

ЗАТВЕРДЖЕНО

Наказ НУЦЗ України

10.09.2020 № 118

ПОЛОЖЕННЯ

про сектор технічного захисту інформації
центру навчально-інформаційних технологій та телекомунікаційних систем
Національного університету цивільного захисту України

1. Загальні положення

1.1. Це положення визначає правовий статус сектору технічного захисту інформації центру навчально-інформаційних технологій та телекомунікаційних систем Національного університету цивільного захисту України (далі – сектор технічного захисту інформації), його завдання, функції, права і обов'язки.

1.2. Сектор технічного захисту інформації є структурним підрозділом центру навчально-інформаційних технологій та телекомунікаційних систем Національного університету цивільного захисту України, та створений з метою реалізації державної політики у сфері технічного захисту інформації (далі – ТЗІ) в університеті.

1.3. Сектор технічного захисту інформації підпорядковується начальнику центру навчально-інформаційних технологій та телекомунікаційних систем.

1.4. У своїй діяльності сектор технічного захисту інформації керується Конституцією і законами України, постановами Верховної Ради України, постановами Кабінету Міністрів України, актами Президента України, державними стандартами України з питань технічного захисту інформації, нормативними документами Адміністрації Держспецзв'язку та захисту інформації України, нормативними документами Державної служби України з надзвичайних ситуацій, Статутом університету, наказами та розпорядженнями ректора університету, Положенням про технічний захист інформації в університеті, а також цим Положенням.

1.5. Працівники сектору технічного захисту інформації призначається на посаду і звільняється з посади наказом ректора університету.

2. Основні завдання

2.1. Організація робіт щодо впровадження заходів ТЗІ на об'єктах інформаційної діяльності (далі – ОІД) та в інформаційно-телекомунікаційних системах (далі – ІТС) університету.

2.2. Здійснення контролю за забезпеченням режиму секретності під час обробки секретної інформації в автоматизованих системах університету.

2.3. Аналіз функціонування ОІД, ІТС університету з метою визначення загроз інформації і розробка заходів захисту інформації.

2.4. Участь у розробці заходів щодо забезпечення режиму секретності під час обробки секретної інформації в автоматизованих системах університету.

2.5. Участь у розробленні плану захисту секретної інформації в автоматизованих системах.

2.6. Участь у розробці посадових інструкцій, організаційно-технічних, розпорядчих та інших документів, що регламентують технологію обробки секретної інформації в автоматизованих системах університету.

2.7. Участь у підготовці та проведенні навчань з питань технічного захисту інформації працівників університету.

2.8. Участь у здійсненні контролю за дотриманням режиму секретності в автоматизованих системах університету.

2.9. Участь у розслідуванні порушень вимог законодавства у сфері ТЗІ та підготовка пропозицій щодо попередження в майбутньому подібних випадків.

2.10. Підготовка пропозицій для комісії з питань ТЗІ щодо шляхів реалізації вимог нормативно-правових актів з питань ТЗІ.

2.11. Здійснення супроводу комплексних систем захисту інформації (далі – КСЗІ) в ІТС університеті.

2.12. Здійснення супроводу державної експертизи КСЗІ в ІТС університету.

2.13. Організація проведення чергових випробувань та атестацій комплексів ТЗІ на ОІД університету.

2.14. Участь у розробці та контролі за виконанням плану забезпечення режиму секретності на період перебування іноземних громадян в університеті.

3. Функції

3.1. Розробляє план робіт із технічного захисту інформації в ІТС, впровадження заходів, спрямованих на його реалізацію.

3.2. Збирає, вивчає та аналізує дані про стан ТЗІ.

3.3. Супроводжує створення, впровадження та функціонування КСЗІ у частині захисту інформації від несанкціонованого доступу, на всіх етапах життєвого циклу ІТС, забезпечує належне функціонування КСЗІ у процесі роботи ІТС.

3.4. Підтримує необхідний рівень захищеності інформаційних ресурсів та технологій в ІТС;

3.5. Контролює виконання користувачами автоматизованих систем де обробляється інформація з обмеженим доступом вимог, норм, правил, інструкцій щодо захисту інформації.

3.6. Розробляє проекти розпорядчих документів, згідно з якими повинен забезпечуватися технічний захист інформації в ІТС.

4. Права і обов'язки

Сектор для виконання покладених на нього завдань має право в установленому порядку:

4.1. Вимагати від усіх працівників університету виконання вимог законодавства у сфері ТЗІ.

4.2. Одержувати в установленому порядку від структурних підрозділів університету відомості, документи та інші матеріали, необхідні для вирішення питань і виконання функцій, що пов'язані з роботою сектору.

4.3. Залучати спеціалістів університету до здійснення заходів щодо ТЗІ.

4.4. Мати безперешкодний доступ до службових приміщень, де функціонують або зберігаються засоби захисту інформації та до інформації, що стосується питань захисту інформації.

4.5. Готувати роз'яснення, інформацію та вказівки структурним підрозділам університету з питань ТЗІ.

4.6. Брати участь у розслідуванні порушень вимог законодавства у сфері ТЗІ.

5. Взаємодія з іншими структурними підрозділами

5.1. Сектор в межах наданих повноважень здійснює взаємодію із структурними підрозділами університету з питань, які належать до його компетенції.

5.2. У процесі виконання завдань сектор взаємодіє зі структурними підрозділами територіальних управлінь та апарату ДСНС за напрямом ТЗІ.

6. Організація роботи

6.1. Сектор технічного захисту інформації провадить свою діяльність на основі квартальних планів роботи центру навчально-інформаційних технологій та телекомунікаційних систем та річного плану робіт із технічного захисту інформації в ІТС.

6.2. Штат сектору технічного захисту інформації затверджується наказом ДСНС.

6.3. Посадові інструкції працівників сектору технічного захисту інформації затверджуються наказом ректора.

7. Керівництво

7.1. Сектор технічного захисту інформації очолює начальник сектору технічного захисту інформації, який призначається на посаду і звільняється з посади наказом ректора.

7.2. Начальник сектору технічного захисту інформації безпосередньо підпорядковується начальнику центру навчально-інформаційних технологій та телекомунікаційних систем.

7.3. Під час відсутності начальника сектору технічного захисту інформації його обов'язки виконує інженер сектору технічного захисту інформації.

7.4. Права, обов'язки, відповідальність начальника сектору технічного захисту інформації:

7.4.1. Здійснює керівництво діяльністю сектору технічного захисту інформації. Відповідає за забезпеченням принципу єдиноначальності в службовій діяльності

7.4.2. Організовує роботу сектору технічного захисту інформації згідно з планами роботи, контролює їх виконання.

7.4.3. Здійснює контроль за роботою працівників сектору технічного захисту інформації.

7.4.4. Здійснює контроль за забезпеченням режиму секретності під час обробки секретної інформації в автоматизованих системах.

7.4.5. Постійно працює з відомостями, що становлять державну таємницю, а саме: про загрози або можливі шляхи реалізації загроз для секретної інформації, що циркулює на ОІД або обробляється в ІТС; за окремими показниками про планування, організацію запровадження заходів, фактичний стан, наявність недоліків в організації технічного захисту секретної інформації, володіння якими дає змогу ініціювати витік секретної інформації на ОІД, ІТС де циркулює секретна інформація зі ступенем секретності «Таємно»; за окремими показниками про організацію, результати перевірок ефективності технічного захисту секретної інформації, що циркулює на ОІД або в конкретній інформаційній (автоматизованій), телекомунікаційній чи ІТС зі ступенем секретності: «Таємно» (ст. ст. 4.11.5, 4.11.9, 4.11.11 ЗВДТ).

7.4.6. Несе персональну відповідальність за організацію та результати своєї діяльності.

7.4.7. Відповідає за стан дисципліни та законності в секторі.

7.4.8. Відповідає за стан соціально – гуманітарної роботи в секторі.

7.4.9. Забезпечує дотримання працівниками сектору вимог Закону України «Про охорону праці», техніки безпеки та додержання ними правил внутрішнього розпорядку.

7.4.10. Здійснює контроль за експлуатаційно-технічним станом засобів технічного захисту інформації.

7.5. На посаду начальника сектору технічного захисту інформації призначається особа, яка має ступінь вищої освіти магістра відповідної спеціальності та стаж роботи у сфері телекомунікаційних технологій не менше трьох років.

Начальник сектору технічного захисту інформації
центру навчально-інформаційних технологій
та телекомунікаційних систем



Олександр БУДАНОВ