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

«05» октября 2021г. **г. Махачкала**

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

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 сентябрь 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.	Угроза безопасности информации при эксплуатации уязвимости в Microsoft Exchange Server	CVE-2021-33766	Уязвимость позволяет удаленному злоумышленнику получить доступ к конфиденциальной информации в целевой системе посредством отправки специально сформированного вредоносного запроса к веб-сервису Exchange Control Panel (ECP). Уязвимость обусловлена небезопасной процедурой аутентификации на почтовом сервере через веб-службы Microsoft Exchange (Outlook Web Access, ECP). Указанная уязвимость актуальна только в случае установленного модуля ECP. Злоумышленник должен отправить запрос на авторизацию со специально сформированным файлом cookie и именем SecurityToken, данный запрос на аутентификацию будет делегирован от веб-сервисов к серверной части. Если со стороны серверной части не происходит загрузка модуля DelegatedAuthModule, то некоторые запросы будут пропущены без аутентификации. С подгруженным модулем DelegatedAuthModule на данный запрос от серверной части Microsoft Exchange вернется ответ с ошибкой HTTP 500, содержащий canary-токен ECP. Используя полученный canary-токен, злоумышленник может обойти процесс аутентификации и изменить некоторые параметры в конфигурации Microsoft Exchange Server, например, настроить правило для конкретного почтового адреса, осуществляющее пересылку всех входящих почтовых сообщений на контролируемый злоумышленником почтовый адрес.	3 сентября 2021 г.	https://nvd.nist.gov/vuln/detail/CVE-2021-33766 https://www.zerodayinitiative.com/blog/2021/8/30/proxytoken-an-authentication-bypass-in-microsoft-exchange-server https://www.zerodayinitiative.com/advisories/ZDI-21-798/ https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-33766	
2.	Выполнение произвольного кода в Microsoft Edge	MITRE: CVE-2021-30606 CVE-2021-30607 CVE-2021-30608 CVE-2021-30609 CVE-2021-	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой	2 сентября 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30624 https://www.cybersecurity-help.cz/vdb/SB2021090211	

		30610	использования после освобождения.			
3.	Выполнение произвольного кода в Microsoft Edge	MITRE: CVE-2021-30614	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти.	2 сентября 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30624 https://www.cybersecurity-help.cz/vdb/SB2021090211	
4.	Выполнение произвольного кода в Microsoft Edge	MITRE: CVE-2021-30615	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к конфиденциальной информации на целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной передачей внутренних данных службой Navigation.	2 сентября 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30624 https://www.cybersecurity-help.cz/vdb/SB2021090211	
5.	Выполнение произвольного кода в Microsoft Edge	MITRE: CVE-2021-30618	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к конфиденциальной информации на целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией инструментов разработчика.	2 сентября 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30624 https://www.cybersecurity-help.cz/vdb/SB2021090211	
6.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30625 CVE-2021-30629 CVE-2021-30633	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным обнулением указателей на освобожденные ячейки памяти в компонентах Google Chrome.	13 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091401 https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	
7.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30626 CVE-2021-30628	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой границ памяти в компоненте ANGLE Google Chrome.	13 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091401 https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	
8.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30627 CVE-2021-30631	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 браузерах на основе Blink.	13 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091401 https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	
9.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30630	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректной реализацией Blink.	13 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091401 https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	

10.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-30632	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 V8.	13 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091401 https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop.html	
11.	Выполнение произвольного кода в Apple iOS	MITRE: CVE-2021-30860	Уязвимость позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного вредоносного PDF файла. Уязвимость обусловлена целочисленным переполнением буфера памяти в библиотеке визуализации изображений CoreGraphics.	25 августа 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091321 https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/ https://support.apple.com/en-us/HT212807 https://support.apple.com/en-us/HT212805	
12.	Выполнение произвольного кода в Microsoft MSHTML	CVE-2021-40444	Эксплуатация уязвимости в Microsoft MSHTML позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного документа Microsoft Office. Уязвимость обусловлена некорректной проверкой входных данных в компоненте MSHTML. По имеющимся сведениям, злоумышленники начали активно использовать данную уязвимость в целевых компьютерных атаках при внедрении различного ВПО. В ходе таких атак ими используются методы социальной инженерии с целью убеждения пользователей открыть зараженный документ Microsoft Office, вследствие чего происходит эксплуатация указанной уязвимости и загрузка полезной нагрузки ВПО.	15 сентября 2021 г.	https://www.securitylab.ru/vulnerability/524175.php https://www.cybersecurity-help.cz/vdb/SB2021090712 https://www.trendmicro.com/en_us/research/21/i/remote-code-execution-zero-day--cve-2021-40444--hits-windows--tr.html?utm_source=trendmicroresearch&utm_medium=smk&utm_campaign=0821_CVE0DAy https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40444	
13.	Выполнение произвольного кода в Adobe Premiere Elements	MITRE: CVE-2021-39824	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	15 сентября 2021 г.	https://helpx.adobe.com/security/products/premiere_elements/apsb21-78.html https://www.cybersecurity-help.cz/vdb/SB2021091505	
14.	Выполнение произвольного кода в Adobe Premiere Elements	MITRE: CVE-2021-40700	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	15 сентября 2021 г.	https://helpx.adobe.com/security/products/premiere_elements/apsb21-78.html https://www.cybersecurity-help.cz/vdb/SB2021091505	
15.	Выполнение произвольного кода в Adobe Premiere Elements	MITRE: CVE-2021-40703	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	15 сентября 2021 г.	https://helpx.adobe.com/security/products/premiere_elements/apsb21-78.html https://www.cybersecurity-help.cz/vdb/SB2021091505	
16.	Выполнение произвольного кода в Adobe Premiere Elements	MITRE: CVE-2021-40702	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия	15 сентября 2021 г.	https://helpx.adobe.com/security/products/premiere_elements/apsb21-78.html https://www.cybersecurity-help.cz/vdb/SB2021091505	

			пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.			
17.	Выполнение произвольного кода в Photoshop Elements	MITRE: CVE-2021-39825	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	15 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091504 https://helpx.adobe.com/security/products/photoshop_elements/apsb21-77.html	
18.	Выполнение произвольного кода в Adobe Photoshop	MITRE: CVE-2021-40709	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	15 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091501 https://helpx.adobe.com/security/products/photoshop/apsb21-84.html	
19.	Выполнение произвольного кода в Adobe Premiere Pro	MITRE: CVE-2021-40710	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	15 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091507 https://helpx.adobe.com/security/products/premiere_pro/apsb21-67.html	
20.	Выполнение произвольного кода в Microsoft Windows	MITRE: CVE-2021-26435	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена ошибкой границ памяти.	14 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091432 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26435	
21.	Множественные уязвимости в Apache HTTP Server	MITRE: CVE-2021-36160	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании в целевой системе посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной обработкой входных данных.	17 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091706	
22.	Множественные уязвимости в Apache HTTP Server	MITRE: CVE-2021-40438	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к данным в локальной сети посредством отправки специально сформированного HTTP-запроса. Уязвимость обусловлена некорректной проверкой входящих данных.	17 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091706	
23.	Выполнение произвольного кода в Microsft Visual Studio	MITRE: CVE-2021-36952	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена некорректным управлением генерирования кода.	14 сентября 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36952 https://www.cybersecurity-help.cz/vdb/SB2021091446 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26434	
24.	Выполнение произвольного кода в Microsft Visual Studio	MITRE: CVE-2021-26434	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена	14 сентября 2021 г.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36952 https://www.cybersecurity-help.cz/vdb/SB2021091446 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26434	

			некорректным управлением доступа.			
25.	Выполнение произвольного кода в Microsoft Office	MITRE: CVE-2021-38646	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена некорректным управлением генерирования кода.	14 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021091445 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38646	
26.	Выполнение произвольного кода в Microsoft Excel	MITRE: CVE-2021-38660	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного запроса. Уязвимость обусловлена некорректной проверки ввода в Microsoft Office Graphics.	14 сентября 2021 г	https://www.cybersecurity-help.cz/vdb/SB2021091423 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38660	
27.	Выполнение произвольного кода в Adobe Adobe Acrobat DC, Adobe Acrobat, Adobe Acrobat Reader DC, Adobe Reader	MITRE: CVE-2021-35982	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена некорректной загрузкой DLL-библиотек.	14 сентября 2021 г.	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html https://www.cybersecurity-help.cz/vdb/SB2021091436	
28.	Выполнение произвольного кода в Adobe Adobe Acrobat DC, Adobe Acrobat, Adobe Acrobat Reader DC, Adobe Reader	MITRE: CVE-2021-35982 MITRE: CVE-2021-39845 CVE-2021-39846	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена ошибкой границ памяти.	14 сентября 2021 г.	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html https://www.cybersecurity-help.cz/vdb/SB2021091436	
29.	Выполнение произвольного кода в Adobe Adobe Acrobat DC, Adobe Acrobat, Adobe Acrobat Reader DC, Adobe Reader	MITRE: CVE-2021-35982 MITRE: CVE-2021-39843	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированного файла. Уязвимость обусловлена ошибкой границ памяти.	14 сентября 2021 г.	https://helpx.adobe.com/security/products/acrobat/apsb21-55.html https://www.cybersecurity-help.cz/vdb/SB2021091436	
30.	Угроза раскрытия учетных данных пользователей при использовании службы Autodiscover в Microsoft Exchange Server	ALRT-20210924.1	Служба Autodiscover в Microsoft Exchange Server предназначена для упрощения процесса настройки почтовых клиентов и последующего подключения пользователей организации к функциям Exchange. Использование указанной выше службы позволяет пользователю получить доступ к функциям Exchange посредством ввода адреса электронной почты и пароля без необходимости дополнительных настроек. В рамках этого почтовый клиент попытается пройти аутентификацию по различным URL-адресам службы Autodiscover и получить необходимые настройки. При работе указанного механизма службе Autodiscover автоматически будут переданы учетные данные пользователя. URL-адреса формируются почтовым клиентом автоматически, исходя из введенного адреса электронной почты. Примером этого служит:	24 сентября 2021 г.	https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-autodiscover-bugs-leak-100k-windows-credentials/	

			Адрес электронной почты – user@example.ru			
31.	Выполнение произвольного кода в VMware vCenter Server	Выполнение произвольного кода в VMware vCenter Server	Эксплуатация уязвимости в VMware vCenter Server позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных запросов на порт 443/TCP. Уязвимость обусловлена некорректной проверкой файла во время загрузки в сервисе Analytics. Отмечаем, что наличие средств эксплуатации указанной уязвимости не подтверждено, но тем не менее, в настоящее время злоумышленники активно осуществляют поиск хостов, подверженных указанной уязвимости, что в свою очередь в будущем может привести к массовым компьютерным атакам на виртуальные инфраструктуры с целью последующего получения несанкционированного доступа.	24 сентября 2021 г.	https://kb.vmware.com/s/article/85717 https://www.tenable.com/blog/cve-2021-22005-critical-file-upload-vulnerability-in-vmware-vcenter-server https://www.cybersecurity-help.cz/vdb/SB2021092117	
32.	Множественные уязвимости Apple iOS	MITRE: CVE-2021-30860	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально сформированных вредоносных файлов PDF. Уязвимость обусловлена целочисленным переполнением в компоненте CoreGraphics.	25 августа 2021 г.	https://support.apple.com/en-us/HT212807 https://www.cybersecurity-help.cz/vdb/SB2021092317 https://support.apple.com/en-us/HT212825 https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits	
33.	Выполнение произвольного кода в Google Chrome	MITRE: CVE-2021-37973	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 при обработке HTML-данных в компоненте Portals.	24 сентября 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021092428 https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_24.html https://crbug.com/1251727 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37973	