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

 Женева, 3 мая 2022 года

|  |  |  |
| --- | --- | --- |
| Осн.: | **Циркуляр 13 БСЭ**TSB Events/VM | **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: | **Практикум по безопасности цифровых финансовых услуг (ЦФУ) – Реагирование на риски безопасности экосистемы цифровых финансов****(полностью виртуальное собрание, 24–25 мая 2022 г.)** |

Уважаемая госпожа,
уважаемый господин,

1 Хотел бы сообщить вам, что 24–25 мая 2022 года Международный союз электросвязи (МСЭ) совместно с Ассоциацией регуляторных органов в области связи стран юга Африки (CRASA) проводит практикум по безопасности цифровых финансовых услуг (ЦФУ) по теме "**Реагирование на риски безопасности экосистемы цифровых финансов**".

2 Основная задача практикума по безопасности ЦФУ состоит в представлении заключений и рекомендаций [Рабочей группы FIGI по безопасности, инфраструктуре и доверию](https://www.itu.int/en/ITU-T/extcoop/figisymposium/Pages/FIGISITWG.aspx) для регуляторных органов и поставщиков ЦФУ в отношении решения проблем безопасности цифровых финансов. В ходе работы мероприятия будут рассмотрены примеры передового опыта в области безопасности, связанные с подменой SIM-карты, приложения мобильных платежей, использующие USSD, STK и Android, методы тестирования безопасности приложений мобильных платежей и реагирование на уязвимости инфраструктуры, например уязвимости SS7. Проект программы работы практикума по безопасностипредставлен в Приложении 1.

3 В рамках программы Глобальной инициативы по охвату финансовыми услугами (FIGI) МСЭ в ноябре 2020 года создал лабораторию безопасности ЦФУ для совместной работы с регуляторными органами в сфере ЦФУ с целью принятия общей методики по управлению рисками безопасности и проведения аудитов безопасности приложений ЦФУ. Перед лабораторией безопасности ЦФУ МСЭ стоят следующие задачи:

a) поддерживать регуляторные органы в выполнении рекомендаций FIGI по безопасности ЦФУ (<https://figi.itu.int/working-group-reports/>);

b) проводить аудиты безопасности приложений ЦФУ (т. е. приложений ЦФУ на базе USSD, STK и Android);

с) обеспечивать руководящие указания по управлению рисками безопасности в экосистеме ЦФУ и мерам по смягчению их последствий;

d) проводить практикумы по безопасности, адресованные регуляторным органам и поставщикам в сфере ЦФУ, для понимания новых уязвимостей и мер по ослаблению их влияния;

e) оценивать уровни киберподготовленности заинтересованных сторон экосистемы ЦФУ к реагированию на инциденты в сфере кибербезопасности, касающиеся цифровых финансов;

f) обеспечивать нейтральную платформу для обмена знаниями по инцидентам и уязвимостям безопасности и в области цифровых финансов.

4 Практикум по безопасности ориентирован на специалистов по ИТ-безопасности и разработчиков политики в отрасли электросвязи, регуляторные органы в области ИКТ, поставщиков ЦФУ, центральные банки и операторов сетей подвижной связи.

5 Вся соответствующая информация, касающаяся мероприятия (докладчики, ссылка для регистрации, подробная информация о порядке дистанционной связи), будет размещена на главной странице мероприятия по адресу: <https://www.itu.int/en/ITU-T/webinars/dfs/sc/20220524/Pages/default.aspx>.

Просьба обратить внимание, что регистрация обязательна.

С уважением,

Чхе Суб Ли
Директор Бюро
стандартизации электросвязи

Приложение 1

Проект программы Практикума по безопасности ЦФУ

|  |
| --- |
| **День 1: 24 мая 2022 года 10 час. 00 мин. – 13 час. 00 мин. (UTC+2)** |
| 10 час 00 мин. – 10 час. 20 мин. | **Вступительные замечания*** **МСЭ**
* **CRASA**
 |
| 10 час 20 мин. – 11 час. 50 мин. | **Уязвимости безопасности ЦФУ: уязвимости платформ USSD, STK и Android**На этой сессии будет представлена лаборатория безопасности ЦФУ МСЭ и освещены уязвимости приложений на базе USSD и STK, а также Android. Будут обсуждаться такие угрозы, как атаки через посредника, которые воздействуют на цифровые финансовые услуги, и уязвимость SIMjacker в SIM-картах. В рамках сессии также будет представлен обзор тестов безопасности, которые проводятся в лаборатории безопасности ЦФУ в МСЭ:• "Знакомство с лабораторией безопасности ЦФУ МСЭ" – **Виджей Мори**, координатор программ, БСЭ МСЭ;• "Тесты Android, USSD и STK" – **Арнольд Кибуука**, сотрудник по проекту, БСЭ МСЭ.**Соответствующие отчеты:**• [Тестирование безопасности приложений ЦФУ, работающих на основе USSD и STK](https://figi.itu.int/wp-content/uploads/2021/04/Security-testing-for-USSD-and-STK-based-Digital-Financial-Services-applications-1.pdf);• [Аудиты безопасности различных приложений ЦФУ](https://figi.itu.int/wp-content/uploads/2021/05/Security-audit-of-various-DFS-applications.pdf) |
| 11 час 50 мин. – 12 час. 00 мин. | **Перерыв на кофе** |
| 12 час 00 мин. – 13 час. 00 мин. | **Уязвимости безопасности ЦФУ: уязвимости SIM-карт и инфраструктуры, меры смягчения их влияния**Уязвимости инфраструктуры электросвязи, например системы SS7, используются злоумышленниками для перехвата вызовов и SMS, обхода биллинга, хищения денежных средств со счетов мобильных денег или воздействия на работу сетей подвижной связи. Эта сессия будет посвящена краткому обзору ключевых рекомендаций МСЭ по ЦФУ, касающихся безопасности ЦФУ, в частности по вопросам SS7, подмены SIM-карт, повторного использования SIM-карт и уязвимостей SIM-карт, таких как SIMjacker, которые могут поставить под угрозу работу ЦФУ.**Соответствующие отчеты:** • [Уязвимости SS7 и меры смягчения их влияния](https://figi.itu.int/wp-content/uploads/2021/04/Technical-report-on-the-SS7-vulnerabilities-and-their-impact-on-DFS-transactions_f-1-1.pdf) на транзакции ЦФУ |
| **День 2: 25 мая 2022 года**  |
| 10 час 00 мин. – 11 час. 15 мин. | **Система обеспечения безопасности ЦФУ**На сессии будет обсуждаться система обеспечения безопасности ЦФУ, которая может быть внедрена поставщиками ЦФУ для более эффективного управления рисками и смягчения их воздействия.• **Виджей Мори**, координатор программ, БСЭ МСЭ**Соответствующий отчет:**• [Система обеспечения безопасности ЦФУ](https://figi.itu.int/wp-content/uploads/2021/04/Technical-report-on-Digital-Financial-Services-Security-Assurance-Framework_f-1-1.pdf) |
| 11 час 15 мин. – 11 час. 25 мин. | **Перерыв на кофе** |
| 11 час 25 мин. – 12 час. 00 мин. | **Руководство по аудиту безопасности ЦФУ**На сессии также будет освещаться вопрос о том, как именно регуляторный орган или поставщик ЦФУ могут оценить соответствие минимальным средствам контроля безопасности, используя руководство по аудиту ЦФУ.• **Арнольд Кибуука**, сотрудник по проекту, БСЭ МСЭ**Соответствующий отчет:**• [Руководство по аудиту безопасности ЦФУ](https://figi.itu.int/wp-content/uploads/2021/05/Digital-Financial-Services-security-audit-guideline.pdf) |
| 12 час 00 мин. – 13 час. 00 мин. | **Выполнение рекомендаций по безопасности ЦФУ и проведение аудитов безопасности ЦФУ**Интерактивная сессия, призванная инициировать процесс выполнения рекомендаций по безопасности ЦФУ и определение приложений мобильных денег ЦФУ, которые могут быть протестированы в лаборатории безопасности ЦФУ МСЭ |