НАЦІОНАЛЬНИЙ БАНК УКРАЇНИ

вул. Інститутська, 9, м. Київ, 01601, Україна
телефон: 0-800-505-240
+380 (50) 462-00-90
e-mail: nbu@bank.gov.ua
web: https://bank.gov.ua
Код ЄДРПОУ 00032106

NATIONAL BANK OF UKRAINE

9, Instytutska St., Kyiv, 01601, Ukraine
phone: +380 (44) 298-65-55
+380 (50) 462-00-90,
e-mail: nbu@bank.gov.ua
web: https://bank.gov.ua

Надавачам небанківських фінансових послуг та їх об'єднанням (за списком)

Про використання програмного забезпечення

Національний банк України (далі – Національний банк) у межах здійснення державного регулювання та нагляду на ринках небанківських фінансових послуг вживає заходів щодо досягнення цілей, визначених Стратегією розвитку фінансового сектору[1], яка, зокрема, передбачає запровадження нульової толерантності до російського та білоруського програмного забезпечення на фінансовому ринку України.

Для досягнення зазначеної цілі Національний банк у минулому році надсилав учасникам ринку небанківських фінансових послуг (далі – НФП) лист від 22.01.2024 № 21-0006/5283 (далі – Лист), який містив рекомендації щодо першочергових кроків, які пропонувалося вжити для забезпечення інформаційної безпеки, а саме:

проаналізувати усі програмні продукти, їх складові, які використовуються в діяльності учасників ринку НФП щодо причетності до їх розроблення, супроводження та розповсюдження осіб, пов'язаних із російською федерацією та/або республікою білорусь;

здійснити розподіл програмного забезпечення, яке має зв'язки з російською федерацією та/або республікою білорусь, на критичне та некритичне;

здійснити аналіз наявності аналогів вищезазначеного програмного забезпечення та оцінку можливих строків і витрат для його заміни тощо.

Крім того, Національний банк за результатами аналізу інформації, отриманої від учасників ринку НФП (опитувальник щодо використання програмного забезпечення), встановив, що НФП використовують у своїй діяльності програмне забезпечення, розробником / власником якого є суб'єкти,

[1] https://bank.gov.ua/admin_uploads/article/Strategy_finsector_NBU.pdf?v=5.

що є резидентами російської федерації та/або республіки білорусь, та/або щодо яких застосовані санкції Україною або її міжнародними партнерами.

Як зазначалось у Листі, використання НФП у своїй діяльності програмного забезпечення, яке має російське / білоруське походження, може мати суттєві ризики, зокрема:

отримання спецслужбами російської федерації / республіки білорусь несанкціонованого доступу до персональних даних клієнтів та інформації щодо їх фінансової поведінки;

несанкціонованої модифікації або знищення даних; порушення безперервності надання фінансових послуг;

неотримання належної технічної підтримки програмного забезпечення або критичних оновлень;

подальшої прив'язки до виключно російських / білоруських програмних продуктів та неможливості чи суттєвого ускладнення міграції на програмні продукти інших виробників.

На сьогодні з метою мінімізації ризиків, пов'язаних із використанням програмного забезпечення, яке має російське / білоруське походження, та забезпечення інформаційної безпеки НФП Національний банк розробив проєкт постанови Правління Національного банку України "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг"[2] (далі – Проєкт), в якому передбачено, що:

1) надавач фінансових послуг зобов'язаний вживати заходів із забезпечення інформаційної безпеки та кіберзахисту на всіх стадіях життєвого циклу інформаційно-комунікаційних систем надавача фінансових послуг (пункт 6);

2) надавач фінансових послуг зобов'язаний запровадити, використовуючи ризик-орієнтовний підхід, заходи із забезпечення інформаційної безпеки та кіберзахисту з урахуванням особливостей функціонування інформаційно-комунікаційних систем надавача фінансових послуг (пункт 10).

Наразі здійснюється доопрацювання Проєкту за результатами публічного обговорення.

Водночас на рівні держави вживаються заходи, спрямовані на посилення захисту державних інформаційних ресурсів та убезпечення інформаційно-комунікаційних систем країни від кіберзагроз. Так, Указом Президента України від 02.09.2024 № 601/2024 уведено в дію рішення Ради національної безпеки і оборони України від 02.09.2024 "Про застосування, скасування та внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", зокрема:

до Товариства з обмеженою відповідальністю "1С" (Общество с ограниченной ответственностью "1С", Limited Liability Company "1С") застосовано, у тому числі, вид обмежувального заходу як інші санкції, що

[2] https://bank.gov.ua/admin_uploads/article/proekt_2025-03-10.pdf.

відповідають принципам їх застосування, встановлених Законом України “Про санкції” (заборона здійснення державних закупівель товарів, послуг, робіт та використання державними підприємствами, установами і організаціями України програмних продуктів “1С: Бухгалтерія 8 для України”, “1С: Бухгалтерія 8 для України Базова”, “1С: Бухгалтерія 8 для України. Учбова версія”, “1С: Підприємство 8. Торгівля для приватних підприємців України”, “1С: Підприємство 8. Комплексний облік для бюджетних установ України”, “1С: Підприємство 8. Комплексний облік для бюджетних установ України Базова”, “1С: Підприємство 8. Управління торгівлею для України”, “1С: Підприємство 8. Управління невеликою фірмою для України”, “1С: Підприємство 8. Зарплата і Управління Персоналом для України”, “1С: Підприємство 8. Зарплата і Управління Персоналом для України Базова”, “1С: Підприємство 8. Управління торговим підприємством для України” (“1С: Управління торговим підприємством 8, 1С: УТП8”), “1С: Підприємство 8. Бухгалтерія для бюджетних установ України” (“1Сбухгалтерія 8 для бюджетних установ”), “1С: Підприємство 8. Зарплата та кадри для бюджетних установ України” (“1С: Зарплата та кадри для бюджетних установ України”), “1С: Підприємство 8. Управління виробничим підприємством для України”, “1С: Підприємство 8. Документообіг КОРП для України”, “1С: Підприємство 7.7. Бухгалтерський облік для України” (1С:Бухгалтерія 7.7.), “1С: Торгівля і Склад 7.7. для України”, “1С: Зарплата і Кадри 7.7. для України”, “1С: Підприємство 7.7. Комплексна поставка для України”, “1С: Підприємство 7.7. Виробництво + Послуги + Бухгалтерія для України”, “BAS ERP”, “BAS Управління холдингом”, “BAS Документообіг КОРП”, “BAS Управління торгівлею”, “BAS Роздрібна торгівля”, “BAS Бухгалтерія КОРП” та інших програмних продуктів “BAS”, “UA-Бюджет”).

Крім того, Кабінетом Міністрів України внесено до Верховної Ради України проєкт Закону України “Про внесення змін до Закону України “Про санкції” щодо заборони використання програмних продуктів та доступу до електронних інформаційних ресурсів[3] (реєстр. № 11492), що передбачає розширення виду санкцій забороною поширення та використання на території України юридичними особами програмних продуктів, їх складових походженням з іноземної держави, до якої застосовано санкції згідно з Законом про санкції, або розробником чи суб’єктом авторського права яких є юридична (фізична) особа – резидент такої іноземної держави або юридична особа, частка у статутному капіталі якої перебуває у власності такої іноземної держави, або юридична особа, яка перебуває під контролем іноземної юридичної особи чи фізичної особи – нерезидента, іноземців, осіб без громадянства, а також суб’єктів, які здійснюють терористичну діяльність, або програмних продуктів, їх складових, розробниками чи суб’єктом авторського права яких є іноземні юридичні чи фізичні особи, до яких застосовано санкції згідно з Законом України

[3] https://itd.rada.gov.ua/billinfo/Bills/Card/44743

“Про санкції”, а також програмних продуктів, створених із використанням вихідного або об’єктного коду програмних продуктів, їх складових, на які поширюються зазначені санкції.

Водночас 27.03.2025 Верховною Радою України прийнято в цілому проєкт Закону України “Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури” (реєстр. № 11290) (далі – законопроєкт № 11290), спрямований на посилення захисту державних інформаційних ресурсів та об’єктів критичної інформаційної інфраструктури, гармонізацію українських стандартів кібербезпеки з європейськими та підвищення рівня захисту інформаційних ресурсів держави. Зокрема, законопроєкт № 11290 передбачає доповнення статті 4 Закону України “Про основні засади забезпечення кібербезпеки України” частиною четвертою такого змісту: “4. Обов’язковою умовою використання програмного забезпечення та комунікаційного (мережевого) обладнання в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також на об’єктах критичної інформаційної інфраструктури є відсутність таких продуктів та обладнання у відкритому переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання. Порядок формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання затверджується Кабінетом Міністрів України. Повноваження щодо забезпечення формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання покладаються на Державну службу спеціального зв’язку та захисту інформації України.”.

З огляду на вищезазначене, а також із метою мінімізації кіберризиків, пов’язаних із використанням програмних продуктів, які мають / можуть мати російське / білоруське походження, зважаючи на можливу заборону на рівні держави використання програмного забезпечення, яке має / може мати російське / білоруське походження, **Національний банк звертає увагу на необхідність вжиття заходів та виконання рекомендацій, наданих Національним банком учасникам ринку небанківських фінансових послуг листом від 22.01.2024 № 21-0006/5283**.

Додаток: на 2 арк.

Заступник Голови Дмитро ОЛІЙНИК

Саченок Вадим
vadym.sachenok@bank.gov.ua

Додаток

Рекомендації з мінімізації кіберризиків, пов’язаних із використанням програмних продуктів

1. Закрити доступ до продуктивного середовища постачальникам програмних продуктів країни-агресора.

2. Виключити автоматичні онлайн-оновлення програмних продуктів країни-агресора.

3. Не використовувати оновлення програмних продуктів країни-агресора з виконуваних файлів.

4. Визначити права, з якими запускаються процеси програмних продуктів країни-агресора (процеси не повинні запускатися з адміністративними правами).

5. Визначити всі зовнішні програмні інтерфейси програмних продуктів країни-агресора, їх призначення, адресатів взаємодії, процеси, які їх використовують.

6. Налаштувати політику фаєрволів на заборону для процесів програмних продуктів країни-агресора всіх взаємодій, крім потрібних за технологічним процесом, визначених документацією, та довірених систем і ресурсів.

7. На серверах розгортання програмних продуктів країни-агресора налаштувати політику локальних брандмауерів та політику керування процесами в системному середовищі відповідно до рекомендацій CIS (Center for Internet security, Inc.) для профілю захисту рівня 2.

8. Налаштувати політику централізованого аудиту подій на серверах розгортання програмних продуктів країни-агресора та постійного моніторингу інцидентів безпеки.

9. Розробити план реагування на інциденти безпеки, пов’язані з несанкціонованими діями в межах програмних продуктів країни-агресора та зовнішніми кіберзагрозами.

10. Вивести сервери з розгорнутими програмними продуктами країни-агресора зі складу домену НФП або сегментувати доменну структуру (створити для ресурсів піддомен).

11. На мережевому рівні максимально (наскільки можливо) ізолювати ресурси з програмними продуктами країни-агресора від інших ресурсів НФП.

12. Передбачити (за потреби) механізми оперативного блокування ресурсів та сегментів розгортання програмних продуктів країни-агресора від іншої структури мережі НФП.

13. Уключити механізми симетричного шифрування (SSL/TLS) між усіма компонентами програмних продуктів країни-агресора (у тому числі розміщених у межах одного захищеного середовища та одного обчислювального ресурсу).

14. Не використовувати криптографічних засобів, розроблених у складі програмних продуктів країни-агресора. Для шифрування доцільно застосовувати

засоби в складі стандартного прикладного та системного програмного забезпечення від довірених вендорів.

15. Налаштувати механізми контролю цілісності (засобами ОС або інших довірених вендорів) для виконуваних файлів, бібліотек та скриптів програмних продуктів країни-агресора.

16. Налаштувати політику регулярного сканування файлів на віруси засобами, які підтримують аналіз на основі поведінки.