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

«18» августа 2021г. **г. Махачкала**

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

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 июль 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.	Повышение привилегий в инструментах VMware	MITRE: CVE-2021-21999	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством размещения вредоносного файла на виртуальной машине. Уязвимость обусловлена некорректным применением политик безопасности.	22 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021062226 https://www.vmware.com/security/advisories/VMSA-2021-0013.html https://www.zerodayinitiative.com/advisories/ZDI-21-754/	Есть
2.	Множественные уязвимости в Microsoft Edge (Chromium-based)	MITRE: CVE-2021-30554	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной использованием памяти в компоненте WebGL в Google Chrome	18 июня 2021 г.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30554 https://www.cybersecurity-help.cz/vdb/SB2021061816	Есть
3.	Множественные уязвимости в Microsoft Edge (Chromium-based)	MITRE: CVE-2021-30555 CVE-2021-30556 CVE-2021-30557	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной использованием памяти в компонентах Google Chrome.	18 июня 2021 г.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-30554 https://www.cybersecurity-help.cz/vdb/SB2021061816	Есть
4.	Выполнение произвольного кода в Windows	MITRE: CVE-2021-34527	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код с привилегиями пользователя SYSTEM в целевой системе посредством отправки специально сформированного запроса диспетчеру очереди печати Windows. Уязвимость обусловлена некорректной проверкой входных данных в функции RpcAddPrinterDriverEx().	29 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021070204 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527	Нет
5.	Множественные уязвимости в Autodesk и AutoCAD	MITRE: CVE-2021-27040 CVE-2021-27042	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного DWG файла.	5 июля 2021 г.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0004	Есть

			Уязвимость обусловлена некорректным определением границ памяти при синтаксическом анализе файла.			
6.	Множественные уязвимости в Autodesk и AutoCAD	MITRE: CVE-2021-27041 CVE-2021-27043	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного DWG файла. Уязвимость обусловлена ошибкой записи за пределы выделенного буфера памяти.	5 июля 2021 г.	https://www.autodesk.com/trust/security-advisories/adsk-sa-2021-0004	Есть
7.	Множественные уязвимости в Apache Traffic Server	MITRE: CVE-2021-32565	Эксплуатация уязвимости позволяет удаленному злоумышленнику повредить целостность данных в целевой системе посредством отправки специально сформированных вредоносных HTTP-запросов. Уязвимость обусловлена некорректной обработкой заголовка Content-Length.	30 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021063020	Есть
8.	Множественные уязвимости в Apache Traffic Server	MITRE: CVE-2021-32566	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных вредоносных HTTP-запросов. Уязвимость обусловлена некорректной проверкой входных данных при обработке HTTP/2.	30 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021063020	Есть
9.	Множественные уязвимости в Apache Traffic Server	MITRE: CVE-2021-35474	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных вредоносных сетевых пакетов. Уязвимость обусловлена некорректным определением границ буфера памяти в плагине cachekey.	30 июня 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021063020	Есть
10.	Выполнение произвольного кода в PHP	MITRE: CVE-2021-21704	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена переполнением буфера в функциях firebird_info_cb(), firebird_handle_doer(), firebird_stmt_execute() и firebird_fetch_blob().	6 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021070611 https://www.php.net/ChangeLog-8.php#8.0.8 https://www.php.net/ChangeLog-7.php#7.4.21 https://www.php.net/ChangeLog-7.php#7.3.29 http://bugs.php.net/76448 http://bugs.php.net/76449 http://bugs.php.net/76450 http://bugs.php.net/76452	Есть
11.	Множественные уязвимости в Mozilla Firefox	MITRE: CVE-2021-29970	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 функции специальных возможностей при обработке HTML данных.	13 июля 2021 г.	https://www.mozilla.org/en-US/security/advisories/mfsa2021-28/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-29/ https://www.cybersecurity-help.cz/vdb/SB2021071316	Есть
12.	Множественные уязвимости в Mozilla Firefox	MITRE: CVE-2021-29972	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость	13 июля 2021 г.	https://www.mozilla.org/en-US/security/advisories/mfsa2021-28/ https://www.mozilla.org/en-US/security/advisories/mfsa2021-29/ https://www.cybersecurity-help.cz/vdb/SB2021071316	Есть

			обусловлена некорректным использованием памяти в библиотеке Cairo.			
13.	Множественные уязвимости в Microsoft Exchange Server	MITRE: CVE-2021-31196	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	13 июля 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31196 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34470 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33768 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31206	Есть
14.	Множественные уязвимости в Microsoft Exchange Server	MITRE: CVE-2021-34470 CVE-2021-33768	Эксплуатация уязвимости позволяет аутентифицированному злоумышленнику из смежной сети повысить свои привилегии в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректным применением ограничений безопасности в Microsoft Exchange Server	13 июля 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31196 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34470 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33768 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31206	Есть
15.	Множественные уязвимости в Microsoft Exchange Server	MITRE: CVE-2021-34473	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	13 июля 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31196 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34470 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33768 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31206	Есть
16.	Множественные уязвимости в Microsoft Exchange Server	MITRE: CVE-2021-34523	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику повысить свои привилегии в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректным применением ограничений безопасности в Microsoft Exchange Server.	13 июля 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31196 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34470 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33768 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31206	Есть
17.	Множественные уязвимости в Microsoft Exchange Server	MITRE: CVE-2021-31206	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных.	13 июля 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31196 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34470 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33768 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31206	Есть
18.	Повышение привилегий в ядре Windows	MITRE: CVE-2021-31979	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код с повышенными привилегиями в целевой системе посредством запуска специально созданного вредоносного файла. Уязвимость обусловлена некорректным	13 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071326 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31979	Есть

			определением границ буфера памяти в ядре Windows.			
19.	Выполнение произвольного кода в Microsoft Windows Media	MITRE: CVE-2021-33740	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного вредоносного запроса. Уязвимость обусловлена некорректной проверкой входных данных в Windows Media.	13 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071325 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33740	Есть
20.	Повышение привилегий в Windows	MITRE: CVE-2021-33771	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством запуска специально созданного вредоносного файла. Уязвимость обусловлена некорректным определением границ буфера памяти.	13 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071322 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33771	Есть
21.	Выполнение произвольного кода в Microsoft Word	MITRE: CVE-2021-34452	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных в Microsoft Word.	13 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071358 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34452	Есть
22.	Выполнение произвольного кода в Microsoft Excel	MITRE: CVE-2021-34501 CVE-2021-34518	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных в Microsoft Excel.	13 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071359 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34501 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34518	Есть
23.	Выполнение произвольного кода в ОС Windows	MITRE: CVE-2021-1675	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных в службе диспетчера очереди печати Windows.	8 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021060813 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675	Есть
24.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30559	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 в ANGLE	15 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071511 https://crbug.com/1228407 https://crbug.com/1219630 https://crbug.com/1221309 https://crbug.com/1219209 https://crbug.com/1214842 https://crbug.com/1220078 https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html https://crbug.com/1219082	Есть
25.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30541	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 в компоненте V8.	15 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071511 https://crbug.com/1228407 https://crbug.com/1219630 https://crbug.com/1221309 https://crbug.com/1219209 https://crbug.com/1214842 https://crbug.com/1220078 https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html https://crbug.com/1219082	Есть
26.	Выполнение произвольного	MITRE: CVE-2021-30560	Эксплуатация уязвимости позволяет удаленному	15 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071511	Есть

	кода в Google Chrome		злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения в компоненте Blink XSLT.		https://crbug.com/1228407 https://crbug.com/1219630 https://crbug.com/1221309 https://crbug.com/1219209 https://crbug.com/1214842 https://crbug.com/1220078 https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html https://crbug.com/1219082	
27.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30561	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.	15 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071511 https://crbug.com/1228407 https://crbug.com/1219630 https://crbug.com/1221309 https://crbug.com/1219209 https://crbug.com/1214842 https://crbug.com/1220078 https://chromereleases.googleblog.com/2021/07/stable-channel-update-for-desktop.html https://crbug.com/1219082	Есть
28.	Повышение привилегий в Microsoft Office	MITRE: CVE-2021-34469	Эксплуатация уязвимости позволяет удаленному злоумышленнику повысить свои привилегии в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной работой функции безопасности в Microsoft Office.	13 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071383 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34469	Есть
29.	Выполнение произвольного кода в Microsoft Defender	MITRE: CVE-2021-34522 CVE-2021-34464	Эксплуатация уязвимости позволяет локальному злоумышленнику выполнить произвольный код в целевой системе посредством запуска специально созданного вредоносного файла. Уязвимость обусловлена некорректной обработкой входных данных в Microsoft Defender	13 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071363 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34522 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34464	Есть
30.	Множественные уязвимости в маршрутизаторе D-LINK DIR-3040	MITRE: CVE-2021-21820	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена наличием жестко закодированных учетный данных в тестовой среде Libeli.	16 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021071610 https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1285 https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1283 https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1282 https://www.talosintelligence.com/vulnerability_reports/TALOS-2021-1284	Нет
31.	Повышение привилегий в Linux kernel	MITRE: CVE-2021-33909	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством размещения файла с именем превышающим определенную длину. Уязвимость обусловлена целочисленным переполнением буфера в функции vmalloc().	21 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021072106 https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4 https://github.com/torvalds/linux/commit/8cae8cd89f05f6de223d63e6d15e31c8ba9cf53b https://www.openwall.com/lists/oss-security/2021/07/20/1	Есть
32.	Повышение привилегий в Windows	MITRE: CVE-2021-36934	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику получить несанкционированный доступ к данным в целевой системе посредством использования данных из сохраненной теневой копии VSS. Уязвимость обусловлена некорректной настройкой прав доступа в Access Control Lists (ACLs).	21 июля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021072105 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934 https://www.kb.cert.org/vuls/id/506989	Нет
33.	Множественные уязвимости в Zabbix	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные SQL-команды	29 июля 2021 г.	https://packetstormsecurity.com/files/163657 https://www.cybersecurity-help.cz/vdb/SB2021072914	Нет

			посредством отправки специально сформированных запросов. Уязвимость обусловлена некорректной очисткой пользовательский данных в скрипте «hostinventoriesoverview.php».			
34.	Множественные уязвимости в Zabbix	Не определен	Эксплуатация уязвимости позволяет удаленному злоумышленнику обойти форму авторизации панели администратора посредством отправки специально сформированных запросов. Уязвимость обусловлена ошибкой в коде страницы авторизации. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-284: Некорректное управление доступом Рекомендации по устранению: ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами	29 июля 2021 г.	https://packetstormsecurity.com/files/163657 https://www.cybersecurity-help.cz/vdb/SB2021072914	Нет