ПромСвязьИнвест
расчетная небанковская кредитная организация
367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»
ОКПО 43340114 БИК № 048209395 корсчет 30103810982090000395
тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 www.psib.ru E-mail: office@psib.ru

«02» марта 2022г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за февраль 2022 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 _____ **Абдурахманов К.А.**
подпись

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за январь 2022 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.	Выполнение произвольного кода в Microsoft Office Visio	MITRE: CVE-2022-21988	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	8 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022020849 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21988	Есть
2.	Множественные уязвимости в Mozilla Firefox и Firefox ESR	MITRE: CVE-2022-22753	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена состоянием гонки в службе обновления.	8 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022020837 http://www.mozilla.org/en-US/security/advisories/mfsa2022-05/ http://www.mozilla.org/en-US/security/advisories/mfsa2022-04/	Есть
3.	Множественные уязвимости в Mozilla Firefox и Firefox ESR	MITRE: CVE-2022-22754	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством установки пользователем определенного типа расширения браузера. Уязвимость обусловлена некорректными ограничениями безопасности.	8 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022020849 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21988	Есть
4.	Множественные уязвимости в Adobe Illustrator CC	MITRE: CVE-2022-23186	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	8 февраля 2022 г.	http://helpx.adobe.com/security/products/illustrator/apsb22-07.html https://www.cybersecurity-help.cz/vdb/SB2022020848	Есть
5.	Выполнение произвольного кода в Adobe Photoshop	MITRE: CVE-2022-23203	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	8 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022020842 http://helpx.adobe.com/security/products/photoshop/apsb22-08.html	Есть
6.	Множественные уязвимости в Foxit PDF Reader и Editor для Windows	MITRE: CVE-2021-44708 CVE-2021-44709	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена ошибкой границ памяти.	28 января 2022 г.	http://www.foxitsoftware.com/support/security-bulletins.html https://www.cybersecurity-help.cz/vdb/SB2022012806	Есть

7.	Множественные уязвимости в Foxit PDF Reader и Editor для Windows	MITRE: CVE-2018-1285	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных.	28 января 2022 г.	http://www.foxitsoftware.com/support/security-bulletins.html https://www.cybersecurity-help.cz/vdb/SB2022012806	Есть
8.	Множественные уязвимости в Foxit PDF Reader и Editor для Windows	MITRE: CVE-2021-40420	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена ошибкой использования после освобождения.	28 января 2022 г.	http://www.foxitsoftware.com/support/security-bulletins.html https://www.cybersecurity-help.cz/vdb/SB2022012806	Есть
9.	Множественные уязвимости в Foxit PDF Reader и Editor для Windows	MITRE: CVE-2022-22150	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного PDF-файла. Уязвимость обусловлена ошибкой границ памяти.	28 января 2022 г.	http://www.foxitsoftware.com/support/security-bulletins.html https://www.cybersecurity-help.cz/vdb/SB2022012806	Есть
10.	Выполнение произвольного кода в TightVNC	MITRE: CVE-2022-23967	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти при обработке данных в функции InitialiseRFBConnection.	30 января 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022012807 http://www.tightvnc.com/licensing-server-x11.php http://github.com/MaherAzzouzi/CVE-2022-23967	Есть
11.	Множественные уязвимости Microsoft Edge (Chromium-based)	MITRE: CVE-2022-0459 CVE-2022-0452 CVE-2022-0453 CVE-2022-0456 CVE-2022-0458	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	1 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022020404 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0452 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0467 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0462 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0457 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0459 http://crbug.com/1287962 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0453 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0454 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0456	Есть
12.	Множественные уязвимости Microsoft Edge (Chromium-based)	MITRE: CVE-2022-23263	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	1 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022020404 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0452 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0467 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0462 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0457 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0459 http://crbug.com/1287962 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0453 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0454 http://portal.msrc.microsoft.com/en-	Есть

					US/security-guidance/advisory/CVE-2022-0456	
13.	Множественные уязвимости Microsoft Edge (Chromium-based)	MITRE: CVE-2022-0462	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	1 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022020404 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0452 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0467 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0462 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0457 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0459 http://crbug.com/1287962 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0453 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0454 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0456	Есть
14.	Множественные уязвимости Microsoft Edge (Chromium-based)	MITRE: CVE-2022-0462 CVE-2022-0466 CVE-2022-0467	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией Scroll.	1 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022020404 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0452 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0467 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0462 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0457 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0459 http://crbug.com/1287962 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop.html http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0453 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0454 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0456	Есть
15.	Выполнение произвольного кода в Apple Safari	MITRE: CVE-2022-22620	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	10 февраля 2022 г.	http://support.apple.com/en-us/HT213091 https://www.cybersecurity-help.cz/vdb/SB2022021014	Есть
16.	Множественные уязвимости в Zabbix	MITRE: CVE-2022-23132	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена некорректными ограничениями безопасности.	23 февраля 2022 г.	http://support.zabbix.com/browse/ZBX-20350 http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6SZYHXINBKCY42ITFSNCYE7KCSF33VRA/ http://support.zabbix.com/browse/ZBX-20341 https://www.cybersecurity-help.cz/vdb/SB2022022306 http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VB6W556GVXOKUYTASTDGL3AI7S3SJHX7/	Есть
17.	Множественные уязвимости в Zabbix	MITRE: CVE-2022-23131	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректной работой процесса аутентификации.	23 февраля 2022 г.	http://support.zabbix.com/browse/ZBX-20350 http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/6SZYHXINBKCY42ITFSNCYE7KCSF33VRA/ http://support.zabbix.com/browse/ZBX-20341	Есть

					https://www.cybersecurity-help.cz/vdb/SB2022022306 http://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/VB6W556GVXOKUYTASTDGL3AI7S3SJHX7/	
18.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-0603 CVE-2022-0605 CVE-2022-0606 CVE-2022-0607 CVE-2022-0609	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	14 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022021430 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html http://crbug.com/1273397 http://crbug.com/1286940 http://crbug.com/1285449 http://crbug.com/1296150 http://crbug.com/1270333 http://crbug.com/1290008 http://crbug.com/1288020 http://crbug.com/1250655	Есть
19.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-0604	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	14 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022021430 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html http://crbug.com/1273397 http://crbug.com/1286940 http://crbug.com/1285449 http://crbug.com/1296150 http://crbug.com/1270333 http://crbug.com/1290008 http://crbug.com/1288020 http://crbug.com/1250655	Есть
20.	Множественные уязвимости в Google Chrome	MITRE: CVE-2022-0608	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена целочисленным переполнением.	14 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022021430 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html http://crbug.com/1273397 http://crbug.com/1286940 http://crbug.com/1285449 http://crbug.com/1296150 http://crbug.com/1270333 http://crbug.com/1290008 http://crbug.com/1288020 http://crbug.com/1250655	Есть
21.	Множественные уязвимости в Mozilla Thunderbird	MITRE: CVE-2022-22753	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе. Уязвимость обусловлена состоянием гонки в службе обновления.	11 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022021114 http://www.mozilla.org/en-US/security/advisories/mfsa2022-06/	Есть
22.	Множественные уязвимости в Mozilla Thunderbird	MITRE: CVE-2022-22754	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством установки пользователем определенного типа расширения. Уязвимость обусловлена некорректными ограничениями безопасности.	11 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022021114 http://www.mozilla.org/en-US/security/advisories/mfsa2022-06/	Есть
23.	Множественные уязвимости в Mozilla Thunderbird	MITRE: CVE-2022-22756	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством переноса пользователем на рабочий стол специально созданного вредоносного изображения. Уязвимость обусловлена некорректной идентификации файлов во время операции перетаскивания.	11 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022021114 http://www.mozilla.org/en-US/security/advisories/mfsa2022-06/	Есть
24.	Множественные уязвимости в Mozilla Thunderbird	MITRE: CVE-2022-22764	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально	11 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022021114 http://www.mozilla.org/en-US/security/advisories/mfsa2022-06/	Есть

			созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.			
25.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2022-0603 CVE-2022-0605 CVE-2022-0606 CVE-2022-0607 CVE-2022-0609	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения.	16 февраля 2022 г.	https://www.cybersecurity-help.cz/vdb/SB2022021622 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0610 http://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html http://crbug.com/1290008 http://crbug.com/1285449 http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0603 http://crbug.com/1273397	Есть