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

«01» июня 2021г. **г. Махачкала**

.

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

Зам. Председателя Правления подпись **Исланов Р.О.**

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 май 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.	Множественные уязвимости в Adobe Reader и Acrobat	MITRE: CVE-2021-28550	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена некорректным обнулением указателей на ячейки памяти. CVSSv3.1: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C CWE-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	11 мая 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021051143 https://helpx.adobe.com/security/products/acrobat/apsb21-29.html	Есть
2.	Множественные уязвимости в Adobe Reader и Acrobat	MITRE: CVE-2021-28562 CVE-2021-28553	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена некорректным обнулением указателей на ячейки памяти. 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-416: Использование после освобождения Рекомендации по устранению: обновить программное обеспечение.	11 мая 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021051143 https://helpx.adobe.com/security/products/acrobat/apsb21-29.html	Есть
3.	Множественные уязвимости в Adobe Reader и Acrobat	MITRE: CVE-2021-28561 CVE-2021-28560 CVE-2021-28558 CVE-2021-28557 CVE-2021-28565 CVE-2021-28564	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством открытия пользователем специально созданного вредоносного PDF-файла. Уязвимость обусловлена некорректным определением границ буфера памяти. 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-122: Переполнение буфера в динамической памяти CWE-125: Чтение за пределами буфера CWE-787: Запись за границами буфера Рекомендации по устранению: обновить программное обеспечение.	11 мая 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021051143 https://helpx.adobe.com/security/products/acrobat/apsb21-29.html	Есть

4.	Об угрозах безопасности информации, вызванных некорректными парольными политиками	-	По каналам НКЦКИ получены сведения об у частившихся случаях компрометации информационных ресурсов государственных и коммерческих организаций. Анализ инцидентов показывает , что распространенной причиной получения злоумышленником несанкционированного доступа является использование пользователями с лабых паролей, а также одинаковых паролей для доступа к корпоративным и личным ресурсам Исходя из указанного выше рекомендуем разработать и внедрить в ваших организациях парольные политики при работе с корпоративными сервисами. А также обратить внимание пользователей на недопустимость использования одинаковых паролей к корпоративным и личным информационным ресурсам. До утверждения парольной политики рекомендуем реализовать набор следующих первоочередных мер		Рекомендации по нейтрализации угрозы: Организовать смену паролей не реже одного раза в 180 дней. • Блокировать пользователей после 10 неудачных попыток входа не менее чем на 5 минут. • Не использовать в качестве пароля имя учетной записи или часть полного имени пользователя длин ой более двух рядом стоящих символов. • Длина пароля должн а быть не менее 9 символов. • Пароль должен включать в себя символ ы из всех следующих наборов - латинские заглавные буквы (от A до Z); - латинские строчные буквы (от a до z); - цифры (от 0 до - специальные символы (например: !, $, #, %). • Не публиковать сведения, позволяющие идентифицировать связь корпоративных и личных информационные ресурсов. • Использовать уникальные пароли для каждой учетной записи. • По возможности использовать двухфакторную аутентификацию.	Есть
5.	Выполнение произвольного кода в Cisco Small Business 100 Series Wireless Access Points	MITRE: CVE-2021-1401	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных HTTP-запросов в веб-интерфейс управления маршрутизатора. Уязвимость обусловлена некорректной проверкой вводимых данных.	6 мая 2021 г.	https://www.cybersecurity-help.cz/vdb/SB2021050631 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-multi-ZAfKGXhF	Есть