NETWORK AND APPLICATION SECURITY

DOI 10.20535/2411-1031.2024.12.1.306259
УДК 004.054

ОЛЬГА ШЕВЧУК,
АРТЕМ ЖИЛІН,
АРТЕМ МИКИТЮК,
АНАТОЛІЙ МІНОЧКІН

НАПРЯМКИ ПІДСИЛЕННЯ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ЩО ОБРОБЛЯЄ ДЕРЖАВНІ ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ ТА ВИКОРИСТОВУЄТЬСЯ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У сучасному світі, де все більше аспектів нашого життя стають залежними від комп'ютерних систем та мереж, питання кібербезпеки стає все більш гострим. Одним з ключових елементів кібербезпеки є захист програмного забезпечення, яке використовується в цих системах. Програмне забезпечення може містити вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до систем, даних та ресурсів. Ці вразливості можуть бути викликані помилками в коді, неправильною конфігурацією або неналежним оновленням програмного забезпечення. Зловмисники постійно вдосконалюють свої методи та тактики, щоб не тільки використовувати вразливості програмного забезпечення але й впливати на їх появу, шляхом проведення атак на ланцюг постачальника. Це робить кіберзахист програмного забезпечення все більш складним завданням. У статті розглянуто актуальну проблему забезпечення кібербезпеки у контексті поширення кібератак на програмне забезпечення, включаючи атаки на ланцюг постачання. Наведено приклади відомих кібератак, які націлені на ланцюг постачальника. Зазначено недоліки в існуючій системі стандартів та правил для безпечної розробки програмного забезпечення, а також відсутність вимог безпеки та управління вразливостями. Запропоновано комплексний підхід до забезпечення безпеки програмного забезпечення, який включає розроблення відповідних вимог, стандартів та механізмів контролю.

Ключові слова: кібербезпека, програмне забезпечення, безпека програмного забезпечення, ланцюг постачання, атака на ланцюг постачання

Постановка проблеми. В сучасну епоху, яка характеризується активною цифровізацією усіх сфер життя, підтримання високого рівня кібербезпеки стає все більш важливим, ніж будь-коли раніше. Особливу увагу в цьому процесі привертає кіберзахист програмного забезпечення, яке зазвичай містить велику кількість потенційних вразливостей, що можуть бути використані зловмисниками. Від прикладних програм, системного програмного забезпечення до програмного забезпечення АСУ ТП та веб-сайтів – жоден аспект не залишається поза увагою кіберзлочинців, які, в свою чергу, вдосконалюють та поширюють атаки не лише на готове програмне забезпечення, а й намагаються компрометувати ланцюг постачання, тим самим розширюючи ландшафт атаки.

Наведемо приклади таких кібератак:

1. **Атака на глобальну клієнтську базу Kaseya.** Атака, що сталася в 2021 році, завдала шкоди сотням американських компаній, які користувалися послугами фірми Kaseya. Фірма Kaseya надає програмне забезпечення для управління і моніторингу комп'ютерних систем, серверів, мереж, робочих станцій та інших елементів IT-інфраструктури, та обслуговує внутрішні комп'ютерні мережі багатьох компаній. Зловмисники змогли впровадити шкідливий код через вразливість в програмному забезпеченні фірми Kaseya. Тобто вони реалізували атаку на ланцюг постачання програмного забезпечення. [1]–[2].

2. **Атака на Colonial Pipeline**. Colonial Pipeline стала жертвою атаки програми-вимагача у травні 2021 року. В результаті атаки були заражені деякі інформаційні системи трубопроводу, вимкнувши його на кілька днів. Під час атаки було використано недоліки в системі безпеки інформаційно-комунікаційних систем трубопроводу Colonial Pipeline і завдяки цьому завантажено в них програму-вимагач [3]. Атака використовувала наявну вразливість віддаленого виконання коду (RCE) у PulseConnect Secure (програмне забезпечення віддаленого захищеного доступу – VPN), яке Colonial Pipeline використовує для моніторингу дій конвеєру. Зловмисники змогли отримати доступ до мережі Colonial Pipeline і зашифрувати її системи [4].

3. **Атака на SolarWinds ("Sunburst" або "Solorigate").** SolarWinds – велика компанія-розробник програмного забезпечення, яка надає інструменти для моніторингу й управління мережею та інфраструктурою, а також інші технічні послуги для сотень тисяч організацій по всьому світу. У результаті кібератаки зловмисниками було скомпрометовано мережі та системи, отримано доступ до даних клієнтів. Компрометація відбулася в наслідок впровадження зловмисниками шкідливого програмного забезпечення в оновлення програмного забезпечення Orion [5]–[7].

4. **Атака на ланцюг постачання Norton.** Norton – це всесвітньо відома компанія поставник антивірусного програмного забезпеченням. При здійсненні на неї кібератаки зловмисники використовували вразливість нульового дня в програмному забезпеченні для управління передачею файлів MOVEit Transfer (MFT), яке компанія Norton використовує для передачі файлів між своїми офісами та клієнтами. В наслідок цього зловмисники змогли отримати доступ до мережі Norton і викрасти особисту інформацію співробітників, включаючи імена, адреси, дати народження та адреси корпоративної електронної пошти. Зловмисники також погрожували оприлюднити викрадені дані [4].

5. **Microsoft Supply Chain Attack**. Атака використовувала вразливість у Jfrog Artifactory, менеджері двійкових репозиторіїв, який Microsoft використовує для зберігання та розповсюдження своїх програмних компонентів. Зловмисникам вдалося отримати доступ до Jfrog Artifactory та впровадити шкідливий код у деякі програмні компоненти Microsoft. Це дозволило зловмисникам отримати доступ до мереж Microsoft і вкрасти вихідний код та іншу конфіденційну інформацію [4].

Представлені вище приклади доводять наявність високих ризиків втручання в процес розробки програмного забезпечення як зловмисників так і представників ворожих держав, зокрема і в програмне забезпечення, що вільно розповсюджується. Зазначене, а також відсутність вимог, правил та рекомендацій для розробки безпечного програмного забезпечення та вимог обов’язковості їх дотримання створюють серйозну загрозу для стійкості і безпеки нашого інформаційного та кібер простору.

Отже, стаття присвячена важливим аспектам забезпечення кібербезпеки в умовах зростаючої кількості вразливостей програмного забезпечення. **Основною метою** даної статті є аналіз розповсюджених технік й тактик кібератак на програмне забезпечення та створення методологічного фундаменту для розробки та впровадження ефективних заходів підсилення захисту програмного забезпечення від несанкціонованого доступу, використання, модифікації або знищення.

Виклад основного матеріалу дослідження. Динаміку збільшення кібератак, техніки і тактики, які при цьому використовуються, можна проаналізувати на основі звітів виробників засобів кіберзахисту, урядових та некомерційних організацій тощо. Подібні звіти є важливим інструментом для аналізу та розуміння ландшафту кіберзагроз, стану кібербезпеки, а також для розробки стратегій і політик щодо її поліпшення. Зі всієї множини таких звітів за останні роки можна виділити:

1. Mandiant: M-Trends reports [8];
2. Qualys: Qualys Survey of Top 10 Exploited Vulnerabilities in 2023 [14];
3. Red Canary Threat Detection Report (2022-2023) [16], [17];

4. CISA Top Vulnerabilities [18]–[22].

Одним з варіантів представлення інформації про актуальні тактики, техніки та процедури, які використовують зловмисники при проведені атак, є матриця MITRE ATT&CK [12]. Вона надає можливість використовувати загальноприйняту термінологію для розуміння та аналізу дій зловмисників при проведені атак на інформаційно-комунікаційні мережі.

Проведемо аналіз статистики ключових технік та тактик кібератак, за даними, що описані у зазначених звітах.

У щорічних звітах Mandiant M-trends [9]–[11] техніки ATT&CK розташовуються за частотою їх використання в інцидентах кібербезпеки, що були проаналізовані цією організацією. В таблиці 1 представлені приклади технік, які прямо або опосередковано використовують вразливості програмного забезпечення, та відсоткові значення, які визначають частоту їх використання. Як видно з цієї таблиці цей відсоток є сталим і достатньо значним.

Таблиця 1 – Техніки та тактики за M-Trends Top Techniques (2019-2022) [9]–[11]

Technique	**1.10.2019-30.09.2020**	**01.10.2020-31.12.2022**	**01.01.2022-31.12.2022**
T1027 - Obfuscated Files or Information	52.6%	51.4%	43.5%
T1059 - Command and Scripting Interpreter	51.3%	44.9%	50.9%
T1059.001 - Command and Scripting Interpreter: PowerShell	40.8%	29.4%	33.2%
T1070 - Indicator Removal on Host	24.4%	31.7%	31.5%
T1071 - Application Layer Protocol	9.5%	36.8%	33.1%
T1021: Remote Services	28.4%	24.7%	26.4%
T1105 - Ingress Tool Transfer	24.2%	26.5%	24.9%
T1190 - Exploit Public-Facing Application	21%	25.8%	21.2%
T1569 - System Services	30.6%	26.5%	21.8%
T1569.002 - System Services: Service Execution	30.6%	26.5%	21.8%
T1055: Process Injection	18.1%	28.5%	23.1%
T1195: Supply Chain Compromise	0.5%	11.1%	0.2%
T1195.002: Compromise Software Supply Chain	0.5%	11.1%	0.2%

В той же час, згідно із даними Red Canary [16]–[17], в ТОП-10 найбільш вживаних технік входять T1055: Process Injection та T1569.002: System Services: Service Execution. Зазначені техніки спрямовані на експлуатацію різноманітних вразливостей програмного забезпечення таких як вразливості мережевих служб, вразливості веб-браузерів, поштових клієнтів тощо, що в свою чергу вказує на помилки при розробці та супроводі програмного забезпечення.

Агентство з кібербезпеки та безпеки інфраструктури США (CISA) [18] в своїх звітах надає перелік технік, які найчастіше використовувались протягом 2020-2022 років [19]–[22]. В більшості випадків ці техніки націлені на виконання шкідливого коду з подальшими зловмисними діями в системі. В звітах зазначається, що зловмисники продовжують використовувати загальновідомі (і часто застарілі) вразливості програмного забезпечення при здійсненні кібератак на широке кола цілей, включаючи організації державного та приватного секторів по всьому світу. У [13] наведена зведена за даними CISA таблиця технік, що найчастіше використовувалися в період за 2020-2022 роки, та відсоткові значення, які визначають частоту їх використання (див. табл. 2).

Аналізуючи наведену таблицю видно, що однією з найбільш поширених технік, які використовувалися в кібератаках у 2020-2022 роках, є T1190 - Exploit Public-Facing Application. Це вказує на те, що вразливістю атакованих систем могла бути помилка програмного забезпечення, його неправильна конфігурація або тимчасовий збій.

Таблиця 2 – Техніки за CISA Alerts Top Techniques (2020-2022) [13]

Technique	2020	2021	2022
T1016 – System Network Configuration Discovery	37.5%	15.38%	21.43%
T1027 - Obfuscated Files or Information	31.25%	46.15%	14.29%
T1057 - Process Discovery	37.5%	23.08%	21.43%
T1059.001 - Command and Scripting Interpreter: PowerShell	37.5%	15.38%	35.71%
T1059.003 - Command and Scripting Interpreter: Windows Command Shell	31.25%	23.08%	21.43%
T1083 - File and Directory Discovery	37.5%	23.08%	35.71%
T1105 - Ingress Tool Transfer	31.25%	23.08%	35.71%
T1133 - External Remote Services	18.75%	38.46%	35.71%
T1190 - Exploit Public-Facing Application	37.5%	23.08%	42.86%
T1566.002 - Phishing: Spearphishing Link	37.5%	46.15%	14.29%

У звіті, представленому компанією Qualys [14] відображається статистика найпопулярніших вразливостей 2023 року за базою вразливостей CVE [15]. У зазначеному звіті доцільно виділити вразливість **CVE-2023-29059 – 3CX Desktop Client Supply Chain Vulnerability,** яка за своєю популярністю у 2023 році посідає 6 місце і полягає в впровадженні .dll файлу (ffmpeg.dll), який містить посилання на шкідливий вміст. Цей файл використовується для завантаження та виконання зловмисного коду після успішної експлуатації вразливості. Як наслідок, після успішної атаки, зловмисники можуть здійснювати різноманітні злочинні дії, включаючи віддалене виконання коду та збір конфіденційної інформації.

Серед вітчизняних звітів слід виділити звіти Урядової команди реагування на комп'ютерні надзвичайні події України [23] та Державного центру кіберзахисту Держспецзв'зяку (ДЦКЗ Держспецзв'язку) [24]–[31].

Категоріювання подій кібербезпеки у зазначених звітах [23]–[31] формувалося відповідно до Переліку категорій кіберінцидентів [32]. В рамках даної праці слід звернути увагу на такі категорії подій як шкідливий програмний код, спроби втручання, втручання та відома вразливість, які мають пряме або опосередковане відношення до експлуатації вразливостей програмного забезпечення. Серед типів подій доцільно виділити зараження ШПЗ, розповсюдження ШПЗ, спробу експлуатації вразливості, компрометацію системи та вразливість. Деякі з категорій та типів подій, що пов'язані зі шкідливим програмним забезпеченням, доцільно розглядати у випадку, коли вони були запроваджені при розробці програмного забезпечення або виникли через недоліки його проектування і розробки. Прикладом такої атаки є атака на SolarWinds [5]–[7], описана раніше. Авторами статті була зведена таблиця кібератак по Україні в період з 2021 року по 2023 рік, на основі вітчизняних звітів [23]–[31] (таблиця 3).

Відповідно до таблиці 3 кількість кібератак за 2022 та 2023 роки зросла більше ніж у 4 рази в порівнянні з 2021 роком. До того ж переважають інциденти, які належать до таких типів подій, як шкідливе підключення, спроба експлуатації та компрометація системи. Ці дані можуть говорити про наявні вразливості програмного забезпечення, що могли з'явитися в наслідок недоліків в процесі розробки програмного забезпечення та можливу недостатню контрольованість цього процесу.

З опрацьованих вище звітів [23]–[31] також виділено вразливості, які з 2021 року найчастіше використовують зловмисники під час проведення кібератак (таблиця 4).

Таблиця 3 — Статистика кібератак по Україні за 2021-2023 роки [23]–[31]

		2021 рік	2022 рік			2023 рік				
			I квартал	III квартал	2022 рік	I квартал	II квартал	III квартал	IV квартал	2023 рік
Детектовано підозрілих подій		41 млн.	14 млн.	1,2 млн.	181 млн.	7 млн.	122 млн.	1,5 млн.	2 млн.	133 млн.
Опрацьовано критичних подій ІБ		160 тис.	78 тис.	73 тис.	179 тис.	34 тис.	55 тис.	12 тис.	46 тис.	148 тис.
Категорія події	02. Шкідливий програмний код	28%	34%	66%	43%	40%	94%	86%	85%	91%
		11,5 млн.	4,7 млн.	400 тис.	78 млн.	2,8 млн.	115 млн.	1,3 млн.	1,7 млн.	121 млн.
	04.Спроби втручання	1%	11%	4%	4%	4%	<1%	2%	3%	<1%
		400 тис.	1.5 млн.	50 тис	2,8 млн.	325 тис.	500 тис.	36 тис.	55 тис.	970 тис.
	05. Втручання	2%	<1%	<1%	<1%	<1%	0%	0%	0%	<1%
		800 тис.	-	-	5 тис.	4 тис.	-	-	-	4 тис.
	09. Відома вразливість	4%	<1%	<1%	<1%	1%	<0%	<1%	<1%	<1%
		1,6 млн.	5 тис.	5 тис.	32 тис.	88 тис.	-	1,8 тис.	1,7 тис.	91 тис.
Тип події	02.01 Зараження ШПЗ	17 тис.	2,3 тис.	-	-	1,8 тис.	-	3 тис.	7 тис.	12 тис.
	02.02 Розповсюдження ШПЗ	17 тис.	10 тис.	120 тис.	переважають	10 тис. +	100 тис.	100 тис.+	100 тис.+	100 тис.+
	02.04 Шкідливе підключення	300 тис.	10 тис.	-	-	10 тис.	100 тис.	100 тис.+	100 тис.+	100 тис.+
	04.01 Спроба експлуатації вразливості	75 тис.	10 тис.	120 тис.	переважають	10 тис. +	100 тис.	37 тис.	55 тис.	100 тис. +
	05.02 Компрометація системи	250 тис.	-	-	-	100 тис. +	-	-	-	100 тис. +
	09.01 Вразливість	300 тис.	8000	128 тис.	переважають	100 тис. +	-	1,8 тис.	1,7 тис.	100 тис. +

Таблиця 4 – Найуживаніші вразливості 2021-2023 року [23]–[31]

	Вразливість									
	CVE-2022-33874	CVE-2022-33872	CVE-2022-41352	CVE-2022-30190	CVE-2021-44228	CVE-2021-26855	CVE-2022-26138	CVE-2021-40539	CVE-2021-21985	CVE-2021-35394
2021 рік					+					
2022 рік	+	+	+	+	+	+	+	+	+	
2023 рік			+	+		+	+	+	+	+

Серед виділених вразливостей доцільно виділити такі, які мають пряме відношення до програмного забезпечення:

1. CVE-2022-33874 – Вразливість компоненти SSH Login Handler у вразливих версіях продуктів Fortinet. Дозволяє реалізовувати віддалене неавторизоване виконання довільного коду.
2. CVE-2022-33872 – Вразливість компоненти Telnet Login Handler у вразливих версіях продуктів Fortinet. Дозволяє реалізовувати віддалене неавторизоване виконання довільного коду.
3. CVE-2022-41352 – Вразливість утиліти "cpio" у фільтрі контенту Amavis, що належить до продукту Zimbra Collaboration, дозволяє реалізовувати розміщення web-shell на комп'ютерах жертв.
4. CVE-2022-30190 – Вразливість у системі Microsoft Support Diagnostic Tool (MSDT) експлуатується за допомогою документів Microsoft Office. Дозволяє реалізовувати віддалене неавторизоване виконання довільного коду.
5. CVE-2021-44228 – Вразливість має назву Log4Shell, пов’язана з бібліотекою Apache Log4j, яка дозволяє реалізовувати віддалене неавторизоване виконання довільного коду.
6. CVE-2021-35394 – Критична вразливість у Realtek Jungle SDK. Успішне використання цієї вразливості дозволяє віддаленим неавторизованим зловмисникам виконувати довільне впровадження команд.
7. CVE-2021-21985 – Вразливість, викликана тим, що компонента програмного забезпечення не перевіряє належним чином дані, які надходять від користувача або іншої системи у програмному забезпеченні VMware vCenter Server.
8. CVE-2021-26855 – Вразливість, викликана тим, що компонента програмного забезпечення не перевіряє належним чином дані, які надходять від користувача або іншої системи у програмному забезпеченні Microsoft Exchange Server.

В той же час слід заначити, що незмінним початковим вектором більш ніж 70% успішних кібератак є фішинг. Проте з другої половини 2022 року хакери почали зміщувати свою увагу з фішингу на використання вразливостей в ІКС організацій і установ, які якимось чином пов’язані з основною ціллю через ланцюги постачання [33]. Найбільшому ризику піддаються компанії, які обслуговують операторів критичної інформаційної інфраструктури, наприклад розробники програмного забезпечення, постачальники послуг Інтернет, тощо.

Атаки на ланцюг постачальників можуть приймати декілька основних напрямків, серед яких можлива атака на постачальника послуг або підрядника (зловмисники атакують менш захищену компанію, яка співпрацює з великою організацією). Іншим напрямком може виступати атака на розробників програмного забезпечення (зловмисники вставляють шкідливий код у продукт або програмне забезпечення, що призначене для клієнтів). Після цього цей код може отримати доступ до системи під прикриттям легітимного програмного забезпечення.

До атак на ланцюг постачання безпосередньо можна віднести кібератаку на SolarWinds [5]–[7]. Компрометація SolarWinds стала великою подією в кіберпросторі, адже не обмежилася лише компрометацією програмного забезпечення однієї компанії, а спровокувала набагато більший інцидент у ланцюзі постачання, який вплинув на тисячі організацій, включаючи уряд США. Об’єми злому є безпрецедентними та одними з найбільших, якщо не найбільшими, у своєму роді з усіх зареєстрованих.

Для запобігання і протидії наведеним атакам в кіберпросторі України необхідно розуміти причини, які призводять до них. На думку авторів, до таких причин можна віднести:

1. Відсутність в Україні стандартів, правил та рекомендацій щодо впровадження процесу безпечної розробки програмного забезпечення, особливо того, що обробляє державні електронні інформаційні ресурси (далі – ДЕІР) та використовується на об’єктах критичної інфраструктури (далі – ОКІ), та вимог обов’язковості їх дотримання.

2. Відсутність затверджених актуальних вимог безпеки, які необхідно впроваджувати в програмному забезпеченні, та вимог щодо обов'язковості їх впровадження.

3. Необхідність розробки й затвердження механізмів верифікації програмного забезпечення на дотримання цих вимог та його валідації.

4. Необхідність (в майбутньому) з боку держави впровадження механізму контролю та перевірки дотримання цих вимог.

5. Відсутність можливості у контролюючих органів самостійно охопити для перевірки (тестування) всього набору програмного забезпечення, яке оброблює ДЕІР та використовується на ОКІ, в короткий час.

6. Необхідність впровадження ефективного управління вразливостями та виправленнями програмного забезпечення, що оброблює ДЕІР та використовується на ОКІ.

Узагальнюючи сказане вище, можна зробити висновки що забезпечення безпеки програмного забезпечення вимагає комплексного підходу, який включає в себе управління безпечною розробкою та тестуванням програмного забезпечення, управління вразливостями та виправленнями, а також впровадження стандартів та рекомендацій для забезпечення безпеки на всіх етапах життєвого циклу програм.

Для усунення зазначених причин необхідно проаналізувати відомі стандарти, підходи, найкращі практики, які дозволять розробити відповідні нормативно-правові документи.

Так для впровадження процесу безпечної розробки програмного забезпечення можливо спиратися на різні моделі SSDLC, включаючи OWASP SAMM [34] та Microsoft SDL, які надають рекомендації для впровадження безпечних процесів розробки. Також слід звернути увагу на стандарт ISO/IEC 27034-3:2018 "Information security management – Application security" [36], який містить загальні вказівки та методику для управління безпекою додатків програмного забезпечення в організаціях і визначає принципи, процеси та методи, які слід застосовувати для забезпечення безпеки програмних додатків на всіх етапах їх життєвого циклу, включаючи розробку, реалізацію, впровадження, експлуатацію та обслуговування.

За основу розробки документу, який би описував вимоги безпеки програмного забезпечення рекомендується взяти, зокрема, ISO/IEC 15408-3:2022 "Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components" [35], який описує критерії оцінки компонентів безпеки програмного забезпечення і надає рамки для оцінки рівня безпеки програмного забезпечення з точки зору його відповідності визначеним стандартам і вимогам безпеки.

При розробці механізмів верифікації програмного забезпечення на дотримання вимог безпеки програмного забезпечення та його валідації можливо використовувати ISO/IEC 25010:2023 "Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Product quality models" [39], який надає критерії оцінки якості, які можуть бути використані для верифікації та валідації програмного забезпечення на дотримання вимог безпеки. В свою чергу ISO/IEC 25022:2019 [40] може використовуватися для оцінки якості використання безпечного програмного забезпечення користувачами та ефективності його застосування в реальних умовах.

Для впровадження ефективного управління вразливостями та виправленнями програмного забезпечення, що оброблює ДЕІР та використовується на ОКІ, слід звернутися до стандартів ISO/IEC 29147:2018 "Information technology – Security techniques – Vulnerability disclosure" [37], та ISO/IEC 30111:2019 "Information technology – Security techniques – Vulnerability handling processes" [38]. Обидва стандарти стосуються обробки та управління вразливостями в інформаційних технологіях . Основна відмінність між ними полягає у тому, що ISO/IEC 29147:2018 визначає вимоги до виявлення та повідомлення про вразливості, тоді як ISO/IEC 30111:2019 описує процеси управління вразливостями, включаючи їх виправлення.

В свою чергу, з однієї сторони є необхідність впровадження з боку держави контролю та перевірки реалізації в програмному забезпеченні, яке оброблює ДЕІР та використовується на ОКІ, вимог безпеки, а з іншої сторони є розуміння того, що контролюючі органи не зможуть

самостійно охопити для перевірки все зазначене програмне забезпечення. Тому стоїть нагальна потреба в розробці такого механізму, який би враховував зазначене.

Наведений перелік стандартів, підходів та найкращих практик є невичерпним, приведеним в якості прикладу і потребує окремого аналізу.

Висновки. Наведена в статті статистика вказує на зростання кількості кібератак, зокрема, спрямованих на ланцюг постачання, підсилений використанням вразливостей у програмному забезпеченні. Причини цих атак можуть бути різні, однак серед них доцільно виділити відсутність стандартів та правил для безпечної розробки програмного забезпечення, а також відсутність затверджених вимог безпеки програмного забезпечення та управління вразливостями. Для запобігання таким загрозам необхідно впроваджувати комплексний підхід до забезпечення безпеки програмного забезпечення, який включає в себе низку напрямів, таких як:

– розроблення вимог та рекомендацій до впровадження процесу безпечної розробки програмного забезпечення;

– розроблення вимог безпеки, які необхідно впроваджувати в програмному забезпеченні;

– розроблення критеріїв перевірки цих вимог;

– розроблення вимог до управління вразливостями програмного забезпечення та управління виправленнями;

– розроблення механізму контролю та перевірки дотримання зазначених вимог розробниками програмного забезпечення.

В статті наведено деякі приклади діючих стандартів, метою яких є забезпечення безпеки програмного забезпечення на всіх етапах його життєвого циклу, від розробки до експлуатації. Після окремого аналізу на основі наведених стандартів в подальшому можливо буде розробити зазначені вище нормативно-правові документи.

Важливо відзначити, що найкращий підхід до забезпечення безпеки програмного забезпечення може варіюватися в залежності від конкретного проекту, технологічного стеку та інших факторів. Однак дотримання вищезазначених напрямків сприяє підвищенню безпеки програмного забезпечення та зменшенню інцидентів безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Ю. Світлик, “Найбільші хакерські атаки: якими вони були та що про них відомо”, *Root Nation*, 2023. [Електронний ресурс]. Доступно: https://root-nation.com/ua/articles-ua/tech-ua/ua-naybilshi-hakerski-ataki. Дата звернення: Лют. 01, 2024.

[2] “Kaseya VSA Supply Chain Ransomware Incident”, *Cloudsek,* 2024. [Online]. Available: https://www.cloudsek.com/blog/kaseya-vsa-supply-chain-ransomware-incident. Accessed on: Feb. 01, 2024.

[3] C. Osborne, “Colonial Pipeline ransomware attack: Everything you need to know”, *ZDNet*, 2021. [Електронний ресурс]. [Online]. Available: https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know. Accessed on: Feb. 01, 2024.

[4] K.S. Sidhu, “Top 5 Famous Software Supply Chain Cyber Attacks in 2023”, *Cloudsek,* 2024. [Online]. Available: https://www.cloudsek.com/blog/top-5-famous-software-supply-chain-cyber-attacks-in-2023. Accessed on: Feb. 01, 2024.

[5] S. Oladimeji, and S.M. Kerner, “SolarWinds hack explained: Everything you need to know”, *TechTarget*, 2023. [Online]. Available: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. Accessed on: Feb. 02, 2024.

[6] B.K. Jena, “SolarWinds Attack And All The Details You Need To Know About It”, *Simplilearn*, 2023. [Online]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack. Accessed on: Feb. 05, 2024.

[7] “SUNBURST”, *MITRE ATT&CK*, 2023. [Online]. Available: https://attack.mitre.org/software/S0559. Accessed on: Feb. 03, 2024.

[8] “Previous M-Trends Reports”, *Mandiant*, 2023. [Online]. Available: https://www.mandiant.com/m-trends. Accessed on: Feb. 05, 2024.
[9] “M-Trends Report 2021”, *Mandiant*, 2021. [Online]. Available: https://services.google.com/fh/files/misc/m-trends-report-2021-en.pdf. Accessed on: Feb. 05, 2024.
[10] “M-Trends 2022: Insights Today's Top Cyber Trends and Attacks”, *Mandiant*, 2022. [Online]. Available: https://www.mandiant.com/resources/reports/m-trends-2022-insights-todays-top-cyber-trends-and-attacks. Accessed on: Feb. 10, 2024.
[11] “M-Trends 2023 Report”, *Mandiant*, 2023. [Online]. Available: https://services.google.com/fh/files/misc/m_trends_2023_report.pdf. Accessed on: Feb. 10, 2024.
[12] “ATT&CK”, *MITRE ATT&CK*. [Online]. Available: https://attack.mitre.org. Accessed on: Feb. 10, 2024.
[13] R. Fetterman, “Zoom: Enhance Finding Value in Macro-Level Attack Reporting”, *Splunk*, 2022. [Online]. Available: https://www.splunk.com/en_us/blog/security/zoom-enhance-finding-value-in-macro-level-att-ck-reporting.html. Accessed on: Feb. 20, 2024.
[14] S. Abbasi, “Qualys Survey of Top 10 Exploited Vulnerabilities in 2023”, *Qualys Blog*, 2023. [Online]. Available: https://blog.qualys.com/qualys-insights/2023/09/26/qualys-survey-of-top-10-exploited-vulnerabilities-in-2023. Accessed on: Feb. 20, 2024.
[15] “CVE – Common Vulnerabilities and Exposures”, *CVE Details*. [Online]. Available: https://www.cve.org. Accessed on: Feb. 15, 2024.
[16] “2023 Threat Detection Report”, *Red Canary*, 2023. [Online]. Available: https://resource.redcanary.com/rs/003-YRU-314/images/2023_ThreatDetectionReport_RedCanary.pdf?mkt_tok=MDAzLVlSVS0zMTQAAAGOorTMDhCsZgrN8O46VVgWSU6Z5b99BYE13gmUp_M-ik7Spkc2uCXkCCTPY2MvmmB5l8vouwcM4y4UHWxkp5_6wfIiscmgeDmuRnilFlnbLK0. Accessed on: Feb. 20, 2024.
[17] “2022 Threat Detection Report”, *Red Canary*, 2022. [Online]. Available: https://redcanary.com/wp-content/uploads/2023/03/2022_ThreatDetectionReport_RedCanary.pdf. Accessed on: Feb. 14, 2024.
[18] “Cybersecurity Alerts & Advisories”, *CISA*. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A94. Accessed on: Feb. 21, 2024.
[19] “2022 Top Routinely Exploited Vulnerabilities”, *CISA*, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-08/aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf. Accessed on: Feb. 18, 2024.
[20] “Top 10 Routinely Exploited Vulnerabilities”, *CISA*, 2020. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-133a. Accessed on: Feb. 12, 2024.
[21] “Top Routinely Exploited Vulnerabilities”, *CISA*, 2021. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a. Accessed on: Feb. 12, 2024.
[22] “2021 Top Routinely Exploited Vulnerabilities”, *CISA*, 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-117a. Accessed on: Feb. 12, 2024.
[23] “Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (2021 р.)”, *CERT-UA*, 2021. [Електронний ресурс]. Доступно: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf. Дата звернення: Лют. 07, 2024.
[24] “Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (перший квартал 2022 року)”, *CERT-UA*, 2022. [Електронний ресурс]. Доступно: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7.pdf. Дата звернення: Лют. 07, 2024.

[25] “Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (третий квартал 2022 року)”, *CERT-UA*, 2022. [Електронний ресурс]. Доступно: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba.pdf. Дата звернення: Лют. 17, 2024.

[26] “Звіт за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (2022 р.)”, *CERT-UA*, 2023. [Електронний ресурс]. Доступно: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf. Дата звернення: Лют. 17, 2024.

[27] “Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (перший квартал 2023 року)”, *CERT-UA*, 2023. [Електронний ресурс]. Доступно: https://scpc.gov.ua/api/files/a7de388d-14d3-4248-b8be-ada8b5cb0710. Дата звернення: Лют. 19, 2024.

[28] “Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (другий квартал 2023 року)”, *CERT-UA*, 2023. [Електронний ресурс]. Доступно: https://scpc.gov.ua/api/files/e4eaafb7-99de-4a60-89f2-f0c05b777b69. Дата звернення: Лют. 19, 2024.

[29] “Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (третий квартал 2023 року)”, *CERT-UA*, 2023. [Електронний ресурс]. Доступно: https://scpc.gov.ua/api/files/22c75b41-d1d8-4da6-bd46-fa5489af9c6e. Дата звернення: Лют. 19, 2024.

[30] “Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (четвертий квартал 2023 року)”, *CERT-UA*, 2023. [Електронний ресурс]. Доступно: https://scpc.gov.ua/api/files/3d552013-d5f6-4c75-9ea3-9e77b429d7a7. Дата звернення: Лют. 20, 2024.

[31] “Звіт за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (2023 р.)”, *CERT-UA*, 2023. [Електронний ресурс]. Доступно: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a. Дата звернення: Лют. 20, 2024.

[32] “Перелік категорії кіберінцидентів”, *CERT-UA*, 2021. [Електронний ресурс]. Доступно: https://cert.gov.ua/recommendation/16904. Дата звернення: Лют. 20, 2024.

[33] “Russia’s Cyber Tactics: Lessons Learned 2022 – аналітичний звіт Держспецзв'язку про рік повномасштабної кібервійни росії проти України”, *ДССЗЗІ*, 2023. [Електронний ресурс]. Доступно: https://cip.gov.ua/ua/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine. Дата звернення: Лют. 22, 2024.

[34] “OWASP SAMM (Software Assurance Maturity Model)”, *OWASP*. [Online]. Available: https://owasp.org/www-project-samm. Accessed on: Feb. 22, 2024.

[35] “Publicly Available Standards”, ISO, 2023. [Online]. Available: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html. Accessed on: Feb. 22, 2024.

[36] ISO/IEC 27034-3, Information technology. Application security. Part 3: Application security management process, *ISO*, 2018. [Online]. Available: https://www.iso.org/standard/55583.html. Accessed on: Feb. 22, 2024.

[37] ISO/IEC 29147, Information technology. Security techniques. Vulnerability disclosure, *ISO*, 2018. [Online]. Available: https://cdn.standards.iteh.ai/samples/72311/06fe3b1905aa4f3f8d9c5824ebc3c396/ISO-IEC-29147-2018.pdf. Accessed on: Feb. 22, 2024.

[38] ISO/IEC 30111, Information technology. Security techniques. Vulnerability handling processes, *ISO*, 2019. [Online]. Available: https://cdn.standards.iteh.ai/samples/69725/127b437f4f0c4b9196fd5b8d3fd294b1/ISO-IEC-30111-2019.pdf. Accessed on: Feb. 22, 2024.

[39] ISO/IEC 25010, Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models, *ISO*, 2023.

[Online]. Available: https://cdn.standards.iteh.ai/samples/78176/13ff8ea97048443f99318920757df124/ISO-IEC-25010-2023.pdf. Accessed on: Feb. 22, 2024.
[40] ISO/IEC 25022: 2016, Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). Measurement of quality, *ISO*, 2016. [Online]. Available: https://www.iso.org/standard/35746.html. Accessed on: Feb. 22, 2024.

Стаття надійшла до редакції 12.04.2024.

REFERENCE

[1] Yu. Svitlyk, "The Biggest Hacker Attacks: What They Were and What Is Known About Them", *Root Nation*, 2023. [Online]. Available: https://root-nation.com/en/articles-en/tech-en/the-biggest-hacker-attacks. Accessed on: Feb. 01, 2024.
[2] "Kaseya VSA Supply Chain Ransomware Incident", *Cloudsek*, 2024. [Online]. Available: https://www.cloudsek.com/blog/kaseya-vsa-supply-chain-ransomware-incident. Accessed on: Feb. 01, 2024.
[3] C. Osborne, "Colonial Pipeline ransomware attack: Everything you need to know", *ZDNet*, 2021. [Online]. Available: https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know. Accessed on: Feb. 01, 2024.
[4] K.S. Sidhu, "Top 5 Famous Software Supply Chain Cyber Attacks in 2023", *Cloudsek*, 2024. [Online]. Available: https://www.cloudsek.com/blog/top-5-famous-software-supply-chain-cyber-attacks-in-2023. Accessed on: Feb. 01, 2024.
[5] S. Oladimeji, and S.M. Kerner, "SolarWinds hack explained: Everything you need to know", *TechTarget*, 2023. [Online]. Available: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. Accessed on: Feb. 02, 2024.
[6] B.K. Jena, "SolarWinds Attack And All The Details You Need To Know About It", *Simplilearn*, 2023. [Online]. Available: https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack. Accessed on: Feb. 05, 2024.
[7] "SUNBURST", *MITRE ATT&CK*, 2023. [Online]. Available: https://attack.mitre.org/software/S0559. Accessed on: Feb. 03, 2024.
[8] "Previous M-Trends Reports", *Mandiant*, 2023. [Online]. Available: https://www.mandiant.com/m-trends. Accessed on: Feb. 05, 2024.
[9] "M-Trends Report 2021", *Mandiant*, 2021. [Online]. Available: https://services.google.com/fh/files/misc/m-trends-report-2021-en.pdf. Accessed on: Feb. 05, 2024.
[10] "M-Trends 2022: Insights Today's Top Cyber Trends and Attacks", *Mandiant*, 2022. [Online]. Available: https://www.mandiant.com/resources/reports/m-trends-2022-insights-todays-top-cyber-trends-and-attacks. Accessed on: Feb. 10, 2024.
[11] "M-Trends 2023 Report", *Mandiant*, 2023. [Online]. Available: https://services.google.com/fh/files/misc/m_trends_2023_report.pdf. Accessed on: Feb. 10, 2024.
[12] "ATT&CK", *MITRE ATT&CK*. [Online]. Available: https://attack.mitre.org. Accessed on: Feb. 10, 2024.
[13] R. Fetterman, "Zoom: Enhance Finding Value in Macro-Level Attack Reporting", *Splunk*, 2022. [Online]. Available: https://www.splunk.com/en_us/blog/security/zoom-enhance-finding-value-in-macro-level-att-ck-reporting.html. Accessed on: Feb. 20, 2024.
[14] S. Abbasi, "Qualys Survey of Top 10 Exploited Vulnerabilities in 2023", *Qualys Blog*, 2023. [Online]. Available: https://blog.qualys.com/qualys-insights/2023/09/26/qualys-survey-of-top-10-exploited-vulnerabilities-in-2023. Accessed on: Feb. 20, 2024.
[15] "CVE – Common Vulnerabilities and Exposures", *CVE Details*. [Online]. Available: https://www.cve.org. Accessed on: Feb. 15, 2024.

[16] “2023 Threat Detection Report”, *Red Canary*, 2023. [Online]. Available: https://resource.redcanary.com/rs/003-YRU-314/images/2023_ThreatDetectionReport_RedCanary.pdf?mkt_tok=MDAzLVlSVS0zMTQAAAGOorTMDhCsZgrN8O46VVgWSU6Z5b99BYE13gmUp_M-ik7Spkc2uCXkCCTPY2MvmmB5l8vouwcM4y4UHWxkp5_6wfIiscmgeDmuRnilFlnbLK0. Accessed on: Feb. 20, 2024.

[17] “2022 Threat Detection Report”, *Red Canary*, 2022. [Online]. Available: https://redcanary.com/wp-content/uploads/2023/03/2022_ThreatDetectionReport_RedCanary.pdf. Accessed on: Feb. 14, 2024.

[18] “Cybersecurity Alerts & Advisories”, *CISA*. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A94. Accessed on: Feb. 21, 2024.

[19] “2022 Top Routinely Exploited Vulnerabilities”, *CISA*, 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-08/aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf. Accessed on: Feb. 18, 2024.

[20] “Top 10 Routinely Exploited Vulnerabilities”, *CISA*, 2020. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-133a. Accessed on: Feb. 12, 2024.

[21] “Top Routinely Exploited Vulnerabilities”, *CISA*, 2021. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a. Accessed on: Feb. 12, 2024.

[22] “2021 Top Routinely Exploited Vulnerabilities”, *CISA*, 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-117a. Accessed on: Feb. 12, 2024.

[23] “Report on the work of the system for detection of vulnerabilities and response to cyber incidents and cyber attacks (2021)”, *CERT-UA*, 2021. [Online]. Available: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf. Accessed on: Feb. 07, 2024.

[24] “Report on the work of the system for detection of vulnerabilities and response to cyber incidents and cyber attacks (Q1 2022)”, *CERT-UA*, 2022. [Online]. Available: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7.pdf. Accessed on: Feb. 07, 2024.

[25] “Report on the work of the system for detection of vulnerabilities and response to cyber incidents and cyber attacks (Q3 2022)”, *CERT-UA*, 2022. [Online]. Available: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1ba.pdf. Accessed on: Feb. 17, 2024.

[26] “Report on the results of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks (2022)”, *CERT-UA*, 2023. [Online]. Available: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf. Accessed on: Feb. 17, 2024.

[27] “Report on the work of the system for detection of vulnerabilities and response to cyber incidents and cyber attacks (Q1 2023)”, *CERT-UA*, 2023. [Online]. Available: https://scpc.gov.ua/api/files/a7de388d-14d3-4248-b8be-ada8b5cb0710. Accessed on: Feb. 19, 2024.

[28] “Report on the work of the system for detection of vulnerabilities and response to cyber incidents and cyber attacks (Q2 2023)", SCPC, 2023. [Online]. Available: https://scpc.gov.ua/api/files/e4eaafb7-99de-4a60-89f2-f0c05b777b69. Accessed on: Feb. 19, 2024.

[29] “Report on the work of the system for detection of vulnerabilities and response to cyber incidents and cyber attacks (Q3 2023)”, *CERT-UA*, 2023. [Online]. Available: https://scpc.gov.ua/api/files/22c75b41-d1d8-4da6-bd46-fa5489af9c6e. Accessed on: Feb. 19, 2024.

[30] "Report on the work of the system for detection of vulnerabilities and response to cyber incidents and cyber attacks (Q4 2023)", *CERT-UA*, 2023. [Online]. Available: https://scpc.gov.ua/api/files/3d552013-d5f6-4c75-9ea3-9e77b429d7a7. Accessed on: Feb. 20, 2024.
[31] "Report on the results of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks (2023)", *CERT-UA*, 2023. [Online]. Available: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a. Accessed on: Feb. 20, 2024.
[32] "List of Cyber Incident Categories", *CERT-UA*, 2021. [Online]. Available: https://cert.gov.ua/recommendation/16904. Accessed on: Feb. 20, 2024.
[33] "Russia's Cyber Tactics: Lessons Learned 2022 – an analytical report by the State Service of Special Communications and Information Protection of Ukraine on the year of Russia's full-scale cyber war against Ukraine", *SSSCIP*, 2023. [Online]. Available: https://cip.gov.ua/ua/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine. Accessed on: Feb. 22, 2024.
[34] "OWASP SAMM (Software Assurance Maturity Model)", *OWASP*. [Online]. Available: https://owasp.org/www-project-samm. Accessed on: Feb. 22, 2024.
[35] "Publicly Available Standards", ISO, 2023. [Online]. Available: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html. Accessed on: Feb. 22, 2024.
[36] ISO/IEC 27034-3, Information technology. Application security. Part 3: Application security management process, *ISO*, 2018. [Online]. Available: https://www.iso.org/standard/55583.html. Accessed on: Feb. 22, 2024.
[37] ISO/IEC 29147, Information technology. Security techniques. Vulnerability disclosure, *ISO*, 2018. [Online]. Available: https://cdn.standards.iteh.ai/samples/72311/06fe3b1905aa4f3f8d9c5824ebc3c396/ISO-IEC-29147-2018.pdf. Accessed on: Feb. 22, 2024.
[38] ISO/IEC 30111, Information technology. Security techniques. Vulnerability handling processes, *ISO*, 2019. [Online]. Available: https://cdn.standards.iteh.ai/samples/69725/127b437f4f0c4b9196fd5b8d3fd294b1/ISO-IEC-30111-2019.pdf. Accessed on: Feb. 22, 2024.
[39] ISO/IEC 25010, Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models, *ISO*, 2023. [Online]. Available: https://cdn.standards.iteh.ai/samples/78176/13ff8ea97048443f99318920757df124/ISO-IEC-25010-2023.pdf. Accessed on: Feb. 22, 2024.
[40] ISO/IEC 25022: 2016, Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). Measurement of quality, *ISO*, 2016. [Online]. Available: https://www.iso.org/standard/35746.html. Accessed on: Feb. 22, 2024.

OLHA SHEVCHUK,
ARTEM ZHYLIN,
ARTEM MYKYTIUK,
ANATOLII MINOCHKIN

DIRECTIONS FOR STRENGTHENING THE PROTECTION OF SOFTWARE PROCESSING STATE ELECTRONIC INFORMATION RESOURCES AND USED AT CRITICAL INFRASTRUCTURE FACILITIES

In the modern world, where more and more aspects of our lives become dependent on computer systems and networks, cybersecurity becomes increasingly critical. One of the key elements of cybersecurity is protecting the software used in these systems. Software can contain vulnerabilities that attackers can exploit to gain unauthorized access to systems, data, and resources. These

vulnerabilities may arise from coding errors, improper configurations, or inadequate software updates. Attackers continuously refine their methods and tactics not only to exploit software vulnerabilities but also to influence their emergence by targeting the supply chain. This makes software cybersecurity an increasingly complex challenge.

This article addresses the pressing issue of cybersecurity in the context of the proliferation of cyberattacks on software, including supply chain attacks. Examples of known cyberattacks targeting the supply chain are provided. The shortcomings in the existing system of standards and rules for secure software development are highlighted, as well as the lack of security requirements and vulnerability management. A comprehensive approach to ensuring software security is proposed, which includes the development of appropriate requirements, standards, and control mechanisms.

Keywords: cybersecurity, software, software security, supply chain, supply chain attack

Шевчук Ольга Сергіївна, викладач кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-2866-439X, olia13511@gmail.com.

Жилін Артем Вікторович, кандидат технічних наук, доцент, професор кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-4959-612X, zhylinartem@gmail.com.

Микитюк Артем В'ячеславович, доктор філософії, заступник завідувача кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-8307-9978, mukuta8888@gmail.com.

Міночкін Анатолій Іванович, доктор технічних наук, професор, провідний науковий співробітник Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна, ORCID 0000-0002-4123-604X, minanatol@gmail.com.

Shevchuk Olha, teacher of the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Zhylin Artem, candidate of technical sciences, associate professor, professor of the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Mykytiuk Artem, PhD in engineering, deputy of the head at the cybersecurity and application of information systems and technologies academic department, Institute of special communications and information security of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Minochkin Anatolii, doctor of technical sciences, professor, leading researcher in Heroiv Krut Military institute of telecommunications and informatization, Kyiv, Ukraine.