

# 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](mailto:office@psib.ru)

«01» ноября 2021г.

г. Махачкала

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



Абдурахманов К.А.

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 октябрь 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	Множественные уязвимости в Apache HTTP Server	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.	17 сентября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101922">https://www.cybersecurity-help.cz/vdb/SB2021101922</a> <a href="http://httpd.apache.org/security/vulnerabilities_24.html">http://httpd.apache.org/security/vulnerabilities_24.html</a>	Есть
2	Множественные уязвимости в Apache HTTP Server	MITRE: CVE-2021-40438	Эксплуатация уязвимости позволяет удаленному злоумышленнику провести SSRF-атаку посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входных данных в модуле mod_proxy на HTTP-сервере Apache.	17 сентября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101922">https://www.cybersecurity-help.cz/vdb/SB2021101922</a> <a href="http://httpd.apache.org/security/vulnerabilities_24.html">http://httpd.apache.org/security/vulnerabilities_24.html</a>	Есть
3	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-37989 CVE-2021-37990	Эксплуатация уязвимости позволяет удаленному злоумышленнику посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией компонента в Google Chrome.	19 октября 2021 г.	<a href="http://crbug.com/1242404">http://crbug.com/1242404</a> <a href="http://crbug.com/1253399">http://crbug.com/1253399</a> <a href="http://crbug.com/1248661">http://crbug.com/1248661</a> <a href="http://crbug.com/1233067">http://crbug.com/1233067</a> <a href="http://crbug.com/1241860">http://crbug.com/1241860</a> <a href="http://crbug.com/1246631">http://crbug.com/1246631</a> <a href="http://crbug.com/1250660">http://crbug.com/1250660</a> <a href="http://crbug.com/1249810">http://crbug.com/1249810</a> <a href="http://crbug.com/1247395">http://crbug.com/1247395</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101923">https://www.cybersecurity-help.cz/vdb/SB2021101923</a> <a href="http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html">http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html</a>	Есть
4	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-37991	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена состоянием гонки в компоненте V8 в Google Chrome.	19 октября 2021 г.	<a href="http://crbug.com/1242404">http://crbug.com/1242404</a> <a href="http://crbug.com/1253399">http://crbug.com/1253399</a> <a href="http://crbug.com/1248661">http://crbug.com/1248661</a> <a href="http://crbug.com/1233067">http://crbug.com/1233067</a> <a href="http://crbug.com/1241860">http://crbug.com/1241860</a> <a href="http://crbug.com/1246631">http://crbug.com/1246631</a> <a href="http://crbug.com/1250660">http://crbug.com/1250660</a> <a href="http://crbug.com/1249810">http://crbug.com/1249810</a> <a href="http://crbug.com/1247395">http://crbug.com/1247395</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101923">https://www.cybersecurity-help.cz/vdb/SB2021101923</a> <a href="http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html">http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html</a>	Есть
5	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-37986 CVE-2021-37984 CVE-2021-37981	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных.	19 октября 2021 г.	<a href="http://crbug.com/1242404">http://crbug.com/1242404</a> <a href="http://crbug.com/1253399">http://crbug.com/1253399</a> <a href="http://crbug.com/1248661">http://crbug.com/1248661</a> <a href="http://crbug.com/1233067">http://crbug.com/1233067</a> <a href="http://crbug.com/1241860">http://crbug.com/1241860</a> <a href="http://crbug.com/1246631">http://crbug.com/1246631</a> <a href="http://crbug.com/1250660">http://crbug.com/1250660</a> <a href="http://crbug.com/1249810">http://crbug.com/1249810</a> <a href="http://crbug.com/1247395">http://crbug.com/1247395</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101923">https://www.cybersecurity-help.cz/vdb/SB2021101923</a>	Есть



					<a href="http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html">http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html</a>	
6	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-37985 CVE-2021-37983 CVE-2021-37982	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.	19 октября 2021 г.	<a href="http://crbug.com/1242404">http://crbug.com/1242404</a> <a href="http://crbug.com/1253399">http://crbug.com/1253399</a> <a href="http://crbug.com/1248661">http://crbug.com/1248661</a> <a href="http://crbug.com/1233067">http://crbug.com/1233067</a> <a href="http://crbug.com/1241860">http://crbug.com/1241860</a> <a href="http://crbug.com/1246631">http://crbug.com/1246631</a> <a href="http://crbug.com/1250660">http://crbug.com/1250660</a> <a href="http://crbug.com/1249810">http://crbug.com/1249810</a> <a href="http://crbug.com/1247395">http://crbug.com/1247395</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101923">https://www.cybersecurity-help.cz/vdb/SB2021101923</a> <a href="http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html">http://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html</a>	Есть
7	Выполнение произвольного кода в Microsoft Windows Graphics Component	MITRE: CVE-2021-41340	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	12 октября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101229">https://www.cybersecurity-help.cz/vdb/SB2021101229</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41340">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41340</a>	Есть
8	Выполнение произвольного кода в Microsoft Windows Media Foundation	MITRE: CVE-2021-41330	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	12 октября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101212">https://www.cybersecurity-help.cz/vdb/SB2021101212</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41330">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41330</a>	Есть
9	Множественные уязвимости в Adobe Acrobat Reader	MITRE: CVE-2021-40728	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла PDF. Уязвимость обусловлена ошибкой использования после освобождения при обработке файлов PDF.	12 октября 2021 г.	<a href="http://helpx.adobe.com/security/products/acrobat/apsb21-104.html">http://helpx.adobe.com/security/products/acrobat/apsb21-104.html</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101243">https://www.cybersecurity-help.cz/vdb/SB2021101243</a>	Есть
10	Множественные уязвимости в Adobe Acrobat Reader	MITRE: CVE-2021-40731	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла PDF. Уязвимость обусловлена ошибкой границ памяти.	12 октября 2021 г.	<a href="http://helpx.adobe.com/security/products/acrobat/apsb21-104.html">http://helpx.adobe.com/security/products/acrobat/apsb21-104.html</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101243">https://www.cybersecurity-help.cz/vdb/SB2021101243</a>	Есть
11	Выполнение произвольного кода в Windows Media Audio Decoder	MITRE: CVE-2021-41331	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	12 октября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101218">https://www.cybersecurity-help.cz/vdb/SB2021101218</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41331">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41331</a>	Есть
12	Множественные уязвимости в Foxit PDF Reader for Windows	MITRE: CVE-2021-41780 CVE-2021-41781 CVE-2021-41782 CVE-2021-41783 CVE-2021-41784 CVE-2021-	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла PDF. Уязвимость обусловлена ошибкой границ памяти при обработке файлов PDF.	12 октября 2021 г.	<a href="http://www.foxitsoftware.com/support/security-bulletins.html">http://www.foxitsoftware.com/support/security-bulletins.html</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101204">https://www.cybersecurity-help.cz/vdb/SB2021101204</a>	Есть



		41785				
13	Выполнение произвольного кода в Microsoft Word	MITRE: CVE-2021-40486	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	12 октября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101216">https://www.cybersecurity-help.cz/vdb/SB2021101216</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40486">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40486</a>	Есть
14	Повышение привилегий в ОС Windows	MITRE: CVE-2021-40449	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код с повышенными привилегиями в целевой системе посредством открытия специально созданного файла. Уязвимость обусловлена ошибкой использования после освобождения в функции Win32k NtGdiResetDC в ядре Microsoft Windows.	12 октября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101211">https://www.cybersecurity-help.cz/vdb/SB2021101211</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449</a> <a href="http://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/">http://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/</a> <a href="http://www.virustotal.com/gui/file/b7fb3623e31fb36fc3d3a4d99829e42910cad4da4fa7429a2d99a838e004366e">http://www.virustotal.com/gui/file/b7fb3623e31fb36fc3d3a4d99829e42910cad4da4fa7429a2d99a838e004366e</a>	Есть
15	Выполнение произвольного кода в Microsoft Office	MITRE: CVE-2021-40480 CVE-2021-40481	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	12 октября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101219">https://www.cybersecurity-help.cz/vdb/SB2021101219</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40480">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40480</a>	Есть
16	Выполнение произвольного кода в Microsoft Excel	MITRE: CVE-2021-40485 CVE-2021-40471 CVE-2021-40473 CVE-2021-40474 CVE-2021-40479	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	12 октября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101217">https://www.cybersecurity-help.cz/vdb/SB2021101217</a> <a href="http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40485">http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40485</a>	Есть
17	Множественные уязвимости в Mozilla Firefox	MITRE: CVE-2021-38496 CVE-2021-38498	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.	5 октября 2021 г.	<a href="http://github.com/crossbeam-rs/crossbeam/security/advisories/GHSA-pqqp-xmhj-wgcw">http://github.com/crossbeam-rs/crossbeam/security/advisories/GHSA-pqqp-xmhj-wgcw</a> <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-45/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-45/</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101208">https://www.cybersecurity-help.cz/vdb/SB2021101208</a> <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-44/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-44/</a> <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-43/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-43/</a>	Есть
18	Множественные уязвимости в Mozilla Firefox	MITRE: CVE-2021-32810	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена состоянием гонки в функциях "Stealer::steal", "Stealer::steal_batch" и "Stealer::steal_batch_and_pop"	5 октября 2021 г.	<a href="http://github.com/crossbeam-rs/crossbeam/security/advisories/GHSA-pqqp-xmhj-wgcw">http://github.com/crossbeam-rs/crossbeam/security/advisories/GHSA-pqqp-xmhj-wgcw</a> <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-45/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-45/</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101208">https://www.cybersecurity-help.cz/vdb/SB2021101208</a> <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-44/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-44/</a> <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-43/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-43/</a>	Есть
19	Множественные уязвимости в Mozilla Firefox	MITRE: CVE-2021-38500 CVE-2021-38501	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость	5 октября 2021 г.	<a href="http://github.com/crossbeam-rs/crossbeam/security/advisories/GHSA-pqqp-xmhj-wgcw">http://github.com/crossbeam-rs/crossbeam/security/advisories/GHSA-pqqp-xmhj-wgcw</a> <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-45/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-45/</a> <a href="https://www.cybersecurity-help.cz/vdb/SB2021101208">https://www.cybersecurity-help.cz/vdb/SB2021101208</a> <a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-44/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-44/</a>	Есть



			обусловлена ошибкой границ памяти при обработке HTML-данных.		<a href="http://www.mozilla.org/en-US/security/advisories/mfsa2021-43/">http://www.mozilla.org/en-US/security/advisories/mfsa2021-43/</a>	
20	Выполнение произвольного кода в OpenOffice	MITRE: CVE-2021-33035	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного документа DBF. Уязвимость обусловлена ошибкой границ памяти.	11 октября 2021 г.	<a href="https://www.cybersecurity-help.cz/vdb/SB2021101111">https://www.cybersecurity-help.cz/vdb/SB2021101111</a> <a href="http://github.com/apache/openoffice/commit/e5fddae0151af3be16078cc4d88c6bae0f911e56#diff-ea66e734dd358922aba12ad4ba39c96bdc6cbde587d07dbc63d04daa0a30e90f">http://github.com/apache/openoffice/commit/e5fddae0151af3be16078cc4d88c6bae0f911e56#diff-ea66e734dd358922aba12ad4ba39c96bdc6cbde587d07dbc63d04daa0a30e90f</a> <a href="http://lists.apache.org/thread.html/r929c0c6a53cad64a1007b878342756badbb05ddd9b8f31a6d0b424cb@%3Cannounce.apache.org%3E">http://lists.apache.org/thread.html/r929c0c6a53cad64a1007b878342756badbb05ddd9b8f31a6d0b424cb@%3Cannounce.apache.org%3E</a> <a href="http://lists.apache.org/thread.html/r1ab8532e11f41bc7ca057ac7e39cab25f2e1f9d5f4929788ae21c8b9@%3Cusers.openoffice.apache.org%3E">http://lists.apache.org/thread.html/r1ab8532e11f41bc7ca057ac7e39cab25f2e1f9d5f4929788ae21c8b9@%3Cusers.openoffice.apache.org%3E</a> <a href="http://www.openwall.com/lists/oss-security/2021/10/07/3">http://www.openwall.com/lists/oss-security/2021/10/07/3</a>	Есть
21	Выполнение произвольного кода в ПО Siemens	MITRE: CVE-2021-37202 CVE-2021-41535 CVE-2021-41536 CVE-2021-41537 CVE-2021-41539 CVE-2021-41540	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной обработкой файлов форматов IFC и OBJ.	30 сентября 2021 г.	<a href="https://support.sw.siemens.com/portal.siemens.com/productcert/txt/ssa-728618.txt">https://support.sw.siemens.com/portal.siemens.com/productcert/txt/ssa-728618.txt</a> <a href="https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf">https://cert-portal.siemens.com/productcert/pdf/ssa-728618.pdf</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-21-1124/">https://www.zerodayinitiative.com/advisories/ZDI-21-1124/</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-21-1123/">https://www.zerodayinitiative.com/advisories/ZDI-21-1123/</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-21-1121/">https://www.zerodayinitiative.com/advisories/ZDI-21-1121/</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-21-1120/">https://www.zerodayinitiative.com/advisories/ZDI-21-1120/</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-21-1119/">https://www.zerodayinitiative.com/advisories/ZDI-21-1119/</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-21-1118/">https://www.zerodayinitiative.com/advisories/ZDI-21-1118/</a> <a href="https://www.zerodayinitiative.com/advisories/ZDI-21-1117/">https://www.zerodayinitiative.com/advisories/ZDI-21-1117/</a>	Есть