**ЗАТВЕРДЖЕНО**
наказ ДП «Інформаційні судові системи»
від «19» 02 2024 № 33/ОД

# ПЕРЕЛІК
## відомостей, що становлять службову інформацію та можуть міститися в документах та на інших матеріальних носіях інформації на державному підприємстві «Інформаційні судові системи»

### 1. Організаційно-управлінська діяльність

1.1. Службова кореспонденція і відомості в організаційно-розпорядчій документації Підприємства (накази, службові/доповідні записки, рекомендації, інструкції, настанови тощо) пов'язані з розробкою напряму діяльності Підприємства та/або процесів прийняття рішень (за умови дотримання сукупності вимог, передбачених частиною другою статті 6 Закону України «Про доступ до публічної інформації»).

1.2. Відомості, що містяться в документах Підприємства, які становлять службову інформацію ДСА України, ТУ ДСА України, судових установ, інших органів державної влади, підприємств, установ та організацій.

1.3. Документи нормативно-правового та претензійно-позовного характеру, які опрацьовуються працівниками Підприємства та мають гриф обмеження доступу «Для службового користування».

### 2. Мобілізаційна робота та військовий облік

2.1. Нормативно-правові акти, нормативні та інші розпорядчі документи з питань мобілізаційної роботи.

2.2. Відомості про виконання законів, інших нормативно-правових актів з питань мобілізаційної роботи.

2.3. Відомості про військовозобов'язаних, забронюваних за Підприємством.

2.4. Документи, справи, видання та інші матеріальні носії інформації, які містять відомості про заходи з мобілізаційної роботи.

2.5. Відомості про довгострокові та річні програми мобілізаційної роботи.

2.6. Звіт про чисельність військовозобов'язаних, які забронювані згідно з переліками посад і професій військовозобов'язаних, які підлягають бронюванню на період мобілізації та на воєнний час.

### 3. Документи з питань криптографічного захисту інформації

3.1. Довідки, листи, таблиці та схеми (за окремими показниками) про: зміст, стан, наявність недоліків в організації чи забезпеченні безпеки, плани розвитку системи криптографічного захисту службової (конфіденційної) інформації, порядок застосування (роботи) засобів криптографічного захисту службової інформації, результати розробки, виробництва, досліджень та експлуатації цих засобів і порядок забезпечення режиму безпеки під час їх проведення, крім тих, що становлять державну таємницю.

3.2. Довідки, листи, таблиці та схеми про взаємодію підрозділів Підприємства з органами державної влади, підприємствами, установами та організаціями у сфері криптографічного захисту службової (конфіденційної), інформації, якщо ці відомості не становлять державної таємниці.

3.3. Довідки, листи, таблиці та схеми про порядок використання, поводження, технічні характеристики ключових документів до засобів криптографічного захисту службової (конфіденційної) інформації.

3.4. Довідки, листи, таблиці та схеми про зміст ключових даних до засобів криптографічного захисту службової інформації.

3.5. Довідки, листи, таблиці та схеми про номенклатуру, кількість засобів криптографічного захисту службової (конфіденційної) інформації, місця їх розташування.

## 4. Документи з питань технічного захисту інформації

4.1. Довідки, листи, таблиці та схеми з питань технічного захисту інформації, вимога щодо захисту якої встановлена законодавством, якщо вони не розкривають норми (вимоги) та методики контролю технічного захисту інформації, крім тих, що становлять державну таємницю.

4.2. Довідки, листи, таблиці про планування, організацію запровадження заходів, фактичний стан, наявність недоліків в організації захисту інформації щодо окремого об'єкта інформаційної діяльності, інформаційної, телекомунікаційної, інформаційно-телекомунікаційної системи, де циркулює (або передбачена циркуляція) інформація, вимога щодо захисту якої встановлена законодавством, крім тих, що становлять державну таємницю. Рекомендації щодо приведення стану захисту інформації на зазначених об'єктах і системах у відповідність із вимогами законодавства, крім тих, що становлять державну таємницю.

4.3. Довідки, листи, таблиці та схеми про зміст заходів, склад засобів комплексу технічного захисту інформації або комплексної системи захисту інформації, призначених для захисту інформації, вимога щодо захисту якої встановлена законодавством (крім тих, що становлять державну таємницю), на конкретному об'єкті інформаційної діяльності або в конкретній інформаційній (автоматизованій), телекомунікаційній чи інформаційно-телекомунікаційній системі.

4.4. Довідки, листи, таблиці та схеми про взаємодію із суб'єктами владних повноважень, військовими формуваннями, підприємствами, установами та організаціями незалежно від форм власності з питань організації технічного захисту інформації, вимога щодо захисту якої встановлена законом, крім тих, що становлять державну таємницю.

4.5. Довідки, листи, таблиці та схеми про організацію заходів щодо створення комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, що містяться у протоколах, звітах, підготовлених та оформлених за результатами нарад і зустрічей з представниками органів державної влади, підприємств, установ.

4.6. Довідки, листи, таблиці та схеми про склад та структуру, результати державної експертизи комплексних систем захисту інформації в інформаційно-

телекомунікаційних системах, заходи, які здійснюються при її проведенні, способи (методи) і порядок проведення цих заходів, що містяться в матеріалах державних експертиз у сфері технічного захисту інформації (що не становить державної таємниці), а також узагальнені довідки, листи, таблиці та схеми щодо виданих/зареєстрованих атестатів відповідності комплексних систем захисту інформації в інформаційно-телекомунікаційних системах вимогам нормативних документів.

4.7. Технологічна інформація щодо формування та підтримки роботи ресурсів судової інформаційної системи, в тому числі автоматизованих систем у її складі.

4.8. Інформація про вжиття та використання спеціальних заходів і засобів для забезпечення захисту інформаційних ресурсів підприємства та судової системи.

## 5. Документи з питань запобігання та виявлення корупції

Довідки, листи, таблиці про зміст заходів, що розкривають конкретні завдання щодо запобігання корупційним правопорушенням та аналітичну (прогнозовану) інформацію за їх результатами, розголошення яких може завдати негативних наслідків репутації або правам інших осіб.

## 6. Несекретне діловодство

6.1. Відомості про втрату документів, виробів або інших матеріальних носіїв інформації, яким надано гриф «Для службового користування», та про факт розголошення службової інформації.

6.2. Відомості, отримані від інших органів державної влади, місцевого самоврядування, військових формувань, підприємств, установ та організацій, яким надано гриф обмеження доступу.

## 7. Кіберзахист

7.1. Відомості щодо діяльності Підприємства з питань організації кіберзахисту державних інформаційних ресурсів, інформації вимога щодо захисту якої встановлена законом, розголошення яких може призвести до негативних наслідків.

7.2. Інформація щодо перспектив і стратегій розвитку інформаційно-комунікаційних систем, адміністрування яких здійснює Підприємство, захисту інформації та кіберзахисту, володіння якою дає змогу заінтересованій стороні впливати на їх реалізацію.

7.3. Відомості щодо окремого об'єкта кіберзахисту про планування, організацію запровадження та зміст заходів, фактичний стан, наявність недоліків в організації кіберзахисту, а також рекомендації щодо підвищення рівня кіберзахисту, розголошення яких може призвести до негативних наслідків у сфері національної безпеки і оборони.

7.4. Відомості про взаємодію із суб'єктами забезпечення кібербезпеки та власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури держави з питань організації кіберзахисту, виявлення, попередження, припинення кібератак та кіберінцидентів, а також усунення їх наслідків,

розголошення яких може призвести до негативних наслідків у сфері національної безпеки та оборони.

7.5. Відомості про структуру та склад програмних та апаратних компонентів об'єкта кіберзахисту, їх налаштування, порядок взаємодії, журнали реєстрації подій (логи) компонентів об'єкта кіберзахисту, виявлення, запобігання, припинення кібератак та кіберінцидентів, а також усунення їх наслідків, розголошення яких може призвести до негативних наслідків.

7.6. Сукупність відомостей про топологію побудови, місце розташування, склад програмних та апаратних засобів систем управління інформаційно-комунікаційних систем, адміністратором яких є Підприємство, принцип та методи забезпечення кіберзахисту та впровадження політик інформаційної безпеки.

7.7. Відомості за окремими показниками про номенклатуру, кількість і тактико-технічні характеристики технічних засобів, що використовуються в інформаційно-комунікаційних системах, адміністратором яких є Підприємство.

СХВАЛЕНО
Протокол засідання комісії
з питань роботи із службовою
інформацією державного підприємства
«Інформаційні судові системи»

від 16.02.2024 №1