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

 Женева, 25 февраля 2022 года

|  |  |  |
| --- | --- | --- |
| Осн.: | **Циркуляр 382 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, 30–31 марта 2022 г.)** |

Уважаемая госпожа,
уважаемый господин,

1 Хотел бы сообщить вам, что 30–31 марта 2022 года Международный союз электросвязи (МСЭ) совместно с Восточноафриканской организацией связи (EACO) проводит практикум по безопасности цифровых финансовых услуг по теме "**Реагирование на риски безопасности экосистемы цифровых финансов**".

2 Основной задачей практикума по безопасности ЦФУ является освещение 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 ЦФУ ориентирован на специалистов в области ИТ-безопасности, руководителей регуляторных органов в сфере электросвязи/ИКТ, поставщиков ЦФУ, представителей центральных банков 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 здесь: [https://www.itu.int/en/ITU-T/webinars/dfs/sc/20220330/Pages/
default.aspx](https://www.itu.int/en/ITU-T/webinars/dfs/sc/20220330/Pages/default.aspx).

Просьба иметь в виду, что регистрация обязательна.

С уважением,

Чхе Суб Ли
Директор Бюро
стандартизации электросвязи

Приложение 1

Проект программы работы Практикума по безопасности ЦФУ – Реагирование на риски безопасности экосистемы цифровых финансов

|  |
| --- |
| **День 1: 30 марта 2022 года 10 час. 00 мин. – 13 час. 00 мин. (восточноафриканское время)** |
| 10 час 00 мин. – 10 час. 20 мин. | **Начало работы и вступительные замечания*** **Билель Джамусси**, руководитель департамента исследовательских комиссий, БСЭ МСЭ
* **Алли Яхайя Симба**, Исполнительный секретарь EACO
 |
| 10 час 20 мин. – 11 час. 50 мин. | **Уязвимости безопасности ЦФУ: Уязвимости инфраструктуры и меры по их смягчению (Уязвимости инфраструктуры подвижной связи)**Уязвимости инфраструктуры электросвязи, например уязвимости SS7, могут быть использованы злоумышленником для перехвата вызовов и SMS, обхода выставления счетов, похищения средств с мобильных счетов или влияния на работу сети подвижной связи. На этой сессии будут представлены основные заключения Рабочей группы по безопасности, инфраструктуре и доверию по защите инфраструктуры от уязвимостей и угроз, связанных с SS7.**Выступающие*** "Безопасность сигнализации" - **Фааез Бурни** и **Карел Ван Дер Лек**, Adaptive Mobile
* "Безопасность SS7: Что должны сделать регуляторные органы?" - **Ассаф Клингер**, Klinger Consulting

Соответствующий отчет:* [Уязвимости SS7 и меры смягчения их влияния на транзакции цифровых финансовых услуг](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)
 |
| 11 час 50 мин. – 12 час. 00 мин. | **Перерыв на кофе** |
| 12 час 00 мин. – 13 час. 00 мин. | **Уязвимости безопасности ЦФУ: Уязвимости USSD, STK и платформы Android**На этой сессии будет представлена лаборатория безопасности ЦФУ МСЭ и освещены уязвимости USSD и STK, а также приложений на базе Android. Будут рассмотрены такие угрозы, как атаки через посредника, которые могут повлиять на цифровые финансовые услуги, и будет обсуждаться уязвимость SIMjacker в SIM-картах. В рамках сессии также будет представлен обзор тестов безопасности, которые можно провести в лаборатории безопасности ЦФУ в МСЭ.**Выступающие*** "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)
 |
| **День 2: 31 марта 2022 года 10 час. 00 мин. – 13 час. 00 мин. (восточноафриканское время)** |
| 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 лучшего 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, 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 |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_