Звіт про громадське обговорення проєкту стандарту вищої освіти першого (бакалаврського) рівня, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації

1. Найменування органу виконавчої влади, який проводив обговорення:

Міністерство освіти і науки України.

2. Зміст питання або назва проєкту документу, що виносилися на обговорення:

Проєкт стандарту вищої освіти України першого (бакалаврського) рівня спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології (далі – проєкт Стандарту).

Розробка стандартів передбачена статтею 10 Закону України «Про вищу освіту».

Стандарт вищої освіти − це сукупність вимог до освітніх програм вищої освіти, які є спільними для всіх освітніх програм у межах певного рівня вищої освіти та спеціальності.

Стандарти вищої освіти розробляються для кожного рівня вищої освіти в межах кожної спеціальності відповідно до Національної рамки кваліфікацій і використовуються для визначення та оцінювання якості вищої освіти та результатів освітньої діяльності закладів вищої освіти (наукових установ), результатів навчання за відповідними спеціальностями.

Враховуючи зміну найменування спеціальності, відповідно до постанови КМУ від 16 грудня 2022 р. № 1392 та затвердження професійних стандартів з кібербезпеки та захисту інформації виникла необхідність нової редакції стандарту.

Громадське обговорення проведено у формі електронних консультацій. Проєкт Стандарту було розміщено 25 грудня 2023 р. на офіційному вебсайті Міністерства освіти і науки України за посиланням:

https://mon.gov.ua/ua/news/mon-proponuye-do-gromadskogo-obgovorennya-proyekt-novoyi-redakciyi-standartu-vishoyi-osviti-zi-specialnosti-125-kiberbezpeka-ta-zahist-informaciyi-na-pershomu-bakalavrskomu-rivni-vishoyi-osviti

Зауваження та пропозиції до проєкту Стандарту приймалися до 09 січня 2024 р. на електронну адресу: mruga@mon.gov.ua.

3. Інформація про осіб, що взяли участь в обговоренні:

Впродовж встановленого для обговорення з громадськістю терміну надіслано зауваження та пропозиції десяти адресантів: **Анатолій Чепинога**, декан факультету інформаційних технологій і систем Черкаського державного технологічного університету; **члени проєктної групи** ОПП «Кібербезпека» підготовки здобувачів першого (бакалаврського) рівня вищої за спеціальністю 125 Кібербезпека та захист інформації у Чернівецькому національному університеті імені Юрія Федьковича; **Пєвнєв Володимир Яковлевич**, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут»; **Пашорін Валерій Іванович**, завідувач кафедри кібербезпеки та захисту інформації Європейського університету; **Владислав Голь**, завідувач СК№1

Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»; **Громадська організація «Українське науково-освітнє ІТ товариство»**; **Михайло Коломицев; Олена Олександрівна Хоменко; Мелкозьорова О. М.; Василь Яцків.**

4. Інформація про пропозиції, що надійшли до Міністерства освіти і науки України за результатами обговорення:

Пропозиції Анатолія Чепиноги, декана факультету інформаційних технологій і систем Черкаського державного технологічного університету.

У розділі ІІ. Загальна характеристика → Опис предметної області →

Об'єкти професійної діяльності:

- об'єкти інформатизації, *включаючи* інформаційні системи, інформаційні ресурси і технології;

Замінити: «включаючи» на «в тому числі»

- технології захисту інформації;

Замінити: на «технології кібербезпеки та захисту інформації»

Теоретичний зміст предметної області:

- теорії інформації, автентифікації та прийняття рішень

Замінити: «теорії інформації, автентифікації» на «методи автентифікації або теорія доступу»

- моделювання складних систем та оптимізації процесів

Замінити: «складних систем» на «складних систем»

- теорії ризиків та інших міждисциплінарних дисциплін та практик

Замінити: «міждисциплінарних» на «дотичних»

Інструменти та обладнання:

Викласти в редакції:

«Засоби, пристрої, мережне устаткування, прикладне, спеціалізоване та системне програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків)»

Розділ ІІІ. Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти

Доповнити:

«На основі ступеня «фаховий молодший бакалавр» заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти.»

У розділі ІV. Перелік компетентностей випускника:

КФ10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти та оцінювати можливі вразливості та загрози інформаційному простору та інформаційним ресурсам *згідно з встановленою політикою безпеки інформації*.

Замінити: «згідно з встановленою політикою безпеки інформації» на «встановленої політики кібербезпеки та захисту інформації»

У розділі V. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті результатів навчання

ПРН8. Вміти використовувати інформаційні технології, сучасні методи та моделі кібербезпеки та систем захисту інформації під час виконання службових обов'язків.

Викласти в редакції: «Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.»

ПРН9. Планувати підготовку та забезпечувати неперервність *процесів* в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.

Замінити: «процесів» на «бізнес-процесів»

ПРН10. Застосовувати методи захисту інформації в інформаційних системах згідно *встановленої політики безпеки інформації*;

Замінити: «встановленої політики безпеки інформації» на «встановленої політики кібербезпеки та захисту інформації»

ПРН12. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного *забезпечення, щодо захисту та відновлення інформації*;

Замінити: «забезпечення, щодо захисту та відновлення інформації» на «забезпечення щодо захисту та відновлення інформації»

ПРН14. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;

Викласти в редакції: «Вирішувати задачі проектування, впровадження та супроводу комплексних систем захисту інформації в інформаційних системах та\або інфраструктурі організації.»

ПРН19. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Викласти в редакції: «Виконувати впровадження, підтримку та аналіз ефективності систем виявлення несанкціонованого доступу і дій з інформацією в інформаційній системі, оцінку вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам і використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.»

Пропозиції членів проєктної групи ОПП «Кібербезпека» підготовки здобувачів першого (бакалаврського) рівня вищої за спеціальністю 125 Кібербезпека та захист інформації у Чернівецькому національному університеті імені Юрія Федьковича.

Розділ проєкту	**Редакція проєкту**	**Пропозиція**
І. Преамбула, Перший абзац	Стандарт вищої освіти України (далі Стандарт) перший (бакалаврський) рівень, галузь знань	Стандарт вищої освіти України (далі Стандарт) перший (бакалаврський) рівень, галузь знань 12 –

	12 Інформаційні технології, спеціальність 125 Кібербезпека та *захисті* інформації.	Інформаційні технології, спеціальність 125 – Кібербезпека та *захист* інформації.
ІІ. Загальна характеристика, Опис предметної області, Інструменти та обладнання:	Засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту *даних (інформаційних потоків)*.	Засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, *відображення та захисту даних/ інформаційних потоків*.
ІV. Перелік компетентностей випускника, Фахові компетентності	**КФ6**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів *та ін.)*	**КФ6**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
V. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті результатів навчання,	**ПРН2**. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.	**ПРН2**. Організовувати власну професійну діяльність *(зокрема в колективі),* обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
	ПРН12. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного	**ПРН12**. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного *забезпечення*

	забезпечення, щодо захисту та відновлення інформації;	*щодо захисту та відновлення інформації.*
	ПРН13. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, *проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.*	**ПРН13.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, *оперативно проводити аналіз та дослідження кіберінциденту.*
	ПРН14. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;	**ПРН14**. Вирішувати задачі *розроблення,* впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
	ПРН18. Визначати загрози *створення* технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи ТЗІ від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.	**ПРН18**. Визначати загрози *формування* технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи ТЗІ від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
	ПРН19. *Виконувати* впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	**ПРН19.** *Здійснювати* впровадження, підтримку, *проводити* аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

VI. Форми атестації здобувачів вищої освіти	За рішенням *навчального захисту* атестація може включати додатково захист кваліфікаційної роботи, яка має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не має бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що *мають* інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.	За рішенням *закладу вищої освіти* атестація може включати додатково захист кваліфікаційної роботи, яка має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не має бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що *містять* інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти чи його структурного підрозділу, або у репозитарії закладу вищої освіти.

Пропозиція Пєвнєва В.Я., Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут».

У розділі ІІ. Загальна характеристика → Опис предметної області → Теоретичний зміст предметної області:

- теорії інформації, автентифікації та прийняття рішень

Замінити: «автентифікації» на «ефективності»

У розділі V. Перелік компетентностей випускника

КФ6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

*Викласти в редакції: «*КФ6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних, *криптографічних* та технічних засобів і методів, процедур, практичних прийомів та ін.)

Коментар: Якщо додати цю пропозицію, то КФ6 поглинає КФ8 та КФ9. Або за аналогією необхідно додати новий КФ такого змісту «Здатність застосовувати організаційні методи та засоби захисту інформації на об'єктах інформаційної діяльності».

У розділі V. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті результатів навчання

Вилучити: ПРН17. Вирішувати задачі щодо організації та контролю стану

криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

Коментар: Цей ПРН вимагає знання документів з обмеженим доступом та наявністю допуску, якого наші студенти отримати не можуть. Невиконання одного з ПРНів веде до закриття спеціальност.

Пропозиції*:* Пашоріна Валерія Івановича, завідувача кафедри кібербезпеки та захисту інформації Європейського університету.

У розділі IV. Перелік компетентностей випускника:

КФ4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.

Викласти в редакції: «**КФ4**. Здатність забезпечувати захист інформації в інформаційних системах *та мережах згідно прийнятої* політики кібербезпеки та захисту інформації.»

КФ5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

Викласти в редакції: «**КФ5**. Здатність відновлювати функціонування інформаційних систем *та мережевої інфраструктури після здійснення кібератак*, збоїв та відмов різних класів та походження.»

КФ6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних, та технічних засобів і методів, процедур, практичних прийомів та ін.)

Викласти в редакції: «Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних, *програмних, апаратних* та технічних засобів і методів, процедур, практичних прийомів та ін.)»

КФ9. Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.

Викласти в редакції: «Здатність застосовувати методи та засоби *програмного, апаратного, та* технічного захисту інформації на об’єктах інформаційної діяльності.»

Пропозиції Владислава Голя, завідувача СК№1 Інституту спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

1. Внести до переліку джерел КЛАСИФІКАТОР ПРОФЕСІЙ ДК 003:2010.
2. Доповнити додаток 1 відповідностями між ЗК і певними ПРН.
3. В розділі «Форми атестації здобувачів вищої освіти» виправити помилку: *Замінити*: «За рішенням навчального захисту атестація ...» на «За рішенням навчального закладу атестація...».
4. КФ2 викласти в редакції: «КФ2. Здатність до використання інформаційних технологій, технологій електронних комунікацій та програмування, сучасних методів і моделей кібербезпеки та систем захисту інформації».
5. ПРН8 викласти в редакції: «ПРН8. Вміти використовувати інформаційні технології, технологій електронних комунікацій, віртуалізації та автоматизації, сучасні методи та моделі кібербезпеки та систем захисту інформації під час

виконання службових обов'язків.»

Пропозиції Громадської організації «Українське науково-освітнє ІТ товариство».

1. Зауваження, дискусійні питання або питання, які потребують пояснення стосовно принципових аспектів:

- стор. 5: «Мінімум 70% (60% при відповідності освітньо-професійної програми певному професійному стандарту у сфері кібербезпеки та захисту інформації) обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених Стандартом вищої освіти» – потребує пояснення;
- стор. 6: *фахові компетентності* мають враховувати:

а) рівні інформаційних та *операційних* технологій;

б) *функційна безпечність* і кібербезпека: кібербезпека індустріальних систем (стандарти IEC61508, IEC 62443…);

в) аспект штучного інтелекту і кібербезпеки (AI powered attacks/protection);

- «За рішенням навчального захисту атестація може включати додатково захист кваліфікаційної роботи» – пропонується для обговорення;
- відповідність окремих вимог за рівнем складності першому (бакалаврському) рівню.

2. Зауваження стосовно повноти, коректності окремих положень:

- об'єкт професійної діяльності, стор. 4: пропонується розглянути не тільки «технології захисту» (програмні, технічні засоби та технології…);
- знання, стор. 4: «… теорії інформації, автентифікації та прийняття рішень…» – пропонується розглянути не лише теорію; пропонується не виокремлювати, оскільки може виникнути питання – чому тільки «автентифікації» тощо; крім того, мають бути враховані знання «…*методів та/або засобів* моделювання, криптографічного захисту…»;
- стор. 5: теорії ризиків та *інших міждисциплінарних дисциплін* та практик;
- стор.5: «Моделі, методи та алгоритми розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації…» – пропонується додати «програмні та технічні засоби»;
- вказані ПРН потребують змістовного і стилістичного опрацювання:

а) ПРН2, стор. 7: «обирати (*чи-та використовувати?*) оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність»;

б) ПРН12, стор. 7: «Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням *процедур резервування* згідно встановленої політики безпеки…» – потребує коригування (наприклад, не тільки процедур, а і *засобів* резервування тощо);

в) ПРН15, стор. 8: «Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі *здійснення процедур кількісної і якісної оцінки ризиків*»;

г) ПРН19, стор. 8: «Виконувати впровадження, *підтримку*, аналіз ефективності систем виявлення несанкціонованого доступу, *дій з інформацією в*

інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам».

3. Стилістичні зауваження, окремі помилки, необхідне редагування тексту:

- стор. 2, перший абзац.

Крім того, на платформі ГО «УНІТ» було проведено публічне обговорення Проєкту нової редакції Стандарту вищої освіти України зі спеціальності 125 – Кібербезпека та захист інформації на першому (бакалаврському) рівні вищої освіти, до якого долучились більше 60 учасників (https://www.facebook.com/po.useit/posts/1119266212530648). За результатами цього обговорення пропонуємо також наступні побажання та зауваження учасників:

1. Наразі ЗВО не має альтернатив у виборі форм атестації – лише ЄДКІ.
2. Не достатньо враховано професійні стандарти (21 шт. і низка в розробці) – 10% насправді не достатньо, рекомендують учасники проєкту USAID.
3. Не враховано можливість сертифікації випускників в органах сертифікації Держспецзвязку (які активно створюються).
4. У переліку джерел до стандарту немає Законів про захист персональних даних, про доступ до публічної інформації, про основні засади забезпечення кібербезпеки тощо, про захист інформації в ІКС.
5. До літератури пропонується врахувати Національний класифікатор професій ДК 003:2010.
6. Чи доцільно в Теоретичний зміст предметної області включати два такі пункти: 1) знання фундаментальних основ фізичних і математичних наук; 2) знання моделювання складних систем та оптимізації процесів? Як вони розкривають суть предметної області. Можливо їх доцільно подати в результатах навчання? Оскільки окреслюється предметна область саме з кібербезпеки та захисту інформації.
7. В теоретичному змісті предметної області відсутній термін *сигнали* в контексті завдань із захисту інформації. Чи будуть *«сигнали»* частиною змісту освіти в цьому стандарті? Наприклад, ПРН з попередньої редакції стандарту могли б бути модифіковані (ПРН 36; ПРН 37; ПРН 38). Стандарти інших спеціальностей, зокрема і 172 ЕКР, саме ці питання не містять.
8. В тексті проєкту стандарту присутній складний термін *«теоретичних і практичних задач кібербезпеки та захисту інформації»*. Можливо доцільно, оскільки це перший (бакалаврський) рівень записувати термін *«задач кібербезпеки та захисту інформації»* без поділу на теоретичні і практичні або написати *«інженерних задач кібербезпеки та захисту інформації»*. Аналогічно у формі атестації здобувачів *«...розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації...»* – *«...розв'язок спеціалізованого завдання в галузі кібербезпеки та захисту інформації...»*.
9. Проєкт цього стандарту недостатньо відповідає змісту ЄДКІ. Можливо доцільно переглянути і зміст ЄДКІ одночасно зі стандартом або врахувати теми з ЄДКІ в цьому стандарті? Наприклад, розділ *«7. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»*. Крім того, багато деталізованих тем в ЄДКІ не відображені детальніше в проєкті стандарту (https://kb.khmnu.edu.ua/wp-content/uploads/sites/6/63861d8f5ff01844854871.pdf).

Пропозиція Михайла Коломицева.

В розділі «Форми атестації здобувачів вищої освіти» виправити помилку:

Замінити: «За рішенням навчального захисту…» на «За рішенням навчального закладу…»

Пропозиція Олени Олександрівни Хоменко.

Зберегти складову щодо «Історії української державності та культури», тому що під час війни і агресії з боку Російської Федерації, знати свою історію, розуміти державотворчі процеси свої країни, шанувати традиції і культуру свого народу – це обов'язок кожного громадянина України.

Пропозиції Мелкозьорової О. М.

У розділі ІІ. Загальна характеристика → Опис предметної області → Інструменти та обладнання:

Засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків).

Викласти в редакції: «Засоби, пристрої, *мережеве обладнання*, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, *зберігання*, обробки, відображення та захисту даних (інформаційних потоків).»

Пропозиція Василя Яцківа.

В розділі «Форми атестації здобувачів вищої освіти» виправити помилку:

Замінити: «За рішенням навчального захисту…» на «За рішенням навчального закладу…»

5. Інформація про рішення, прийняті за результатами обговорення:

Під час доопрацювання проєкту Стандарту зауваження та пропозиції, отримані під час громадського обговорення, враховано частково.