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

«02» марта 2021г. **г. Махачкала**

.

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за февраль 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 «ПРОМСВЯЗЬ ИНВЕСТ» (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 номеру 8 (8722) 51-70-44.

ВРИО Председателя Правления **Исланов Р.О.**

подпись

М.П.

Исп. Ирганов Ю.Г.
Руководитель СИБ
8 (8722) 62-62-39

Приложение № 1
к информационному письму
«Информирование клиентов системы
дистанционного банковского
обслуживания «iBank2» о мерах
защиты за февраль 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.	Выполнение произвольного кода в VLC Media Player	MITRE: CVE-2020-26664	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного MKV-файла. Уязвимость обусловлена некорректной работой функции EbmlTypeDispatcher::send() при обработке файла в медиаплеере VideoLAN VLC.	8 января 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021012902 https://gist.githubusercontent.com/henices/db11664dd45b9f322f8514d182aef5ea/raw/d56940c8bf211992bf4f3309a85bb2b69383e511/CVE-2020-26664.txt	Есть
2.	Множественные уязвимости в продуктах компании Apple	MITRE: CVE-2020-29611	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного изображения. Уязвимость обусловлена ошибкой границ памяти при обработке изображений в компоненте ImageIO. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение.	27 января 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2020121518 https://www.cybersecurity-help.cz/vdb/SB2020121517 https://www.cybersecurity-help.cz/vdb/SB2021012728 https://support.apple.com/en-us/HT212003	Есть
3.	Множественные уязвимости в продуктах компании Apple	MITRE: CVE-2020-29618	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного изображения. Уязвимость обусловлена повреждением кучи при обработке изображений в компоненте ImageIO. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: обновить программное обеспечение.	27 января 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2020121518 https://www.cybersecurity-help.cz/vdb/SB2020121517 https://www.cybersecurity-help.cz/vdb/SB2021012728 https://support.apple.com/en-us/HT212003	Есть
4.	Множественные уязвимости в Cisco SD-WAN	MITRE: CVE-2021-1261	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированного вредоносных входных данных. Уязвимость обусловлена некорректной	20 января 2021 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	Есть

			обработкой вводимых пользователем команд для утилиты командной строки tcpdum. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H /A:H/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.			
5.	Множественные уязвимости в Cisco SD-WAN	MITRE: CVE-2021-1260	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных вредоносных входных данных. Уязвимость обусловлена некорректной обработкой вводимых пользователем данных в командной строке. CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H /A:N/E:U/RL:O/RC:C CWE-20: Некорректная проверка входных данных Рекомендации по устранению: обновить программное обеспечение.	20 января 2021 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn	Есть
6.	Выполнение произвольных команд в VMware vSphere Replication	MITRE: CVE-2021-21976	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированного вредоносного запроса со страницы "Startup Configuration". Уязвимость обусловлена некорректной обработкой входных данных.	11 февраля 2021 г.	https://www.vmware.com/security/advisories/VMSA-2021-0001.html https://www.cybersecurity-help.cz/vdb/SB2021021201	Есть
7.	Множественные уязвимости в Google Chrome и Microsoft Edge (Chromium-based)	MITRE: CVE-2021-21149 CVE-2021-21153 CVE-2021-21152 CVE-2021-21154 CVE-2021-21155 CVE-2021-21156	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена переполнением буфера при некорректной обработке входных данных в компонентах уязвимого приложения. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I: H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение. 8.8	18 февраля 2021 г.	https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_16.html https://www.cybersecurity-help.cz/vdb/SB2021021703 https://www.cybersecurity-help.cz/vdb/SB2021021808	Есть
8.	Выполнение произвольного кода в VMware vCenter Server	MITRE: CVE-2020-21972	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных сетевых пакетов на порт 443. Уязвимость обусловлена некорректным функционированием плагина для vROPs, входящего в стандартный комплект поставки.	23 февраля 2021 г.	https://www.vmware.com/security/advisories/VMSA-2021-0002.html	Есть
9.	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-21142	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия	3 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021020301 https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	Есть

			пользователем специально созданной веб-страницы. Уязвимость обусловлена ошибкой использования после освобождения памяти в компоненте Payments. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.			
10.	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-21143	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных в расширении браузера. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение.	3 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021020301 https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	Есть
11.	Множественные уязвимости в Google Chrome	MITRE: CVE-2021-21144	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной веб-страницы. Уязвимость обусловлена ошибкой границ памяти при обработке HTML-данных в компоненте Tab Groups. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение.	3 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021020301 https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html	Есть
12.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-21148	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ в памяти в движке V8 в Google Chrome.	4 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021020420 https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html https://crbug.com/1170176	Есть
13.	Множественные уязвимости в Microsoft Edge	MITRE: CVE-2021-21142	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента Payments. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	4 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021020420 https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html https://crbug.com/1170176	Есть
14.	Множественные уязвимости в	MITRE: CVE-2021-21143	Эксплуатация уязвимости позволяет удаленному	4 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021020420	Есть

	Microsoft Edge	CVE-2021-21144	злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированной веб-страницы. Уязвимость обусловлена некорректной обработкой HTML-контента. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение.		https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop_4.html https://crbug.com/1170176	
15.	Множественные уязвимости в Adobe Reader и Acrobat	MITRE: CVE-2021-21058 CVE-2021-21059 CVE-2021-21063 CVE-2021-21062 CVE-2021-21038 CVE-2021-21044 CVE-2021-21036	системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена переполнением буфера при некорректной обработке файла PDF. CVSSv3.1: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-119: Выполнение операций за пределами буфера памяти CWE-787: Запись за границами буфера CWE-190: Целочисленное переполнение или циклический возврат Рекомендации по устранению: обновить программное обеспечение.	10 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021021001	Есть
16.	Множественные уязвимости в Adobe Reader и Acrobat	MITRE: CVE-2021-21041 CVE-2021-21040 CVE-2021-21039 CVE-2021-21035 CVE-2021-21033 CVE-2021-21028 CVE-2021-21021	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена возможностью использования освободившейся памяти при некорректной обработке файлов PDF. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	10 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021021001	Есть
17.	Множественные уязвимости в Adobe Reader и Acrobat	MITRE: CVE-2021-21017	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена переполнением буфера при некорректной обработке файла PDF. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: обновить программное обеспечение.	10 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021021001	Есть
18.	Множественные уязвимости в Adobe Reader и Acrobat	MITRE: CVE-2021-21045	Эксплуатация уязвимости позволяет удалённому злоумышленнику получить НСД к целевой системе. Уязвимость обусловлена некорректными настройками ограничения доступа. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C CWE-284: Некорректное управление	10 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021021001	Есть

			доступом Рекомендации по устранению: обновить программное обеспечение.			
19.	Множественные уязвимости в Adobe Reader и Acrobat	MITRE: CVE-2021-21037	Эксплуатация уязвимости позволяет удалённому злоумышленнику перезаписать произвольные файлы в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF-файла. Уязвимость обусловлена некорректной обработкой абсолютного пути расположения PDF-файла. CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-22: Некорректные ограничения путей для каталогов (Выход за пределы каталога) Рекомендации по устранению: обновить программное обеспечение.	10 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021021001	Есть
20.	Выполнение произвольного кода в Adobe Illustrator	MITRE: CVE-2021-21053 CVE-2021-21054	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена переполнением буфера при некорректной обработке файлов Illustrator.	9 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021020972	Есть
21.	Выполнение произвольного кода в Adobe Photoshop	MITRE: CVE-2021-21051 CVE-2021-21048	Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного файла. Уязвимость обусловлена переполнением буфера при некорректной обработке файлов Photoshop.	9 февраля 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021020971	Есть
22.	Выполнение произвольного кода в расширении npm-script для Microsoft Visual Studio Code	MITRE: CVE-2020-26700	Эксплуатация уязвимости позволяет злоумышленнику выполнить произвольный код в целевой системе посредством клонирования пользователем специально сформированного вредоносного репозитория. Уязвимость обусловлена некорректной проверкой входных данных в расширении npm-script.	9 февраля 2021 г.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26700	Есть