорит, что без усилий специалистов по реагированию на инциденты интернет, как мы его знаем, не существовал бы. «Одно дело придумать новый алгоритм или новую технику, скажем, для обнаружения вторжений. Но на самом деле, чтобы заставить её работать и эксплуатироваться, требуется, чтобы люди внедряли и поддерживали её на постоянной основе.» — говорит Слейтон.