ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2023.2(60) **Issue 2(60) 2023**
УДК 343.973

Сахарова Олена Борисівна,
кандидат юридичних наук, старший науковий співробітник,
начальник відділу ДНДІ МВС України,
м. Київ, Україна
ORCID ID 0000-0002-9759-5324
Близнюк Ігор Леонідович,
кандидат юридичних наук, старший науковий співробітник,
головний науковий співробітник ДНДІ МВС України,
м. Київ, Україна
ORCID ID 0000-0003-3882-5790

ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ І КІБЕРАТАКИ ЯК ЗАХОДИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

У статті обґрунтовуються положення, на основі яких автори приходять до висновку, що виявлення та реагування на кіберінциденти і кібератаки необхідно вважати заходами запобігання кіберзлочинності. Розгорнуто розкрито особливості збирання та збереження доказів, пов'язаних з кіберінцидентом, основні завдання процесу реагування на кіберінциденти, першочергові настанови щодо процедур управління кіберінцидентами, цілі управління кіберінцидентами, зміст процедур звітування про події інформаційної безпеки / кіберінциденти тощо.

Ключові слова: *кіберінцидент, кібератаки, кібербезпека, інформаційна безпека, запобігання кіберзлочинності, кіберзлочин, цифрові докази, захист інформації, управління кіберінцидентами, кібераудит, події інформаційної безпеки, критична інфраструктура, кіберзагроза, кіберзахист, система управління інформаційною безпекою (СУІБ), ризик-орієнтований підхід, кіберризик.*

Україна вже тривалий час є об'єктом регулярних і масштабних кібератак, які загрожують стабільному функціонуванню критичної інфраструктури, зокрема під час дії воєнного стану. Кібернапади стають дедалі більше досконалими, цілеспрямованими, широко розповсюдженими, дедалі складніше стає ідентифіковувати зловмисників. Поряд з цим спостерігається постійне зростання кількості зареєстрованих інцидентів інформаційної безпеки, зокрема в системах, які підключені до мережі Internet, причому останніми роками темп приросту кількості кіберінцидентів прискорюється. Водночас втілювані заходи протидії не відповідають зростанню кількості кіберінцидентів. У такій ситуації виникає нагальна потреба у проведенні моніторингу, виявлення та реагування на кіберінциденти і кібератаки з метою запобігання кіберзлочинності, оскільки існуючі підходи до захисту інформації та управління кіберінцидентами є недостатньо ефективними. Такі негативні тенденції спонукають здійснювати пошук нових методів удосконалення процесів реагування, обробки, розслідування та запобігання кіберінцидентам, які в сукупності складають процес управління кіберінцидентами [1, с. 119].

DOI (Article): https: //doi.org/10.36486/np.2023.2(60).23

У свою чергу, під системою протидії кіберзлочинності у широкому сенсі (не обмежуючись правоохоронною діяльністю) можна розуміти взаємопов'язану сукупність організаційно-правових, організаційно-технічних заходів запобігання, виявлення, припинення та розкриття кіберзлочинів [9, с. 98].

Для управління кіберінцидентами необхідно реалізувати можливість своєчасного виявлення кіберінцидентів та адекватного реагування на них відповідними контрзаходами. У цьому відношенні з метою моніторингу захищеності інфраструктури, управління кіберінцидентами, контролю відповідності вимогам у держоргані, на підприємстві, в організації, установі необхідно здійснювати пошук та усунення вразливостей, аналіз зовнішніх та внутрішніх джерел щодо актуальних кіберзагроз та розроблення заходів щодо кіберзахисту, збору, аналізу та аудиту журналів подій інформаційної безпеки в системі, а також виявлення, аналіз, реагування, розслідування кіберінцидентів та розроблення заходів щодо покращення діючих процесів та заходів кібербезпеки на основі отриманого досвіду [3, с. 119].

Зміст процесу управління кіберінцидентами включає: ідентифікацію та фіксацію кіберінцидентів; реакцію; розслідування; документування [2].

У держорганах, на підприємствах, в організаціях, установах доцільно упровадити систему реагування та управління кіберінцидентами та протидії кіберзлочинам, а також управління інформаційною безпекою передусім згідно з вимогами національного стандарту України з питань інформаційної безпеки ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» («Information technology – Security techniques – Information security management systems – Requirements») для визначеної сфери застосування, після обов'язкового проведення кібераудиту з урахуванням вимог міжнародних стандартів, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту з метою підвищення рівня кібербезпеки установи. У межах цього стандарту ISO/IEC 27001:2015 висуваються загальні вимоги до побудови системи управління інформаційною безпекою, які стосуються, зокрема і процесів управління кіберінцидентами.

Управління кіберінцидентами та протидії кіберзлочинам є проблемою, яку необхідно вирішувати не перманентно, а постійно мати в полі уваги як послідовний безперервний процес, що динамічно протікає в режимі реального часу, починаючи з розробки вимог кібербезпеки та складання технічного завдання на проєктування системи управління інформаційною безпекою, технічної експлуатації, наступної модернізації та вдосконалення, і не закінчуючи, а й надалі продовжуючи на наступних життєвих циклах управління інформаційною безпекою в межах установи.

Водночас слід наголосити, що упровадження стандартів з питань реагування та управління кіберінцидентами та протидії кіберзлочинам, а також управління інформаційною безпекою не може бути разовою акцією. Це фактично є безперервним процесом розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою (СУІБ) та кіберзахисту, а також реагування, управління кіберінцидентами та протидії кіберзлочинам. Для процесів СУІБ має бути застосована класична модель ПВПД (PDCA – англ.) (плануй (Plan) – виконуй (Do) – перевіряй (Check) – дій

DOI (Article): https: //doi.org/10.36486/np.2023.2(60).23

(Act)), наведена у вступі до стандарту ISO/IEC 27001:2022. Модель PDCA є основою функціонування всіх процесів системи управління інформаційною безпекою [3, с. 120].

Передумовою впровадження системи реагування, управління кіберінцидентами та протидії кіберзлочинам, а також управління інформаційною безпекою у держоргані, на підприємстві, в організації, установі має бути реалізація ризик-орієнтованого підходу до забезпечення кібербезпеки. Ризик-орієнтований підхід до забезпечення кібербезпеки – прийняття управлінських рішень у держоргані, на підприємстві, в організації, установі на підставі аналізу порівняння поточних ризиків кібербезпеки з прийнятними.

У держоргані, на підприємстві, в організації, установі доцільно запровадити, використовуючи ризик-орієнтований підхід, заходи кібербезпеки, визначені додатком А до ДСТУ ISO/IEC 27001:2015, а також згідно з ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки» («Information technology – Security techniques – Code of practice for information security controls»).

З метою ефективного реагування та виявлення кіберінцидентів, а також протидії кіберзлочинам у держоргані, на підприємстві, в організації, установі рекомендується дотримуватися вимог міжнародних стандартів управління інформаційною безпекою серії ISO 27000.

Критично важливим компонентом реагування та розслідування кіберінциденту є збирання та збереження доказів, пов'язаних з кіберінцидентом, оскільки проаналізовані дані про інцидент кібербезпеки можуть стати потенційними цифровими доказами у судових розглядах. Крім того, зібрані докази кіберінциденту можуть бути використані для вивчення кібервразливостей з метою підвищення рівня кібербезпеки у держоргані, на підприємстві, в організації, установі.

Для обробки подій інформаційної безпеки та кіберінцидентів необхідно ефективно організувати процес реагування на кіберінциденти. Це пов'язано з тим, що зниження потенційних ризиків порушення доступності, цілісності та конфіденційності інформаційних ресурсів внаслідок кіберінцидентів може бути досягнуто шляхом їх своєчасного виявлення у комплексі з реагуванням. До того ж реагування на кіберінциденти – часто менш дорогий і ефективніший засіб, ніж їх розслідування, оскільки кіберінцидент, що відбувся, може призвести до збою працездатності систем, сервісів, мереж, і, як наслідок, до тривалої недоступності критичних процесів, втрати / модифікації інформації, що передається або зберігається, без можливості її відновлення, репутаційних ризиків власника інформаційних ресурсів.

Методика реагування на кіберінциденти повинна давати можливість динамічно в режимі реального часу прогнозувати, враховувати та адаптуватися до можливих інцидентів, змін у множині кіберзагроз і вразливостей [1, с. 118].

Основними завданнями процесу реагування на кіберінциденти є:

координація реагування на кіберінцидент;

підтвердження / спростування факту виникнення кіберінциденту;

забезпечення збереження і цілісності доказів виникнення кіберінциденту, створення умов для накопичення і зберігання точної інформації про вчинені кіберінциденти, про корисні рекомендації;

мінімізація порушень порядку роботи і пошкодження даних ІТ-системи, відновлення в найкоротші терміни її працездатності після кіберінциденту;

мінімізація наслідків порушення конфіденційності, цілісності та доступності інформації ІТ-систем;

створення умов для відкриття цивільного або кримінального провадження проти зловмисників;

захист інформаційних ресурсів;

швидке виявлення та / або попередження подібних кіберінцидентів в майбутньому;

навчання персоналу діям з виявлення, усунення наслідків кіберінцидентів та запобігання кіберінцидентам [2].

На підготовчому етапі процесу реагування на кіберінциденти, який призначений для організації та регламентування діяльності з реагування на кіберінциденти, необхідно:

виділити людські та матеріальні ресурси;

розробити схему реагування на кіберінциденти;

розробити та затвердити ряд організаційно-регламентуючих документів;

провести необхідне навчання персоналу та апробацію обраної схеми реагування на кіберінциденти;

провести тестування схеми реагування на кіберінциденти [2].

Крім того, має бути визначена документована процедура реєстрації та оброблення кіберінцидентів, а також відповідальності персоналу. Зокрема, повинні бути визначені:

процедури для забезпечення швидкого та ефективного реагування на кіберінциденти;

у посадових інструкціях працівників або організаційно-розпорядчих документах – персональні функції та обов'язки з виявлення, класифікації, реагування та аналізу кіберінцидентів.

При цьому доцільно забезпечити документування інформації щодо кіберінцидентів, що відбулись, та її зберігання не менше ніж один рік. Також доречно автоматизувати процес управління кіберінцидентами.

Загалом у держоргані, на підприємстві, в організації, установі мають бути реалізовані наведені нижче настанови щодо процедур управління кіберінцидентами:

а) повинні бути розроблені процедури обробки різних видів кіберінцидентів, охоплюючи:

1) відмови інформаційної системи;

2) зловмисний код;

3) помилки внаслідок неповних або неточних даних;

4) порушення конфіденційності та цілісності;

5) зловживання інформаційними системами;

б) додатково до звичайних планів дій в аварійних обставинах процедури мають також включати:

1) аналіз та ідентифікацію причини кіберінциденту;

2) його локалізацію;

3) планування та впровадження коригувальних дій для запобігання рецидивам, за необхідності;

4) зв'язок з тими, хто постраждав від кіберінциденту або залучений до відновлення;

5) звітування про кіберінцидент працівниками, які мають належні повноваження;

в) журнали кібераудиту та докази щодо кіберінцидентів повинні збиратися і за необхідності захищатися для:

1) внутрішнього аналізу проблеми;

2) застосування як судового доказу стосовно потенційного порушення контрактних чи нормативних вимог або у разі цивільних чи кримінальних позовів;

3) ведення переговорів щодо компенсації від постачальників програмного забезпечення та послуг;

г) діяльність з відновлення після порушень кібербезпеки і відмов у коректній роботі системи повинна ретельно контролюватися з офіційним оформленням; процедури мають забезпечувати, щоб:

1) лише чітко ідентифікованому та авторизованому персоналу дозволявся доступ до діючих систем та оперативних даних;

2) усі вжиті аварійні дії були детально задокументовані;

3) аварійні дії звітувалися керівництву і системно переглядалися;

4) цілісність інформаційних систем та заходів кібербезпеки підтверджувалась з мінімальною затримкою.

Реагування на кіберінциденти (застосування необхідних заходів для запобігання, зменшення і відновлення після завданого ушкодження) має здійснюватися також відповідно до задокументованої процедури.

Отже, управління кіберінцидентами є важливим процесом, що сприяє оперативному відновленню нормальної роботи служб і зведення до мінімуму негативного впливу кіберінциденту на діяльність держоргану, підприємства, організації, установи з метою підтримки якості і доступності служб (сервісів) на максимально можливому рівні [3, с. 119-120].

Цілі управління кіберінцидентами повинні бути погоджені з керівництвом держоргану, підприємства, організації, установи. Водночас слід забезпечити, щоб особи, відповідальні за управління кіберінцидентами, правильно розуміли пріоритети щодо обробки кіберінцидентів.

Зокрема, цілями управління кіберінцидентами є:

відновлення нормальної роботи служб в найкоротші терміни;

зведення до мінімуму впливу кіберінцидентів на діяльність держоргану, підприємства, організації, установи;

забезпечення злагодженої обробки всіх кіберінцидентів і запитів обслуговування;

зосередження ресурсів підтримки на найбільш важливих напрямках забезпечення кібербезпеки;

надання відомостей, які уможливлюють оптимізацію процесів підтримки, зменшення кількості кіберінцидентів та ефективне планування управління кіберінцидентами [4, с. 117].

Управління кіберінцидентами – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються інформаційних систем, а на виході цих процесів отримують інформацію про причини кіберінциденту, що відбувся, про нанесений збиток та заходи, які необхідно вжити для того, щоб кіберінцидент не повторився у майбутньому. Таким чином, управління кіберінцидентами

спрямоване на вдосконалення системи забезпечення кібербезпеки держоргану, підприємства, організації, установи та запобігання кіберзлочинності. Водночас одержувані на виході дані є, по суті, єдиною об'єктивною інформацією для визначення ймовірності кіберзагроз при аналізі кіберризиків.

При цьому необхідно усвідомлювати, що управління кіберінцидентами не запобігає нанесенню збитку юридичній особі, проте розслідування кіберінциденту та своєчасне впровадження превентивних та корегувальних заходів знижує ймовірність його повторення. До цього слід додати, що статистика кіберінцидентів має особливу цінність для держоргану, підприємства, організації, установи як показник ефективності функціонування системи управління інформаційною безпекою.

Особливості управління кіберінцидентами регламентуються міжнародними та національними нормативними документами, зокрема, ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27035, ISO/IEC 27042 та ISO/IEC 27043, NIST SP 800-16 тощо.

Крім того, необхідно якнайшвидше звітувати стосовно подій інформаційної безпеки / кіберінцидентів через належні канали управління. З цією метою у держоргані, на підприємстві, в організації, установі повинні бути розроблені офіційно оформлені процедури звітування про події інформаційної безпеки / кіберінциденти, а також процедури реагування та ескалації щодо них, де встановлено дії, яких треба вжити персоналу після отримання звіту про події інформаційної безпеки / кіберінциденти. Також у держоргані, на підприємстві, організації, установі має бути контактна особа для звітування про події інформаційної безпеки / кіберінциденти.

Процедури звітування про події інформаційної безпеки / кіберінциденти повинні включати:

а) відповідні процедури зворотного зв'язку для забезпечення того, щоб ті, хто звітував про події інформаційної безпеки / кіберінциденти, були сповіщені про результати після того, як проблему було оброблено й закрито;

б) форми звітування про подію інформаційної безпеки / кіберінцидент;

в) правильну поведінку, якої треба дотримуватися у разі події інформаційної безпеки / кіберінцидента, тобто:

1) негайно записувати усі важливі подробиці (наприклад, тип невідповідності або порушення, збій, повідомлення на екрані, незвичайний режим роботи);

2) не виконувати жодних власних дій, а негайно звітувати контактній особі;

г) посилання на офіційно оформлений дисциплінарний процес поводження з персоналом, користувачами третьої сторони, які здійснили порушення кібербезпеки.

Прикладами подій інформаційної безпеки та кіберінцидентів є:

втрата послуги, обладнання або засобів обслуговування;

збій або перевантаження системи;

людські помилки;

невідповідності політиці або настановам;

порушення заходів фізичної безпеки;

неконтрольовані зміни системи;

збій програмного забезпечення або апаратних засобів;

порушення доступу.

Поряд із зазначеним вище також треба вимагати від усього персоналу, що користується інформаційними системами, звертати увагу та звітувати щодо будь-яких спостережених або очікуваних слабких місць кібербезпеки у системах. При цьому персоналу та користувачам третьої сторони слід рекомендувати не намагатися знайти підтвердження очікуваного слабкого місця кібербезпеки. У подальшому події інформаційної безпеки оцінюються та приймається рішення стосовно віднесення їх до кіберінцидентів.

Оцінювання кіберінцидентів може вказати на потребу в удосконалених або додаткових контролях для обмеження частоти, ушкодження та вартості майбутніх кіберінцидентів або може бути взяте до уваги в процесі перегляду Політики інформаційної безпеки держоргану, підприємства, організації, установи. Знання, отримані з аналізу та розв'язання кіберінцидентів, мають використовуватися для зменшення ймовірності чи впливу майбутніх кіберінцидентів та для запобігання кіберзлочинності.

Крім того, у держоргані, на підприємстві, в організації, установі повинні бути визначені і застосовані процедури для ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як докази щодо кіберінцидентів.

Докази інцидентів кібербезпеки (cybersecurity incident evidence) – це згідно з Рекомендацією Міжнародного союзу електрозв'язку МСЕ-Т Х.1216 (09/2020) «Вимоги до збирання та збереження доказів інцидентів кібербезпеки» («Requirements for collection and preservation of cybersecurity incident evidence») [5] інформація або дані, які зберігаються або передаються та які в процесі аналізу були визначені як такі, що стосуються розслідування інциденту кібербезпеки. Це визначення доказів щодо кіберінцидентів базується на визначенні «цифровий доказ» ISO/IEC 27037:2012 «Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence» («Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, накопичення та збереження цифрових доказів»).

При цьому цілісність усіх доказових матеріалів щодо кіберінцидентів повинна бути захищена. Копіювання доказового матеріалу має здійснюватися під наглядом персоналу, який заслуговує довіри, та повинна бути зареєстрована інформація: коли і де виконувався процес копіювання, хто здійснював копіювання і які інструменти та програми були застосовані.

Водночас у держоргані, на підприємстві, в організації, установі регулярно має проводитися моніторинг системи управління інформаційною безпекою (СУІБ), який має використовуватися для перевірки ефективності прийнятих заходів кібербезпеки.

Частота перегляду результатів діяльності з моніторингу СУІБ повинна залежати від кіберризиків. Фактори кіберризику, які треба розглядати, включають: критичність прикладних процесів; цінність, чутливість та критичність оброблюваної інформації; минулий досвід проникнення в систему та зловживання, частоту використання вразливостей; ступінь взаємозв'язаності систем (особливо загальнодоступних мереж) тощо.

У держоргані, на підприємстві, в організації, установі мають бути розроблені процедури моніторингу використання засобів оброблення інформації та результати такого моніторингу повинні регулярно переглядатися.

Використання процедур моніторингу СУІБ дозволяє переконатися в тому, що ко-

ристувачі виконують лише ту діяльність, яка чітко авторизована (дозволена). У зв'язку з цим, у держоргані, на підприємстві, в організації, установі повинен вестися та зберігатися протягом погодженого періоду для сприяння в майбутніх розслідуваннях кіберінцидентів і моніторингу контролю доступу журнал аудиту подій, у якому повинна записуватися діяльність користувачів, винятки, збої та події кібербезпеки. Ці журнали аудиту мають бути захищені та регулярно переглядатися.

У держоргані, на підприємстві, в організації, установі також слід здійснювати моніторинг інформаційних систем та реєструвати події кібербезпеки. Для забезпечення ідентифікації проблем інформаційної системи повинні використовуватися журнали реєстрації оператора і реєстрація несправностей. Перегляд журналу реєстрації призводить до розуміння кіберзагроз, на які наражається система, та способу, в який вони можуть виникнути.

Засоби реєстрування та інформація реєстрації подій кібербезпеки мають бути захищені у держоргані, на підприємстві, в організації, установі від фальсифікації та несанкціонованого доступу. За можливості, системні адміністратори не наділені повноваженнями стирати або деактивувати журнали реєстрації власної діяльності.

У 2012 р. був оприлюднений міжнародний стандарт ISO/IEC 27037:2012 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, накопичення та збереження цифрових доказів», який регламентує керівні принципи для конкретних видів діяльності у сфері обробки цифрових даних, що можуть мати доказове значення [6, с. 54]. Протягом 2015–2019 рр. також набули чинності ще чотири міжнародні стандарти, які стосуються експертизи цифрових доказів [6, с. 54]: ISO/IEC 27041:2015 «Інформаційні технології. Методи захисту. Настанова щодо забезпечення прийнятності та адекватності методів розслідування»; ISO/IEC 27042:2015 «Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу»; ISO/IEC 27043:2015 «Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів»; ISO/IEC 27050:2019 «Інформаційні технології. Технології безпеки. Електронне відкриття (в 4-х частинах)». Наприклад, ISO/IEC 27043 пропонує настанови, що описують процеси та принципи, які застосовують до різних видів досліджень, включаючи несанкціонований доступ, пошкодження даних, збої в системі або порушення інформаційної безпеки, а також будь-які інші цифрові дані розслідування [7].

На сьогодні зазначені вище чотири міжнародних стандарти у галузі дослідження цифрових доказів гармонізовані в Україні як ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT); ДСТУ ISO/IEC 27041:2016 (ISO/IEC 27041:2015, IDT), ДСТУ ISO/IEC 27042:2016 (ISO/IEC 27042:2015, IDT); ДСТУ ISO/IEC 27043:2016 (ISO/IEC 27043:2015, IDT) шляхом їх прийняття як національних стандартів України методом підтвердження [6, с. 56].

Узагальненою метою забезпечення інформаційної безпеки держоргану, підприємства, організації, установи є зниження ризиків, діючих відносно інформаційних ресурсів, і, як наслідок, – запобігання або мінімізація збитку від можливих кіберінцидентів [8, с. 97]. Основним завданням процесу управління кіберінцидентами є усунення кіберінцидентів у гранично стислі терміни.

Таким чином, на основі зазначеного вище, можна констатувати, що кіберінцидентом, у першу чергу, є певна недозволена подія інформаційної безпеки, вона має бути

неприпустимою, забороненою. Отже, існує необхідність розробки та затвердження внутрішньо організаційних документів, що чітко описують усі дії, які можна виконувати в інформаційній системі і які виконувати заборонено. При цьому процес управління кіберінцидентами, як правило, покладається на службу ІТ-підтримки, яка обробляє кіберінциденти [8, с. 97].

Варто також розуміти, що управління кіберінцидентами не попереджає нанесення збитку, проте розслідування кіберінциденту та своєчасне впровадження превентивних і коригувальних заходів знижує ймовірність його рецидиву [8, с. 97].

Діяльність держоргану, підприємства, організації, установи без системи управління кіберінцидентами може обернутися низкою неприємностей. У результаті впровадження процесу управління кіберінцидентами держорган, підприємство, організація, установа отримують такі важливі й корисні властивості, як якість сервісів, скорочення кількості кіберінцидентів та безперервне функціонування. Як наслідок, в умовах зростання впливу ІТ на діяльність будь-якої установи значна увага приділяється організації підтримки та супроводу ІТ-систем та управлінню кіберінцидентами.

Формування групи для проведення розслідування, реагування на кіберінциденти включає визначення осіб, відповідальних за розслідування. У держоргані, на підприємстві, організації, установі існує три варіанти вирішення цього питання: провести внутрішнє розслідування кіберінциденту; звернутися до правоохоронних органів; звернутися до спеціалізованих груп реагування на кіберінциденти [8, с. 98]. Під час проведення внутрішнього розслідування кіберінциденту у держоргані, на підприємстві, організації, установі стикаються з такими проблемами: низька кваліфікація співробітників у питаннях реагування на кіберінциденти; недостатня кількість співробітників і часу; неможливість отримати необхідну інформацію під час розслідування кіберінциденту та ін. Під час вибору третього варіанту слід розуміти, що конфіденційна інформація може стати відомою стороннім організаціям.

Гарантією безпечної роботи внутрішньої інформаційної системи є виконання необхідних заходів, які зводять до мінімуму всі існуючі ризики з урахуванням їх ступеня впливу на кібербезпеку. Ці вимоги визначаються необхідністю врахування всіх ризиків і інтересів, що виникають у процесі впровадження нових інформаційних технологій. Одним зі шляхів вирішення цих питань є побудова моделей створення й оцінки ефективності систем кібербезпеки, що забезпечують кібербезпеку на основі системного підходу до врахування впливу ризиків [8, с. 99].

Передусім для визначення необхідного комплексу заходів проєктують і розробляють модель системи кібербезпеки. Юридичні особи, що мають стратегії кібербезпеки, повинні гарантувати, що кожна з підкатегорій кібербезпеки буде врахована [8, с. 99].

Сьогодні кіберзахист не може обмежуватися технічними заходами, а має бути інтегрований у такі традиційні види діяльності з безпеки, як забезпечення фізичної безпеки та безпеки персоналу, бути частиною загальноорганізаційних зусиль з метою захисту всіх критичних процесів як від зовнішніх, так і від внутрішніх загроз [8, с. 99]. Активності з кібербезпеки мають бути пріоритетними та узгоджуватися з основною діяльністю установи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Гладиш С.В.* Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах. Реєстрація, зберігання і обробка даних. 2008. Т. 10. № 1. С. 116–124. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7536/11-Gladysh.pdf?sequence=1 (дата звернення: 11.06.2023).

2. Управління інцидентами інформаційної безпеки. URL: https://studfile.net/preview/16435760/ (дата звернення: 11.06.2023).

3. *Козаченко П.П., Панаско О.М.* Управління інцидентами в контексті інформаційної безпеки підприємства. Specialized and multidisciplinary scientific researches: збірник наукових праць ΛΌΓΟΣ. 2020. Vol. 2. P. 119–120. URL: https://ojs.ukrlogos.in.ua/index.php/logos/article/view/7127/7110 (дата звернення: 11.06.2023).

4. Аудит та управління інцидентами інформаційної безпеки: навч. посіб.: *Корченко О.Г., Гнатюк С.О., Казмірчук С.В*. та ін. К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с.

5. Recommendation ITU-T X.1216 (09/2020) "Requirements for collection and preservation of cybersecurity incident evidence": SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY «Cyberspace security – Cybersecurity». URL: https://www.itu.int/rec/T-REC-X.1216-202009-I (дата звернення: 11.06.2023).

6. *Рувін О.Г., Полтавський А.О.* Стандартизація техніко-криміналістичного та судово-експертного забезпечення правосуддя в Україні: праксеологічний аспект. Криміналістика і судова експертиза: міжвідом. наук.-метод. зб. / Київський НДІ судових експертиз; редкол.: О.Г. Рувін (голов. ред.) та ін. К., 2017. Вип. 62. С. 51–58.

7. Нові стандарти для інформаційної безпеки. URL: http://volynstandart.com.ua/info_security/4193/news/ (дата звернення: 11.06.2023).

8. *Воскобойников С., Решетніков О.* Проєктування освітнього процесу професійної підготовки майбутніх фахівців до управління інцидентами інформаційної та кібернетичної безпеки. Педагогічні науки: теорія, історія, інноваційні технології. 2020. № 8 (102). С. 95–106.

9. *Довгань О.Д., Тарасюк А.В.* Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. Інформація і право. 2018. № 3 (26). С. 94–103.

REFERENCES

1. *Hladysh S.V*. (2008). Pidtrymka pryiniattia rishen shchodo keruvannia intsydentamy informatsiinoi bezpeky v orhanizatsiino-tekhnichnykh systemakh. "Support for decision-making regarding the management of information security incidents in organizational and technical systems". Registration, storage and processing of data. Vol. 10, № 1. P. 116–124. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7536/11-Gladysh.pdf?sequence=1. (Date of Application: 11.06.2023) [in Ukrainian].

2. Upravlinnia intsydentamy informatsiinoi bezpeky. "Management of information security incidents". URL: https://studfile.net/preview/16435760/. (Date of Application: 11.06.2023) [in Ukrainian].

3. *Kozachenko P.P., Panasko O.M*. (2020). Upravlinnia intsydentamy v konteksti informatsiinoi bezpeky pidpryiemstva. "Incident management in the context of enterprise information security". Abstracts of Papers ΛΌΓΟΣ. Vol. 2. P. 119–120. 'Proccedings of the Conference Title'. URL: https://ojs.ukrlogos.in.ua/index.php/logos/article/view/7127/7110. (Date of Application: 11.06.2023) [in Ukrainian].

4. *Korchenko O.H., Hnatiuk S.O., Kazmirchuk S.V*. (2014). Audyt ta upravlinnia intsydentamy informatsiinoi bezpeky. "Audit and management of information security incidents". Kyiv. 190 p. [in Ukrainian].

5. Recommendation ITU-T X.1216 (09/2020). "Requirements for collection and preservation of cybersecurity incident evidence": SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY 'Cyberspace security – Cybersecurity'. URL: https://www.itu.int/rec/T-REC-X.1216-202009-I. (Date of Application: 11.06.2023) [in English].

6. *Ruvin O.H., Poltavskyi A.O.* (2017). Standartyzatsiia tekhniko-kryminalistychnoho ta sudovo-ekspertnoho zabezpechennia pravosuddia v Ukraini: prakseolohichnyi aspekt. "Standardization of technical-criminological and judicial-expert provision of justice in Ukraine: praxeological aspect". Abstracts of Papers, vol. 62: Forensics and forensic examination: 'Proccedings of the Conference Title' Kyiv. P. 51–58. [in Ukrainian].

7. Novi standarty dlia informatsiinoi bezpeky. "New standards for information security". URL: http://volynstandart.com.ua/info_security/4193/news/. (Date of Application: 11.06.2023) [in Ukrainian].

8. *Voskoboinykov S., Reshetnikov O.* (2020). Proiektuvannia osvitnoho protsesu profesiinoi pidhotovky maibutnikh fakhivtsiv do upravlinnia intsydentamy informatsiinoi ta kibernetychnoi bezpeky. "Designing the educational process of professional training of future specialists for information and cyber security incident management". Pedagogical sciences: theory, history, innovative technologies. №. 8(102). P. 95–106. [in Ukrainian].

9. *Dovhan O.D., Tarasiuk A.V*. (2018). Hlobalna kultura kiberbezpeky v systemi zapobihannia kiberzlochynnosti v Ukraini. "Global culture of cyber security in the system of cybercrime prevention in Ukraine". Information and Law. №. 3 (26). P. 94–103. [in Ukrainian].

UDC 343.973

Sakharova Olena,
Candidate of Juridical Sciences, Senior Research Officer,
Head of the Department,
State Research Institute MIA Ukraine,
Kyiv, Ukraine,
ORCID ID 0000-0002-9759-5324
Blyzniuk Ihor,
Candidate of Juridical Sciences, Senior Research Officer, Chief Researcher,
State Research Institute MIA Ukraine,
Kyiv, Ukraine,
ORCID ID 0000-0003-3882-5790

IDENTIFYING AND RESPONDING TO CYBER INCIDENTS AND CYBERATTACKS AS CYBERCRIME PREVENTION MEASURES

The article substantiates the provisions underlying the authors' conclusion that detecting and responding to cyber incidents and cyberattacks should be considered as cybercrime prevention measures. Consequently, they believe that monitoring, detecting and responding to cyber incidents and cyberattacks is necessary to prevent cybercrime, since existing approaches to information security and cyber incident management are not effective enough.

The article explains the content and defines the cyber incident management process. The authors recommend that state bodies, enterprises, organizations, and institutions implement a system for responding to and managing cyber incidents and countering cybercrimes, as well as information security management in accordance with the requirements of the national standard

of Ukraine on information security DSTU ISO/IEC 27001:2015 'Information technology – Security techniques – Information security management systems – Requirements' for a defined scope of application, after a mandatory cyber audit taking into account the requirements of international standards, the principles of information security and cyber protection generally accepted in international practice in order to increase the level of cyber security institutions At the same time, the authors especially emphasize that the management of cyber incidents and combating cybercrimes is a problem that must not be solved permanently, but must be constantly kept in the field of attention as a consistent, continuous process that flows dynamically in real time, starting with the development of cybersecurity requirements and drawing up a technical the task of designing the information security management system, technical operation, subsequent modernization and improvement, and not ending, but continuing in the following life cycles of information security management within the institution.

Along with this, this article addresses the issues of collecting and preserving evidence related to a cyber incident, as the analyzed data on a cybersecurity incident may become potential digital evidence in court proceedings. Furthermore, the authors of the article disclose in detail key tasks of the cyber incident response process, basic guidelines of cyber incident management procedures, goals of cyber incident management, content of procedures for reporting information security events/cyber incidents, etc.

Keywords: cyber incident, cyberattacks, cybersecurity, information security, cybercrime prevention, cybercrime, digital evidence, information protection, cyber incident management, cyber audit, information security events, critical infrastructure, cyber threat, cyber defense, information security management system (ISMS), risk-based approach, cyber risk.

Отримано 14.06.2023