ЗАТВЕРДЖЕНО

Наказ від 26 січня 2015 року

№ 1-од

ПОЛОЖЕННЯ

з порядку побудови та впровадження комплексної системи захисту інформації інформаційно-телекомунікаційної системи в Крижопільському районному суді Вінницької області

Загальні положення

Положення з порядку побудови та впровадження комплексної системи захисту інформації інформаційно-телекомунікаційної системи (далі - Положення) визначає порядок побудови та впровадження комплексної системи захисту інформації інформаційно-телекомунікаційної системи, містить необхідні вимоги щодо забезпечення виконання законодавства в сфері технічного захисту інформації, яка належить до державних інформаційних ресурсів, та обробляється із використанням ресурсів інформаційно-телекомунікаційної системи.

Це Положення є обов'язковими для ознайомлення і дотримання особами, які здійснюють діяльність пов'язану з побудовою та впровадженням комплексної системи захисту інформації інформаційно-телекомунікаційної системи

1. Визначення понять

Захист інформації в автоматизованій системі (далі – АС) — діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Обробка інформації в АС — виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Обчислювальна система (далі - ОС) — сукупність програмних-апаратних засобів, призначених для обробки інформації.
Автоматизована система (далі - АС) — організаційно-технічна система, що реалізує інформаційну технологію і об'єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється.

Інформаційна (автоматизована) система — організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Телекомунікаційна система — сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Інформаційно-телекомунікаційна система (далі - ІТС) — сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Безпека інформації — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Політика безпеки інформації — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Комплексна система захисту інформації (далі - КСЗІ) — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Комплекс засобів захисту (далі - КЗЗ) — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Технічний захист інформації (далі - ТЗІ) — вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

2. Обґрунтування необхідності створення КСЗІ

2.1 Необхідність створення КСЗІ ІТС є вимогою чинного законодавства, що встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, зокрема:

- Нормативний документ системи технічного захисту інформації (далі – НД ТЗІ) НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" пункт 6.1.1;
- Закон України "Про інформацію" стаття 3;
- Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" стаття 8;
- Закон України "Про захист персональних даних" стаття 24;
- Закон України "Про доступ до публічної інформації" розділ 2;
- Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 року № 373 зі змінами та доповненнями пункти 4-6, 9, 13, 16;
- Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію, затверджена постановою Кабінету Міністрів України від 27 листопада 1998 року № 1893 (зі змінами та доповненнями) пункт 18;
- Порядок підключення до глобальних мереж передачі даних, затверджений постановою Кабінету Міністрів України від 12 квітня 2002 року № 522 (зі змінами та доповненнями) пункт 10;
- НД ТЗІ 2.5-010-03 "Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу" пункти 5.3 – 5.6.

3. Види інформації, що потребують обмеження доступу або забезпечення цілісності, доступності, конфіденційності відповідно до вимог нормативно-правових актів

Захисту в ІТС під час здійснення автоматизованого оброблення, підлягають такі види інформації:

- відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність судової системи України, яка оприлюднюється в інтернеті, інших глобальних інформаційних мережах і системах та передається телекомунікаційними мережами;
- інформація, вимога щодо захисту якої встановлена законодавством;
- службова інформація.

3.1 **Відкрита інформація, та інформація, вимога щодо захисту якої встановлена законом,** під час обробки в системі повинна зберігати зазначені властивості, що досягається шляхом забезпечення захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

3.2 Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. До такої інформації відноситься:

- Інформація загального електронного діловодства (публічна інформація, яка не підлягає сторонньому ознайомленню в процесі її створення та обробки, доступ до якої дозволяється виключно співробітникам в рамках їх облікових записів в ІТС та Єдиній судовій інформаційній системі України (далі – ЄСІС));
- Технологічна інформація функціонування компонентів ІТС (інформація доступ до якої обмежено виключно адміністративним персоналом ІТС).

3.3 **Службова інформація** - інформація профільної діяльності, що обробляється ресурсами ІТС та становить внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і

передують публічному обговоренню та/або прийняттю рішень. Документам, що містять таку інформацію, може бути надано найвищий ступінь обмеження доступу, в порядку визначеному законодавством. Під час обробки в системі інформація повинна зберігати конфіденційність, цілісність, доступність.

3.4 Модифікувати або знищувати службову інформацію можуть лише визначені користувачі, яким надано відповідні повноваження, до такої інформації може бути віднесено:

- інформацію електронного судового діловодства;
- інформацію судової статистики;
- обліково-фінансову інформацію діяльності господарського забезпечення;
- технологічну інформацію обліку користувачів та їх повноважень в ІТС та ЄСІС (інформація, доступ до якої обмежено виключно персоналом забезпечення політики безпеки в ІТС, ступінь обмеження доступу до даних відомостей визначається найвищим ступенем інформації, яка обробляється в рамках компонентів ІТС - бази даних автентифікації, інформація облікових записів користувачів в ІТС та ЄСІС).

4. Оцінки можливих переваг при створенні КСЗІ ІТС.

4.1 Побудова комплексної системи захисту інформації в інформаційно-телекомунікаційній системі забезпечить створення необхідних умов для здійснення заходів з реалізації державної політики в сфері інформатизації суспільства, створить умови для забезпечення збереження Державних інформаційних ресурсів, надання користувачам достовірної інформації з питань судочинства в Україні.

4.2 Реалізація побудови КСЗІ ІТС у відповідності до організаційно-технічних рішень, що мають експертні висновки Державної служби спеціального зв'язку та захисту інформації України від 1 жовтня 2013 року № 468 (ІТС типу 1) та від 15 жовтня 2013 року № 471 (кінцевий вузол) дасть змогу отримати атестат відповідності ІТС Крижопільському районному суду Вінницької області без організації та здійснення комплексу робіт по розробленню технічної, нормативно-розпорядчої документації та проведення Державної експертизи в сфері технічного захисту інформації, що значною мірою економить витрати і дає змогу забезпечити виконання законодавства за визначеним напрямком, та реалізувати Концепцію галузевої програми інформатизації судів загальної юрисдикції, інших органів та установ судової системи.

5. Прикінцеві положення

5.1 Здійснити побудову та впровадження комплексної системи захисту інформації інформаційно-телекомунікаційної системи Крижопільського районного суду у відповідності до організаційно-технічних рішень що мають експертні висновки Державної служби спеціального зв'язку та захисту інформації України від 1 жовтня 2013 року № 468 (ІТС тип 1) та від 15 жовтня 2013 року № 471 _____ (кінцевий вузол).

5.2 Відповідальній особі за координацію побудови та впровадження і подальше супроводження комплексної системи захисту інформації інформаційно-телекомунікаційної системи здійснити заходи з побудови та впровадження комплексної системи захисту інформації, в своїй роботі керуватись нормативно-розпорядчою документацією організаційно-технічних рішень та законодавством України в сфері технічного захисту інформації.