КРЕМЕНЧУЦЬКА РАЙОННА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ПОЛТАВСЬКОЇ ОБЛАСТІ

РОЗПОРЯДЖЕННЯ

15.06.2023 м. Кременчук № 132

Про затвердження Положення
про службу захисту інформації
в автоматизованих системах класу "1".

Відповідно до вимог Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", постанови Кабінету Міністрів України від 26.03.2006 року №373 "Про Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах", на виконання розпорядження голови райдержадміністрації від 15.06.2023 №. 127 «Про створення служби захисту інформації в автоматизованій системі класу "1" в райдержадміністрації" та з метою проведення заходів із створення та впровадження комплексної системи захисту інформації в автоматизованих системах класу "1", яка призначені для обробки інформації зі ступенем обмеження доступу "Для службового користування":

1.Затвердити Положення про службу захисту інформації в аавтоматизованих системах класу «1».

2. Контроль за виконанням розпорядження залишаю за собою.

Голова районної
державної адміністрації Олег ЛЄДНІК

ЗАТВЕРДЖЕНО
Розпорядження голови
райдержадміністрації
15.06.2023 № 192

Положення
про службу захисту інформації в автоматизованої системі класу "1"

1. Положення про службу захисту інформації (далі - Положення) на об'єкті електронно-обчислювальної техніки Кременчуцької районної державної адміністрації визначає завдання, функції, штатну структуру, повноваження та відповідальність служби захисту інформації, взаємодію з іншими підрозділами та зовнішніми організаціями.

2. Терміни, що вживаються, мають таке значення:
АС – автоматизована система;
АС1-ДСК – автоматизована система для роботи з документами ДСК;
СЗІ – служба захисту інформації;
КСЗІ – комплексна система захисту інформації;
НСД- несанкціонований доступ;
РСО – режимно секретний орган.

3. У зв'язку з умовами функціонування та порядком експлуатації АС, які визначаються відповідно до статті 8 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та пункту 18 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 N 373, окрема служба захисту інформації в АС райдержадміністрації не створюється. Здійснення обов'язків СЗІ в АС покладаються на особу, яка призначається розпорядженням голови райдержадміністрації.

На час відсутності особи, на яку покладено здійснення обов'язків СЗІ (у зв'язку з відпусткою, службовим відрядженням, хворобою тощо), його обов'язки тимчасово виконує інша визначена керівником райдержадміністрації особа.

4. У своїй роботі СЗІ взаємодіє з РСО, а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби до виконання робіт можуть залучатися зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації (за їх згодою).

5. Завданнями СЗІ є:

1) захист прав щодо безпеки інформації в АС класу "1" в процесі інформаційної діяльності та внутрішньої взаємодії;

2) дослідження технології обробки інформації в АС з метою виявлення загроз для безпеки інформації, участь у формуванні моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

3) організація та координація робіт, пов'язаних із забезпеченням захисту інформації, необхідність захисту якої визначається чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;

4) участь у розробленні проектів розпорядчих документів, згідно з якими повинен забезпечуватися захист інформації в АС класу "1";

5) організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу АС;

6) участь в організації підвищення кваліфікаційного рівня користувачів АС з питань захисту інформації;

7) організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації в АС класу "1" та проведення контрольних перевірок їх виконання;

8) організація та координація робіт, пов'язаних з захистом інформації під час її обробки в АС класу "1".

6. Функції СЗІ під час створення комплексної системи захисту інформації включають:

1) визначення переліків відомостей, які підлягають захисту в процесі обробки, інших об'єктів захисту в АС, класифікація інформації за вимогами до її конфіденційності або важливості для організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією в АС;

2) участь у розробленні та коригуванні моделі загроз і моделі захисту інформації в АС, політики безпеки інформації в АС;

3) визначення і формування вимог до КСЗІ;

4) організація і координація робіт з проектування та розроблення КСЗІ, безпосередня участь у проектних роботах з створення КСЗІ;

5) підготовка технічних пропозицій, рекомендацій щодо попередження спроб несанкціонованого доступу до інформації під час створення КСЗІ;

6) організація робіт і участь у випробуваннях КСЗІ, проведенні її експертизи;

7) вибір організацій-виконавців робіт з створення КСЗІ (у разі необхідності), здійснення контролю за дотриманням встановленого порядку проведення робіт з захисту інформації, у взаємодії з підрозділом РСО погодження основних технічних і розпорядчих документів, що супроводжують процес створення КСЗІ (технічне завдання, технічний і робочий проекти, програма і методика випробувань, плани робіт та ін.);

8) участь у розробленні розпорядчих документів, які встановлюють правила доступу користувачів до ресурсів АС, визначають порядок, норми, правила з захисту інформації та здійснення контролю за їх дотриманням (інструкцій, положень, наказів, рекомендацій).

8. Функції СЗІ під час експлуатації комплексної системи захисту інформації включають:

1) організацію процесу керування КСЗІ;

2) розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження архіву даних таких подій;

3) вжиття заходів у разі виявлення спроб НСД до ресурсів АС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;

4) забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;

5) спостереження за функціонуванням КСЗІ та її компонентів;

6) підготовку пропозицій щодо удосконалення порядку забезпечення захисту інформації в АС, впровадження нових технологій захисту і модернізації КСЗІ;

7) організацію та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій АС або КСЗІ;

8) участь в роботах з модернізації АС - узгодженні пропозицій з введення до складу АС нових компонентів, нових функціональних завдань і режимів обробки інформації, заміни засобів обробки інформації тощо;

9) забезпечення супроводження і актуалізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їхнього зберігання і тестування;

10) проведення аналітичної оцінки поточного стану безпеки інформації в АС (прогнозування виникнення нових загроз і їх врахування в моделі загроз, визначення необхідності її коригування, аналіз відповідності технології обробки інформації і реалізованої політики безпеки поточній моделі загроз та ін.);

11) негайне втручання в процес роботи АС у разі виявлення атаки на КСЗІ або АС, проведення у таких випадках робіт з викриття порушника;

12) подання звітів керівництву про виконання користувачами АС вимог з захисту інформації;

13) контроль за виконанням персоналом і користувачами АС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації.

9. Функції СЗІ з організації навчання персоналу з питань забезпечення захисту інформації включають:

1) надання у встановленому порядку керівництву пропозицій щодо підвищення кваліфікації адміністраторів та користувачів АС класу "1";

2) участь в організації і проведенні навчання користувачів і персоналу АС правилам роботи з КСЗІ, захищеними технологіями, захищеними ресурсами;

3) взаємодію з державними органами, навчальними закладами, іншими організаціями з питань навчання та підвищення кваліфікації.

10. СЗІ має право:

1) подавати пропозиції керівництву райдержадміністрації щодо призупинення процесу обробки інформації, заборони обробки, зміни режимів обробки тощо у разі виявлення порушень політики безпеки або виникнення реальної загрози порушення безпеки;

2) складати і подавати керівництву організації акти щодо виявлених порушень політики безпеки, готувати рекомендації щодо їхнього усунення;

3) блокувати обліковий запис користувача, якщо в рамках його роботи було зафіксовано загрозу АС;

4) перевіряти дотримання належного рівня інформаційної безпеки в процесі збереження/використання атрибутів доступу користувача;

5) брати участь у будь-яких перевірках компонентів АС;

6) обмежувати права користувачів щодо доступу до послуг АС;

7) брати участь у проведенні службових розслідувань у випадках виявлення порушень та готувати рекомендації щодо їхнього усунення;

8) готувати пропозиції щодо залучення на договірній основі до виконання робіт з захисту інформації інші організації, що мають ліцензії на відповідний вид діяльності;

9) готувати пропозиції щодо забезпечення АС (та КСЗІ в її складі) необхідними технічними і програмними засобами захисту інформації та іншою спеціальною технікою, які дозволені для використання в Україні з метою забезпечення захисту інформації;

10) узгоджувати умови включення до складу АС нових компонентів та подавати керівництву пропозиції щодо заборони їхнього включення, якщо вони порушують прийняту політику безпеки або рівень захищеності ресурсів АС.

11. Особи, на яких покладено здійснення обов'язків СЗІ, за невиконання або неналежне виконання службових обов'язків, допущені ними порушення встановленого порядку захисту інформації в АС несуть дисциплінарну, адміністративну, цивільно-правову, кримінальну відповідальність згідно з законодавством України.

12. СЗІ зобов'язана:

1) організовувати забезпечення повноти та якісного виконання організаційно-технічних заходів з захисту інформації в АС;

2) вчасно і в повному обсязі доводити до користувачів і адміністратора АС інформацію про зміни в галузі захисту інформації, які їх стосуються;

3) перевіряти відповідність прийнятих в АС правил, інструкцій щодо обробки інформації, здійснювати контроль за виконанням цих вимог;

4) здійснювати контрольні перевірки стану захищеності інформації в АС;

5) забезпечувати конфіденційність робіт з монтажу, експлуатації та технічного обслуговування засобів захисту інформації, встановлених в АС;

6) за вказівкою керівництва брати безпосередню участь у проведенні органами, що мають право здійснювати перевірки, перевірок стану захищеності інформації в АС;

7) негайно повідомляти керівництво про виявлені факти реалізації загроз та викриття порушників.

13. Особи, на яких покладено здійснення обов'язків СЗІ, є відповідальними за виконання покладених на них функцій та коректне використання наданих повноважень, зокрема:

1) додержання вимог нормативних документів, що визначають порядок організації робіт з захисту інформації, інформаційних ресурсів та технологій її обробки;

2) повноту та якість розроблення і впровадження організаційно-технічних заходів з захисту інформації в АС, точність та достовірність отриманих результатів і висновків з питань, що належать до компетенції відповідальної особи;

3) дотримання термінів проведення заходів з оцінки стану захищеності інформації в АС;

4) забезпечення захисту програмно-апаратних та інформаційних ресурсів АС;

5) дотримання встановлених процедур відпрацювання штатних ситуацій;

6) виконання розпоряджень голови райдержадміністрації, правил внутрішнього трудового розпорядку, встановленого режиму, правил охорони праці та протипожежної охорони.

14. Особам, на яких покладено здійснення обов'язків СЗІ, забороняється зберігати або ознайомлюватись із інформацією з обмеженим доступом, яка стала їм доступною внаслідок виконання своїх обов'язків.

15. Особи, на яких покладено здійснення обов'язків СЗІ, є відповідальними за якість виконуваних ними робіт з контролю дій користувачів при використанні послуг АС.

У випадку порушення вимог Положення особи, на яких покладено здійснення обов'язків СЗІ, є відповідальними відповідно до чинного законодавства України.

17. СЗІ взаємодіє з:

1) РСО райдержадміністрації;

2) зовнішніми організаціями, які є постачальниками та виконавцями робіт із захисту інформації чи розроблення засобів АС;

3) іншими державними органами у сфері захисту інформації.

Взаємодію з іншими підрозділами з питань, що безпосередньо не пов'язані з захистом інформації, СЗІ здійснює відповідно до доручень керівництва установи.

18. Зміна структури СЗІ здійснюється за розпорядженням голови райдержадміністрації.

19. Засоби захисту інформації та захищені засоби, що використовуються СЗІ при виконанні своїх службових обов'язків, повинні мати одержаний у встановленому порядку документ (сертифікат відповідності, експертний висновок), що засвідчує їхню відповідність вимогам нормативних документів.

20. Матеріально-технічне та інше спеціальне забезпечення СЗІ здійснюється структурними підрозділами райдержадміністрації у встановленому порядку.

Керівник апарату
райдержадміністрації Таміла САМБУР