

# ПРОМСВЯЗЬИНВЕСТ

расчетная небанковская кредитная организация

367000 РФ, Республика Дагестан, г. Махачкала, ул. Ирчи-Казака 2 «б»

ОКПО 43340114 БИК № 048209395 корсчет 301038109820900000395

тел.(8722) 62-16-24, 61-58-22 факс.(8722) 62-16-94 [www.psib.ru](http://www.psib.ru) E-mail: office@psib.ru

«10» января 2022г.

г. Махачкала

## «Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за декабрь 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.

ВРИО Председателя Правления



Исланов Р.О.

подпись

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 декабрь 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 уязвимости | Описание уязвимости  | Дата выявления     | Ссылка на источники  | Наличие обновлений |
|---|---|--------------------------|--|--------------------|--|--------------------|
| 1 | Выполнение произвольного кода в D-Link DSL-3782           | Не определен             | 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.        | 28 октября 2021 г. | <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37997">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37997</a><br><a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37998">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37998</a>   | Есть               |
| 2 | Выполнение произвольного кода в D-Link DSL-3782           | Не определен             | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.                                    | 2 декабря 2021 г.  | <a href="https://www.cybersecurity-help.cz/vdb/SB2021120209">https://www.cybersecurity-help.cz/vdb/SB2021120209</a><br><a href="http://packetstormsecurity.com/files/165084">http://packetstormsecurity.com/files/165084</a>   | Есть               |
| 3 | Множественные уязвимости в Cisco Security Manager         | MITRE: CVE-2021-34798    | Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена ошибкой разыменования указателя NULL.                                | 29 ноября 2021 г.  | <a href="https://www.cybersecurity-help.cz/vdb/SB2021112903">https://www.cybersecurity-help.cz/vdb/SB2021112903</a><br><a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-2.4.49-VWL69sWQ">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-2.4.49-VWL69sWQ</a>   | Есть               |
| 4 | Выполнение произвольного кода в Apache Log4j              | MITRE: CVE-2021-44228    | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.                                    | 10 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121003">https://www.cybersecurity-help.cz/vdb/SB2021121003</a><br><a href="http://www.lunasec.io/docs/blog/log4j-zero-day/">http://www.lunasec.io/docs/blog/log4j-zero-day/</a><br><a href="http://github.com/apache/logging-log4j2/pull/608">http://github.com/apache/logging-log4j2/pull/608</a><br><a href="http://github.com/advisories/GHSA-jfh8-c2jp-5v3q">http://github.com/advisories/GHSA-jfh8-c2jp-5v3q</a>   | Есть               |
| 5 | Выполнение произвольного кода в Mozilla NSS               | MITRE: CVE-2021-43527    | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти при обработке DSA-подписей в формате DER или RSA-PSS. | 1 декабря 2021 г.  | <a href="https://www.cybersecurity-help.cz/vdb/SB2021120123">https://www.cybersecurity-help.cz/vdb/SB2021120123</a><br><a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-51/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-51/</a>   | Есть               |
| 6 | Выполнение произвольного кода в FortiGate FortiOS SSL VPN | MITRE: CVE-2021-26109    | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена целочисленным  | 7 декабря 2021 г.  | <a href="https://www.cybersecurity-help.cz/vdb/SB2021120715">https://www.cybersecurity-help.cz/vdb/SB2021120715</a><br><a href="http://www.fortiguard.com/psirt/FG-IR-21-049">http://www.fortiguard.com/psirt/FG-IR-21-049</a><br><a href="https://www.cybersecurity-help.cz/vdb/SB2021120701">https://www.cybersecurity-help.cz/vdb/SB2021120701</a><br><a href="http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html">http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html</a> | Есть               |



|    |  |  |  |                    |   |      |
|----|--|--|--|--------------------|---|------|
|    |  |  | переполнением  |                    | <a href="http://crbug.com/1272403">http://crbug.com/1272403</a><br><a href="http://crbug.com/1274641">http://crbug.com/1274641</a><br><a href="http://crbug.com/1274499">http://crbug.com/1274499</a><br><a href="http://crbug.com/1273674">http://crbug.com/1273674</a><br><a href="http://crbug.com/1273197">http://crbug.com/1273197</a><br><a href="http://crbug.com/1273176">http://crbug.com/1273176</a><br><a href="http://crbug.com/1271456">http://crbug.com/1271456</a><br><a href="http://crbug.com/1267661">http://crbug.com/1267661</a><br><a href="http://crbug.com/1270990">http://crbug.com/1270990</a><br><a href="http://crbug.com/1267496">http://crbug.com/1267496</a><br><a href="http://crbug.com/1262183">http://crbug.com/1262183</a><br><a href="http://crbug.com/1267791">http://crbug.com/1267791</a><br><a href="http://crbug.com/1239760">http://crbug.com/1239760</a><br><a href="http://crbug.com/1266510">http://crbug.com/1266510</a><br><a href="http://crbug.com/1260939">http://crbug.com/1260939</a>   |      |
| 7  | Множественные уязвимости в Google Chrome   | MITRE: CVE-2021-4055 CVE-2021-4058 CVE-2021-4062 | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.                         | 7 декабря 2021 г.  | <a href="https://www.cybersecurity-help.cz/vdb/SB2021120701">https://www.cybersecurity-help.cz/vdb/SB2021120701</a><br><a href="http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html">http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html</a><br><a href="http://crbug.com/1272403">http://crbug.com/1272403</a><br><a href="http://crbug.com/1274641">http://crbug.com/1274641</a><br><a href="http://crbug.com/1274499">http://crbug.com/1274499</a><br><a href="http://crbug.com/1273674">http://crbug.com/1273674</a><br><a href="http://crbug.com/1273197">http://crbug.com/1273197</a><br><a href="http://crbug.com/1273176">http://crbug.com/1273176</a><br><a href="http://crbug.com/1271456">http://crbug.com/1271456</a><br><a href="http://crbug.com/1267661">http://crbug.com/1267661</a><br><a href="http://crbug.com/1270990">http://crbug.com/1270990</a><br><a href="http://crbug.com/1267496">http://crbug.com/1267496</a><br><a href="http://crbug.com/1262183">http://crbug.com/1262183</a><br><a href="http://crbug.com/1267791">http://crbug.com/1267791</a><br><a href="http://crbug.com/1239760">http://crbug.com/1239760</a><br><a href="http://crbug.com/1266510">http://crbug.com/1266510</a><br><a href="http://crbug.com/1260939">http://crbug.com/1260939</a> | Есть |
| 8  | Множественные уязвимости в Google Chrome   | MITRE: CVE-2021-4054                             | Эксплуатация уязвимости позволяет удаленному злоумышленнику подделать содержимое веб-страницы посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной проверкой входных данных при автозаполнении. | 7 декабря 2021 г.  | <a href="https://www.cybersecurity-help.cz/vdb/SB2021120701">https://www.cybersecurity-help.cz/vdb/SB2021120701</a><br><a href="http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html">http://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html</a><br><a href="http://crbug.com/1272403">http://crbug.com/1272403</a><br><a href="http://crbug.com/1274641">http://crbug.com/1274641</a><br><a href="http://crbug.com/1274499">http://crbug.com/1274499</a><br><a href="http://crbug.com/1273674">http://crbug.com/1273674</a><br><a href="http://crbug.com/1273197">http://crbug.com/1273197</a><br><a href="http://crbug.com/1273176">http://crbug.com/1273176</a><br><a href="http://crbug.com/1271456">http://crbug.com/1271456</a><br><a href="http://crbug.com/1267661">http://crbug.com/1267661</a><br><a href="http://crbug.com/1270990">http://crbug.com/1270990</a><br><a href="http://crbug.com/1267496">http://crbug.com/1267496</a><br><a href="http://crbug.com/1262183">http://crbug.com/1262183</a><br><a href="http://crbug.com/1267791">http://crbug.com/1267791</a><br><a href="http://crbug.com/1239760">http://crbug.com/1239760</a><br><a href="http://crbug.com/1266510">http://crbug.com/1266510</a><br><a href="http://crbug.com/1260939">http://crbug.com/1260939</a> | Есть |
| 9  | Выполнение произвольного кода в Tenda AC15 | MITRE: CVE-2021-44352                            | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.  | 7 декабря 2021 г.  | <a href="https://www.cybersecurity-help.cz/vdb/SB2021120709">https://www.cybersecurity-help.cz/vdb/SB2021120709</a><br><a href="http://github.com/zhlu32/cve/blob/main/tenda/Tenda-ac15-buffer-overflow.md">http://github.com/zhlu32/cve/blob/main/tenda/Tenda-ac15-buffer-overflow.md</a>  | Есть |
| 10 | Множественные уязвимости в Apple Safari    | MITRE: CVE-2021-30934                            | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.                         | 15 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121510">https://www.cybersecurity-help.cz/vdb/SB2021121510</a><br><a href="http://support.apple.com/en-us/HT212978">http://support.apple.com/en-us/HT212978</a>  | Есть |
| 11 | Множественные уязвимости в Apple Safari    | MITRE: CVE-2021-30936 CVE-2021-30951             | Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой  | 15 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121510">https://www.cybersecurity-help.cz/vdb/SB2021121510</a><br><a href="http://support.apple.com/en-us/HT212978">http://support.apple.com/en-us/HT212978</a>  | Есть |

|    |   |                       |   |  |                    |  |      |
|----|---|-----------------------|---|--|--------------------|--|------|
|    |   |                       | использования<br>освобождения.  | после  |                    |  |      |
| 12 | Множественные уязвимости в Apple Safari                         | MITRE: CVE-2021-30952 | Эксплуатация позволяет злоумышленнику произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена целочисленным переполнением.                      | уязвимости удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.                         | 15 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121510">https://www.cybersecurity-help.cz/vdb/SB2021121510</a><br><a href="http://support.apple.com/en-us/HT212978">http://support.apple.com/en-us/HT212978</a>   | Есть |
| 13 | Выполнение произвольного кода в TP-Link TL-WR840N EU v5         | MITRE: CVE-2021-41653 | Эксплуатация позволяет злоумышленнику произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.                                       | уязвимости удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной проверкой входных данных.                  | 10 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121007">https://www.cybersecurity-help.cz/vdb/SB2021121007</a><br><a href="http://k4m1l10.com/cve-2021-41653.html">http://k4m1l10.com/cve-2021-41653.html</a><br><a href="http://tp-link.com">http://tp-link.com</a><br><a href="http://www.tp-link.com/us/press/security-advisory/">http://www.tp-link.com/us/press/security-advisory/</a>   | Есть |
| 14 | Множественные уязвимости в Adobe Photoshop                      | MITRE: CVE-2021-43018 | Эксплуатация позволяет злоумышленнику произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PSD-файла. Уязвимость обусловлена ошибкой границ памяти.                             | уязвимости удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PSD-файла. Уязвимость обусловлена ошибкой границ памяти.                             | 14 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121490">https://www.cybersecurity-help.cz/vdb/SB2021121490</a><br><a href="http://helpx.adobe.com/security/products/photoshop/apsb21-113.html">http://helpx.adobe.com/security/products/photoshop/apsb21-113.html</a>   | Есть |
| 15 | Множественные уязвимости в Adobe Photoshop                      | MITRE: CVE-2021-44184 | Эксплуатация позволяет злоумышленнику произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PSD-файла. Уязвимость обусловлена ошибкой границ памяти.                             | уязвимости удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PSD-файла. Уязвимость обусловлена ошибкой границ памяти.                             | 14 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121490">https://www.cybersecurity-help.cz/vdb/SB2021121490</a><br><a href="http://helpx.adobe.com/security/products/photoshop/apsb21-113.html">http://helpx.adobe.com/security/products/photoshop/apsb21-113.html</a>   | Есть |
| 16 | Выполнение произвольного кода в Microsoft Remote Desktop Client | MITRE: CVE-2021-43233 | Эксплуатация позволяет злоумышленнику произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в клиенте удаленного рабочего стола. | уязвимости удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных в клиенте удаленного рабочего стола. | 14 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121486">https://www.cybersecurity-help.cz/vdb/SB2021121486</a><br><a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43233">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43233</a>   | Есть |
| 17 | Выполнение произвольного кода в Microsoft Excel                 | MITRE: CVE-2021-43256 | Эксплуатация позволяет злоумышленнику произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных  | уязвимости удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной проверкой входных данных  | 14 декабря 2021 г. | <a href="https://www.cybersecurity-help.cz/vdb/SB2021121447">https://www.cybersecurity-help.cz/vdb/SB2021121447</a><br><a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43256">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43256</a>   | Есть |
| 18 | Множественные уязвимости в Mozilla Thunderbird                  | MITRE: CVE-2021-43537 | Эксплуатация позволяет злоумышленнику произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным преобразованием типа.                | уязвимости удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным преобразованием типа.                | 7 декабря 2021 г.  | <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-52/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-52/</a><br><a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-53/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-53/</a><br><a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-54/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-54/</a><br><a href="https://www.cybersecurity-help.cz/vdb/SB2021120712">https://www.cybersecurity-help.cz/vdb/SB2021120712</a> | Есть |