ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000039 5
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«01» июля 2021г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за июнь 2021 г.»

В связи с необходимостью снижения рисков воздействия вредоносного кода, рисков использования уязвимостей программного обеспечения и повышения уровня защиты информации при работе с системой дистанционного банковского обслуживания «iBank2» (Интернет-банком) служба информационной безопасности РНКО «ПРОМСВЯЗЬИНВЕСТ» (ООО) рекомендует it-специалистам наших клиентов (организаций и индивидуальных предпринимателей) применять в своей работе рекомендации по защите информации, указанные в Приложении 1 к данному письму. В случае возникновения вопросов по применению рекомендаций просим Вас позвонить в службу информационной безопасности по номерам 8 (8722) 67-72-75, 8(8722) 62-16-94.

Председатель Правления подпись **Абдурахманов К.А.**

М.П.

Исп. Ирганов Ю.Г.
руководитель СИБ
8 (8722) 67-72-75

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за июнь 2021 г.»

На компьютере, с использованием которого осуществляется работа в системе ДБО «iBank2», не рекомендуется устанавливать программное обеспечение, имеющее уязвимости с критичным уровнем опасности. К такому программному обеспечению относится программное обеспечение, указанное в таблице ниже.

№	Наименование уязвимого программного Обеспечения	Идентификатор уязвимостей	Описание уязвимости	Дата выявления	Ссылка на источники	Наличие обновлений
1.	Обход авторизации в веб-портале FortiOS SSL VPN	MITRE: CVE-2018-13382	Эксплуатация уязвимости позволяет удаленному злоумышленнику посредством отправки специально созданных HTTP-запросов изменить пароль произвольного пользователя портала SSL VPN. Уязвимость обусловлена некорректной авторизацией на портале SSL VPN.	30 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021060122 https://fortiguard.com/psirt/FG-IR-18-389	Есть
2.	Множественные уязвимости в Cisco ASR 5000 серии	MITRE: CVE-2021-1539	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику обойти процесс авторизации TACACS в целевой системе посредством отправки специально сформированного SSH-запроса. Уязвимость обусловлена некорректной обработкой команд из интерфейса командной строки. CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C CWE-863: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение.	2 июня 2021 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	Есть
3.	Множественные уязвимости в Cisco ASR 5000 серии	MITRE: CVE-2021-1540	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику, с учетной записью администратора и включенной опцией «nocli», обойти процесс авторизации в целевой системе посредством отправки специально сформированного SSH-запроса. Уязвимость обусловлена некорректной обработкой команд из интерфейса командной строки. CVSSv3.0: AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C CWE-863: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение.	2 июня 2021 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n	Есть
4.	Выполнение произвольного кода в Cisco Small Business серии RV	MITRE: CVE-2021-1309	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти в реализации протокола LLDP.	8 апреля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021040812 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-multi-lldp-u7e4chCe	Есть

5.	Выполнение произвольного кода в Visual Studio	MITRE: CVE-2021-27068	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных в Visual Studio.	11 мая 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021051138 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27068	Есть
	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-30544	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным использованием памяти в компоненте BFCache.	10 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021061001 https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop.html https://crbug.com/1212618	Есть
	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-30545 CVE-2021-30546 CVE-2021-30548 CVE-2021-30549 CVE-2021-30550	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным использованием памяти в компонентах Google Chrome.	10 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021061001 https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop.html https://crbug.com/1212618	Есть
	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-30547	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной обработкой HTML-данных в ANGLE.	10 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021061001 https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop.html https://crbug.com/1212618	Есть
	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-30551	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой смешения типов в компоненте V8.	10 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021061001 https://chromereleases.googleblog.com/2021/06/stable-channel-update-for-desktop.html https://crbug.com/1212618	Есть
	Выполнение произвольного кода в ОС Windows	MITRE: CVE-2021-31954	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии и выполнить произвольный код с привилегиями SYSTEM в целевой системе посредством открытия специально созданной вредоносной программы. Уязвимость обусловлена ошибкой границ памяти в драйвере clfs.sys.	11 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021060810 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31954 https://www.zerodayinitiative.com/advisories/ZDI-21-668/	Есть