|  |  |
| --- | --- |
|  | **Международный союз электросвязи****Бюро стандартизации электросвязи** |

 Женева, 30 октября 2020 года

|  |  |  |
| --- | --- | --- |
| Осн.: | **Циркуляр 278 БСЭ** | **Кому**:– Администрациям Государств – Членов Союза– Членам Сектора МСЭ-Т– Ассоциированным членам МСЭ-Т– Академическим организациям − Членам МСЭ**Копии**:– Председателям и заместителям председателей исследовательских комиссий – Директору Бюро развития электросвязи– Директору Бюро радиосвязи– Директорам региональных отделений МСЭ |
| Для контактов:Тел.:Факс:Эл. почта: | г-н Виджей Мори (Mr Vijay Mauree)+41 22 730 5591+41 22 730 5853tsbevents@itu.int |
|  |  |

|  |  |
| --- | --- |
| **Предмет**: | **Серия вебинаров по теме** "**Роль цифровых финансовых услуг в условиях распространения вируса COVID-19**"**(12-й выпуск: полностью виртуальное собрание, 10 ноября 2020 г.)** |

Уважаемая госпожа,
уважаемый господин,

1 Международный союз электросвязи (МСЭ) организует 12-й выпуск серии вебинаров по теме [Роль цифровых финансовых услуг (ЦФУ) в период распространения вируса COVID-19](https://www.itu.int/en/ITU-T/webinars/Pages/dfs.aspx), который пройдет **10 ноября 2020 года с 15 час. 00 мин. до 16 час. 30 мин. CEST**. В рамках этого эпизода будет обсуждаться тема **уменьшения уязвимости инфраструктуры цифровых финансов**.

2 В этом выпуске основное внимание будет уделено уязвимостям базовой инфраструктуры электросвязи, такой как сети SS7, а также SIM-карты, и их потенциальной угрозе для цифровых финансовых услуг, а также передовому опыту в области их уменьшения. Сфера цифровых финансов в значительной степени зависит от инфраструктуры и услуг электросвязи. В связи с преобладанием обычных мобильных телефонов среди пользователей в развивающихся странах, которые составляют большинство конечных пользователей цифровых финансовых услуг, каналами связи конечного пользователя с поставщиком цифровых финансовых услуг являются, главным образом, неструктурированные данные дополнительных услуг (USSD), услуга передачи службы коротких сообщений (SMS) и комплект поддержки SIM-карты (STK). Давно известно, что USSD и SMS как средства связи подвержены атакам и имеют множество опубликованных уязвимостей. SIM-карта телефона является еще одной уязвимостью в области безопасности, которая также требует особого внимания. Например, SIM-карты, подверженные уязвимости Simjacker, могут быть уязвимы для атаки, которая содержит серию инструкций комплекта поддержки SIM-карты (STK), специально разработанных для передачи на SIM-карту внутри устройства. Использование этих уязвимостей позволяет злоумышленникам совершать мошеннические действия и похищать средства у ничего не подозревающих жертв, которые в большинстве случаев не знают о том, что их учетная запись скомпрометирована или взломана.

3 Принять участие в этих вебинарах могут Государства – Члены МСЭ, Члены Секторов МСЭ, Ассоциированные члены МСЭ и Академические организации – Члены МСЭ, а также любое лицо из страны, являющейся Членом МСЭ, которое пожелает внести свой вклад в работу этих вебинаров. К таким лицам относятся также члены международных, региональных и национальных организаций.

4 Вся необходимая информация, касающаяся вебинаров (докладчики, ссылки для регистрации, подробная информация о порядке дистанционной связи), будет размещена по адресу: <https://www.itu.int/en/ITU-T/webinars/20201110/Pages/default.aspx>. Данные веб-сайт будет регулярно обновляться по мере появления новой или измененной информации. Участникам предлагается периодически знакомиться с обновленной информацией на веб-страницах выпусков. Ознакомиться с предыдущими выпусками можно на основной странице [здесь](https://www.itu.int/en/ITU-T/webinars/Pages/dfs.aspx).

С уважением,

Чхе Суб Ли
Директор Бюро
стандартизации электросвязи