

Перелік  
Відомостей, що становлять службову  
інформацію і яким надається гриф  
«Для службового користування»

№ п/п	Відомості, які містять службову інформацію
<b>1 Мобілізаційна робота</b>	
1.1	Відомості, які не включені до Зводу відомостей, що становлять державну таємницю (наказ СБУ № 383 від 23.12.2020) про заходи мобілізаційної підготовки, мобілізаційного плану та інших документів щодо:
1.1.1	створення, розвитку, утримання, передачі, ліквідації, реалізації та фінансування мобілізаційних потужностей;
1.1.2	виконання робіт, надання послуг для задоволення потреб Збройних Сил України, інших військових формувань в особливий період;
1.1.3	забезпечення виконавців затверджених мобілізаційних завдань матеріально-технічними, сировинними та енергетичними ресурсами в особливий період;
1.1.4	мобілізаційних завдань із замовлення на виробництво продукції, виконання робіт, надання послуг в особливий період;
1.1.5	кількості автотранспортної, дорожньо-будівельної, підйомно-транспортної техніки, повітряних суден, які підлягають передачі до складу Збройних Сил України;
1.1.6	показників із праці та кадрів, джерел забезпечення кадрами потреб підприємства на особливий період;
1.1.7	забезпечення медичними, транспортними, поштовими, телекомунікаційними, житлово-комунальними, побутовими, ремонтними та іншими послугами в особливий період;
1.1.8	створення та накопичення нестандартного обладнання та устаткування на особливий період;
1.1.9	номенклатури, обсягів (норм) накопичення, місць зберігання, фактичної наявності, якісного стану матеріальних цінностей мобілізаційного резерву підприємства.
1.1.10	капітального будівництва в особливий період;
1.1.11	створення страхового фонду документації для забезпечення виконання робіт в особливий період;
1.2	Відомості про заходи, які заплановані або здійснюються для забезпечення сталості функціонування підприємства за умов воєнного стану щодо організації та проведення відновлювальних робіт, технічного прикриття об'єктів.
1.3	Відомості про загальну кількість військовозобов'язаних, заброньованих за підприємством.
1.4	Відомості про стан мобілізаційної підготовки, рівня мобілізаційної готовності підприємства.
1.5	Відомості щодо методичного та інформаційного забезпечення розроблення мобілізаційних планів.
1.6	Відомості про виділення будівель, споруд, земельних ділянок, транспортних та інших матеріально-технічних засобів Збройним Силам України, іншим військовим формуванням в особливий період.
1.7	Відомості про виконання законів, інших нормативно-правових актів з питань мобілізаційної підготовки та мобілізації.

1.8	Відомості про довгострокові та річні програми мобілізаційної підготовки.
1.9	Відомості про заходи мобілізаційної підготовки та мобілізаційного плану щодо життєзабезпечення населення в особливий період.
1.10	Відомості, які містяться в експлуатаційній документації на програмні засоби та комплексну систему захисту інформації в автоматизованих системах із питань мобілізаційної підготовки національної економіки.
1.11	Відомості про дислокацію, характеристики запасних пунктів управління, обсяги матеріально-технічних засобів, продовольства, систему їх охорони та захисту.
1.12	Відомості про структуру мобілізаційного плану підприємства.
1.13	Відомості про заходи основних робіт керівного складу за ступенями готовності підприємства, установи і організації та терміни їх виконання.
1.14	Відомості про організаційно-штатну структуру та штатний розпис органу управління, підприємства, установи і організації на особливий період.
1.15	Відомості за окремими показниками про організацію оповіщення, зв'язку, управління мобілізацією, порядку термінів виконання заходів у разі введення ступенів готовності, переведення підприємства з мирного на воєнний стан.
1.16	Відомості за окремими показниками про потребу, плани асигнувань фактичні витрати на мобілізаційну підготовку в цілому щодо підприємства.
<b>2 Цивільний захист</b>	
2.1	Відомість про заходи основних робіт керівного складу за ступенями готовності підприємства, установи, організації та терміни їх виконання.
<b>3 Відомості щодо організації та забезпечення літерних рейсів</b>	
3.1	Інструкцію щодо організації та забезпечення літерних рейсів у Державному підприємстві «Міжнародний аеропорт «Бориспіль»
<b>4 Режимно-секретна діяльність</b>	
4.1	Номенклатура посад працівників підприємств, організацій, перебування на яких потребує оформлення допуску до державної таємниці
4.2	Накази щодо допуску працівників до державної таємниці.
4.3	Облікові картки громадянина про надання допуску до державної таємниці.
4.4	Листування з питань надання або скасування допуску працівників до державної таємниці.
4.5	Номенклатура секретних справ.
4.6	Акти перевірок наявності документів з грифом обмеження доступу, стану режимно-секретної діяльності, за винятком інформації, що становить державну таємницю
4.7	Перелік режимних приміщень та їх місце розташування.
4.8	Рішення державного експерта з питань таємниць про віднесення (або продовження терміну дії рішення) інформації до державної таємниці.
4.9	Висновок державного експерта з питань таємниць про зміну ступеня секретності інформації.
4.10	Облікові журнали з питань секретного діловодства, акти на знищення носіїв секретної інформації.
4.11	Статистична звітність про стан охорони державної таємниці.
4.12	Листування з питань технічного захисту інформації: а) акти обстеження, категоріювання приміщень та об'єктів інформаційної діяльності; б) відомості про загальний стан технічного захисту інформації; в) технічна документація комплексної системи захисту інформації.
4.13	Відомості, що розкривають систему охорони, пропускний та внутрішньооб'єктовий режим, технічне оснащення конкретного об'єкта, який охороняється.
4.14	Листування з питань застосування окремих статей «Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого

	самоврядування, на підприємствах, в установах і організаціях» (постанова КМУ від 18.12.2013 р. № 939).
4.15	Листування з питань організації, ведення режимно-секретної роботи та спецзв'язку, які не становлять державної таємниці.
<b>5 Діяльність у сфері інформаційних технологій</b>	
5.1	Відомості з питань технічного захисту інформації, вимога щодо захисту якої встановлена законодавством, якщо вони розкривають норми (вимоги) та методики контролю технічного захисту інформації, крім тих, що становлять державну таємницю.
5.2	Відомості 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.
5.3	Відомості 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.
5.4	Відомості про планування, організацію та аналіз результатів контрольно-інспекційної роботи з питань технічного захисту інформації, вимога щодо захисту якої встановлена законодавством.
5.5	Відомості про організацію та аналіз заходів оцінки стану захищеності державних інформаційних ресурсів в інформаційних (автоматизованих), телекомунікаційних чи інформаційно-телекомунікаційних системах, а також про результати цієї оцінки та результати державної експертизи у сфері технічного захисту інформації, крім тих, що становлять державну таємницю
5.6	Відомості про результати перевірок додержання суб'єктами господарювання ліцензійних умов провадження господарської діяльності у галузі технічного захисту інформації, вимога щодо захисту якої встановлена законом (крім тих, що належать до державної таємниці), а також умов проведення робіт із технічного захисту інформації для власних потреб, щодо окремого об'єкта інформаційної діяльності, інформаційної (автоматизованої), телекомунікаційної чи інформаційно-телекомунікаційної системи.
5.7	Відомості 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.
5.8	Відомості про зміст проектів нормативно-правових актів і нормативних документів у сфері технічного захисту інформації, а також матеріалів, що їх супроводжують у процесі розроблення до затвердження документів і введення їх в дію, якщо необхідність цього визнана розробником.
5.9	Загальні відомості, що розкривають сферу нормативного регулювання відомчих нормативно-правових актів і нормативних документів з питань технічного захисту інформації (у тому числі назва документа, який введений в дію), якщо ці відомості

	не становлять державної таємниці.
5.10	Відомості про технічний захист інформації з обмеженим доступом, що не становлять державну таємницю щодо: <ul style="list-style-type: none"> <li>- обмеження, категоріювання приміщень та об'єктів інформаційної діяльності, інформаційно-телекомунікаційних систем і копіювально-розмножувальної техніки;</li> <li>- експлуатації автоматизованих систем для обробки інформації з обмеженим доступом;</li> <li>- проведення вимірювань комплексних систем захисту інформації автоматизованих систем для обробки інформації з обмеженим доступом;</li> <li>- експертних висновків комплексної системи захисту інформації в автоматизованих системах</li> </ul>
5.11	Відомості щодо забезпечення абонентів ДП МА «Бориспіль» урядовим зв'язком.
5.12	Відомості, що розкривають систему охорони, пропускний та внутрішньо об'єктовий режим, технічне оснащення конкретного об'єкта, який охороняється.
5.13	Інформація щодо системи забезпечення кібернетичної безпеки інформаційно-телекомунікаційних систем, якщо вони розкривають технологічні схеми інформаційних (автоматизованих), телекомунікаційних чи інформаційно-телекомунікаційних систем (схеми захисту, принципи побудови, параметри) та/або розголошення яких може призвести до негативних наслідків у сфері національної безпеки і оборони.