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

«02» декабря 2020г. **г. Махачкала**

«Информирование клиентов системы дистанционного банковского обслуживания «iBank2» о мерах защиты за ноябрь 2020 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.

Председатель Правления _____ **Абдурахманов К.А.**
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 ноябрь 2020 г.»

По информации **ФИНЦЕРТ (центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, специального структурного подразделения Банка России)** участились случаи распространения вредоносного программного обеспечения семейства «RTM», ориентированного на клиентов кредитно-финансовых организаций, являющихся юридическими лицами и индивидуальными предпринимателями.

URL-адреса и IP-адреса, рекомендуемые к блокировке it-специалистами организаций и индивидуальных предпринимателей через сетевые экраны, брандмауэры, сетевое оборудование	**wsus.ga** **gsv2@fabrikant.ru** **exch.strata.ru** **212.44.151.58** **hxxp://risu.fi/J9.jpg** **med-star.gr** **144.91.112.76:21** **159.89.225.77** **161.35.110.203** **77.208.157.70** **172.86.75.89**

При работе с электронной почтой организациям и индивидуальным предпринимателям следует учитывать, что участились случаи отправки по электронной почте ложных писем от мошенников. Целью данных писем является распространение вредоносного кода с целью кражи денежных средств. Подобные письма содержат файлы со следующими именами:

Документы.rar
Акт сверки бн за период 01.07.2020 по 15.11.2020.exe
19.11.2020 Получение перевода.chm
J9.jpg
Paket dokumentov dlya oplaty za oktyabn'.exe
Dokumenty, sverka za ves' oktyabr'.exe
Dok-ty za proshlyj mesyac.exe

При обнаружении во входящих письмах своей электронной почты писем с файлами с подобными именами не рекомендуется открывать такие файлы и такие письма.

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 Cisco Webex Meeting Desktop App для ОС Windows	MITRE: CVE-2020-3588	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки вредоносных сообщений приложению, используя интерфейс канала виртуализации. Уязвимость обусловлена некорректной проверкой входных данных.	4 ноября 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-vdi-qQrpBwuJ	Есть
2.	Отказ в обслуживании в Cisco IP Phone	MITRE: CVE-2020-3574	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированных TCP-пакетов. Уязвимость обусловлена некорректной обработкой TCP-пакетов.	4 ноября 2020 г.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voip-phone-flood-dos-YnU9EXOv	Есть
3.	Выполнение произвольного кода в ядре Linux	MITRE: CVE-2020-25669	Эксплуатация уязвимости позволяет локальному злоумышленнику вызвать отказ в обслуживании или выполнить произвольный код в целевой системе посредством запуска специально созданной программы. Уязвимость обусловлена некорректной работой функции sunkbd_reinit в файле drivers/input/keyboard/sunkbd.c.	5 ноября 2020 г.	https://www.openwall.com/lists/oss-security/2020/11/05/2 https://exchange.xforce.ibmcloud.com/vulnerabilities/191229	Есть
4.	Множественные уязвимости в продуктах компании Adobe	MITRE: CVE-2020-24435	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена поддержкой встроенного JavaScript кода в PDF-файлах. 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.	5 ноября 2020 г.	https://helpx.adobe.com/security/products/acrobat/apsb20-67.html https://talosintelligence.com/vulnerability_reports/TALOS-2020-1157 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1156	Есть
5.	Выполнение произвольного кода в Microsoft Excel	MITRE: CVE-2020-17064 CVE-2020-17065 CVE-2020-17066 CVE-2020-17019	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных 10 ноября 2020 г.	10 ноября 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020111054	Есть
6.	Выполнение произвольного кода в Visual Studio Code JSHint Extension	MITRE: CVE-2020-17104	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного файла. Уязвимость обусловлена некорректной проверкой входных данных.	10 ноября 2020 г.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17104	Есть
7.	Удаленное выполнение кода в Mozilla	MITRE: CVE-2020-26950	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить	9 ноября 2020 г.	https://www.cybersecurity-help.cz/vdb/SB2020110949 https://www.mozilla.org/en-	Есть

	Thunderbird, Mozilla Firefox и Firefox ESR		произвольный код в целевой системе посредством открытия пользователем специально сформированной вредоносной веб-страницы. Уязвимость обусловлена возможностью использования освободившейся памяти после выполнения операции MCallGetProperty.		US/security/advisories/mfsa2020-49/	
8.	Выполнение произвольного кода в Juniper OC Junos	MITRE: CVE-2020-1679	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы посредством отправки специально сформированного сетевого пакета. Уязвимость обусловлена некорректной обработкой сетевых пакетов.	14 октября 2020 г.	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11076&actp=METADATA	Есть
9.	Обход механизма DNS-фильтрации в Juniper OC Junos	MITRE: CVE-2020-1660	Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании сервиса Multiservices PIC Management (mspmand) и обойти механизм фильтрации DNS-пакетов целевой системы посредством отправки специально сформированных DNS-пакетов. Уязвимость обусловлена использованием общих ресурсов службой mspmand и службой DNS-фильтрации.	16 октября 2020 г.	https://kb.juniper.net/JSA11054 https://nvd.nist.gov/vuln/detail/CVE-2020-1660	Есть
10.	Выполнение произвольного кода в пакете netkit-telnet для протокола telnet	MITRE: CVE-2020-10188	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной работой компонента «utility.c».	6 марта 2020 г.	https://nvd.nist.gov/vuln/detail/CVE-2020-10188	Есть
11.	Множественные уязвимости в Mozilla Thunderbird и Mozilla Firefox	MITRE: CVE-2020-26951	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством использования XSS-уязвимости. Уязвимость обусловлена несоответствием синтаксического анализа и загрузки событий в коде SVG Firefox. CVSSv3.0: AV:N/AC:H/PR:N/UI:R/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	17 ноября 2020 г.	-	Есть
		MITRE: CVE-2020-26959	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой использования памяти после освобождения в компоненте WebRequestService во время завершения работы.	17 ноября 2020 г.	-	Есть
		MITRE: CVE-2020-26960	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена ошибкой	17 ноября 2020 г.	-	Есть

			использования памяти после освобождения в массиве данных nsTArray.			
		MITRE: CVE-2020-15999	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного TTF-файла. Уязвимость обусловлена ошибкой границ памяти в библиотеке freetype при обработке файлов.	17 ноября 2020 г.	-	Есть
		MITRE: CVE-2020-26968	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.	17 ноября 2020 г.	-	Есть
12.	Удаленное выполнение кода в Oracle WebLogic Server	MITRE: CVE-2020-14750	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе путем отправки специально сформированных сетевых пакетов. Уязвимость обусловлена некорректной проверкой входных данных.	1 ноября 2020 г.	-	Есть
	Множественные уязвимости в Google Chrome	MITRE: N/A	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке HTML-содержимого.	3 ноября 2020 г.	-	
		MITRE: CVE-2020-16004	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента интерфейса пользователя.	3 ноября 2020 г.	-	
		MITRE: CVE-2020-16005	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным применением политик безопасности в компоненте ANGLE.	3 ноября 2020 г.	-	
		MITRE: CVE-2020-16006	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента	3 ноября 2020 г.	-	

			V8.			
		MITRE: CVE-2020-16008	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке HTML-содержимого компонентом WebRTC.	3 ноября 2020 г.	-	
		MITRE: CVE-2020-16009	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным функционированием компонента V8.	3 ноября 2020 г.	-	
		MITRE: CVE-2020-16011	Эксплуатация уязвимости позволяет удаленному злоумышленнику получить НСД к целевой системе посредством открытия пользователем специально созданной вредоносной веб-страницы. Уязвимость обусловлена некорректным определением границ буфера памяти при обработке HTML-содержимого компонентом интерфейса пользователя в версии для Windows.	3 ноября 2020 г.	-	