ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 489

від 21 липня 2025 року

Щодо визначення заходів із запобігання підтоплень в долині р. Зубра

Заслухавши Протокол №1 робочої групи щодо визначення заходів із запобігання підтоплень в долині р.Зубра від 15.07.2025 року про результати обстеження робочою групою та визначення заходів із запобігання підтоплень в долині р. Зубра, яке відбулось 15.07.2025 року в селі Зубра Львівського району Львівської області, керуючись Водним Кодексом України, Кодексом цивільного захисту України, Законами України «Про місцеве самоврядування в Україні», «Про благоустрій населених пунктів» та на виконання протоколу позачергового засідання комісії ТЕБ та НС від 10.07.2025 № 10/07-1, розпорядження голови Солонківської сільської ради «Про створення робочої групу щодо визначення заходів із запобігання підтоплень в долині річка Зубра в межах села Зубра на території Солонківської сільської ради Львівського району Львівської області» від 14.07.2025 № 72-01, у зв'язку із затопленням житлових будинків та об'єктів комунальної інфраструктури внаслідок проходження паводку та з метою попередження надзвичайних ситуацій внаслідок паводків

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ВИРІШИВ:

1. Прийняти до уваги протокол №1 від 15.07.2025 року робочої групи щодо визначення заходів із запобігання підтоплень в долині р. Зубра.
2. Звернутись до Львівської обласної військової адміністрації з проханням розглянути можливість реконструкції мосту в с. Зубра, по вул. Михайла Гориня для збільшення пропускної спроможності русла ріки шляхом підняття рівня мосту на 1 – 1,5 м. спрямлення русла у підмостовому просторі для збільшення кута повороту (більше 90^0).
3. Коригувати проектно-кошторисну документацію «Заходи щодо відновлення і підтримання сприятливого гідрологічного режиму та санітарного стану р.Зубра, а також боротьби з шкідливою дією вод Львівської області. Капітальний ремонт. Коригування» в частині:

- розширення русла ріки, укріплення берегів та влаштування підпірних стінок;
- спрямлення русла у підмостовому просторі для збільшення кута повороту (більше 90^0) під мостом по вул. Михайла Гориня;
- провести розчистку русла від засмічення, провести зрізку аварійних дерев;
- проектом розглянути можливість влаштування акумулюючих водойм.

3. Контроль за виконанням даного рішення покласти на виконавчий комітет Солонківської сільської ради Львівського району Львівської області.

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 490

від 21 липня 2025 року

Про призначення піклувальника над неповнолітньою дитиною, позбавленої батьківського піклування

Відповідно до Закону України «Про місцеве самоврядування в Україні», Сімейного кодексу України, Цивільного кодексу України, статей 1, 3, 6, 8, 11 Закону України «Про забезпечення організаційно-правових умов соціального захисту дітей-сиріт та дітей, позбавлених батьківського піклування», керуючись постановою Кабінету Міністрів України від 24.09.2008 № 866 «Питання діяльності органів опіки та піклування, пов'язаної із захистом прав дитини» (зі змінами), враховуючи заяву від 07.07.2025 року № 02-07/1320 громадянки Білас Марії Ігорівни ХХХ року народження про призначення її піклувальником над неповнолітньою дитиною, позбавленої батьківського піклування ОСОБА1 26.06.2010 року народження. та рішення комісії з питань захисту прав дитини Солонківської сільської ради від 11 липня 2025 року № 278, з метою захисту прав та інтересів дитини,

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ВИРІШИВ:

1. Затвердити висновок комісії з питань захисту прав дитини Солонківської сільської ради про доцільність встановлення піклування та відповідність його інтересам неповнолітньої дитини ОСОБА1 26.06.2010 року народження (додається).

2. Призначити Білас Марію Ігорівну ХХХ року народження піклувальником над неповнолітньою дитиною, позбавленої батьківського піклування ОСОБА1 26.06.2010 року народження.

3. Покласти персональну відповідальність за життя, здоров'я, фізичний та розумовий розвиток ОСОБА1 26.06.2010 року народження на піклувальника Білас Марію Ігорівну.

4. Службі у справах дітей Солонківської сільської ради забезпечити здійснення контролю за захистом прав та інтересів неповнолітньої дитини, позбавленої батьківського піклування ОСОБА1 26.06.2010 року народження, відповідно до чинного законодавства України.

5. Контроль за виконанням даного рішення покласти на виконавчий комітет.

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 491

від 21 липня 2025 року

Про забезпечення функціонування прийомної сім'ї
Пацкана Миколи Миколайовича та Пацкан Галини Петрівни
на території Солонківської сільської ради

Відповідно до ЗУ «Про місцеве самоврядування», ст. 6,12 Закону України «Про забезпечення організаційно-правових умов соціального захисту дітей-сиріт та дітей, позбавлених батьківського піклування», постанови Кабінету Міністрів України від 26.04.2002 № 565 «Про затвердження Положення про прийомну сім'ю (із змінами та доповненнями), постанови Кабінету Міністрів України від 26.06.2019 № 552 «Деякі питання виплати державної соціальної допомоги на дітей-сиріт та дітей, позбавлених батьківського піклування, осіб з їх числа, у тому числі з інвалідністю, грошового забезпечення батькам-вихователям і прийомним батькам за надання соціальних послуг у дитячих будинках сімейного типу та прийомних сім'ях за принципом «гроші ходять за дитиною, оплати послуг із здійснення патронату над дитиною та виплати соціальної допомоги на утримання дитини в сім'ї патронатного вихователя, підтримки малих групових будинків», Постанову Кабінету Міністрів України від 18.06.2025 року № 702 «Про внесення до деяких постанов Кабінету Міністрів України змін щодо здійснення органами опіки та піклування, службами у справах дітей повноважень стосовно організації діяльності дитячих будинків сімейного типу та прийомних сімей», заяву від 16.07.2025 року Пацкан Галини Петрівни ХХХ року народження та Пацкана Миколи Миколайовича ХХХ року народження, з метою захисту законних прав і інтересів дітей:

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ВИРІШИВ:

1.Забезпечити функціонування на території Солонківської сільської ради прийомної сім'ї на базі Пацкан Галини Петрівни ХХХ року народження та Пацкана Миколи Миколайовича ХХХ року народження, за адресою:

Львівська область, Львівський район, с.ХХХ, вул.ХХХ, у якій виховуються діти, позбавлені батьківського піклування: ОСОБА1, 30.12.2007 року народження, ОСОБА2, 19.09.2014 року народження, ОСОБА3 17.03.2011 року народження.

2.Покласти на прийомну матір та батька (прийомних батьків) персональну відповідальність за життя, здоров'я, фізичний і психічний розвиток дітей, позбавлених батьківського піклування:

ОСОБА1, 30.12.2007 року народження, ОСОБА2, 19.09.2014 року народження, ОСОБА3 17.03.2011 року народження.

3.Службі у справах дітей Солонківської сільської ради (Г. Гичка):

3.1.Підготувати проект договору про влаштування ОСОБА1, 30.12.2007 року народження, ОСОБА2, 19.09.2014 року народження, ОСОБА3 17.03.2011 року народження у прийомну сім'ю Пацкан Галини Петрівни ХХХ року народження та Пацкана Миколи Миколайовича ХХХ року народження на виховання і спільне проживання.

3.2.Здійснювати контроль за умовами проживання, виховання дітей в прийомній сім'ї.

3.3. Готувати щорічно до 31 грудня звіт про стан утримання та розвиток дітей в прийомній сім'ї.

4. Відділу у справах ветеранів та соціального захисту населення Солонківської сільської ради (Л. Богун):

4.1.Закріпити за прийомною сім'єю Пацкан Галини Петрівни ХХХ року народження та Пацкана Миколи Миколайовича ХХХ року народження соціального працівника.

4.2.Забезпечити соціальний супровід з надання комплексу послуг, спрямованих на створення належних умов функціонування прийомної сім'ї.

4.3.Подавати Службі у справах дітей Солонківської сільської ради до 30 грудня щорічну інформацію про ефективність функціонування прийомної сім'ї.

5. Комунальному некомерційному підприємству «4-а Міська Поліклініка м. Львова» № 23970286 (М. Павлов):

5.1.Закріпити дільничного лікаря за дітьми.

5.2.Забезпечити проходження дітьми медогляду двічі на рік.

5.3.Подавати службі у справах дітей Солонківської сільської ради щорічно до 30 грудня звіт про стан здоров'я дітей, дотримання прийомними батьками рекомендацій лікаря.

6. Відділу освіти Сихівського та Личаківського районів управління освітньої інфраструктури департаменту освіти та культури ЛМР (Д. Гавриляк):

6.1.Забезпечити право дітей на здобуття освіти, а у разі потреби - забезпечити індивідуальне навчання.

6.2.Подавати Службі у справах дітей Солонківської сільської ради щорічно до 15 листопада звіт про рівень розвитку та знань дітей, наявність у них шкільного одягу та шкільного приладдя, систематичність відвідування уроків та своєчасність і якість виконання домашніх завдань, відвідування дітьми гуртків, секцій, позашкільних заходів, участь прийомної матері у вихованні дітей.

7. Сектору взаємодії громад Львівського районного управління поліції №2 ГУНП у Львівській області (Р. Боянівський):

7.1. Подавати Службі у справах дітей Солонківської сільської ради до 30 грудня щорічний звіт про відсутність проявів асоціальної поведінки з боку дітей, які виховуються в прийомній сім'ї та зі сторони прийомних батьків.

8. Контроль за виконанням цього рішення покласти на виконавчий комітет.

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 492

від 21 липня 2025 року

Про виготовлення проектно-кошторисної документації на «Реконструкція системи газопостачання з монтажем газових котлів у приміщенні теплогенераторної амбулаторії АЗПСМ с. Зубра за адресою: вул. Шкільна, 1-Б, с. Зубра Львівський район Львівська область»

Відповідно до ст.31 Закону України «Про місцеве самоврядування в Україні», «Про архітектурну діяльність», «Про регулювання містобудівної діяльності», заслухавши інформацію начальника відділу капітального будівництва, ЖКГ, транспорту та благоустрою Копача О.Б. щодо необхідності виготовлення проектно-кошторисної документації на «Реконструкція системи газопостачання з монтажем газових котлів у приміщенні теплогенераторної амбулаторії АЗПСМ с. Зубра за адресою: вул. Шкільна, 1-Б, с. Зубра Львівський район Львівська область»,

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ВИРІШИВ:

1. Надати дозвіл на виготовлення проектно-кошторисної документації на «Реконструкція системи газопостачання з монтажем газових котлів у приміщенні теплогенераторної амбулаторії АЗПСМ с. Зубра за адресою: вул. Шкільна, 1-Б, с. Зубра Львівський район Львівська область».

2. Звернутися в сертифіковану проектну організацію з питанням виготовлення проектно-кошторисної документації.

3. Надати дозвіл сільському голові на укладання договору на проектно-кошторисні роботи.

4. Контроль за виконання даного рішення покласти на виконавчий комітет Солонківської сільської ради.

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 493

від 21 липня 2025 року

Про затвердження проектно-кошторисної документації на «Благоустрій території по вул. Шкільна (біля церкви) в с. Зубра Львівського району Львівської області (Капітальний ремонт)»

Відповідно ст.31 Закону України "Про місцеве самоврядування в Україні", статті 7 Закону України «Про архітектурну діяльність», «Про регулювання містобудівної діяльності», ЗУ «Про публічні закупівлі» та Порядку затвердження проектів будівництва і проведення їх експертизи, затвердженого постановою Кабінету Міністрів України від 11.05.2011 № 560 та на підставі позитивного експертного звіту ТОВ «УКРЕКСПЕРТИЗА ГРУП» №ЛВ 0085-5957-25/УЕГ/Г від 18 липня 2025р. по проекту «Благоустрій території по вул. Шкільна (біля церкви) в с. Зубра Львівського району Львівської області (Капітальний ремонт)»,

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ ВИРІШИВ:

1. Затвердити проектно-кошторисну документацію за робочим проектом «Благоустрій території по вул. Шкільна (біля церкви) в с. Зубра Львівського району Львівської області (Капітальний ремонт)», з такими техніко-економічними показниками:

Об'єкт	ТЕП			
Територія по вул. Шкільна(біля церкви) в с. Зубра Львівського району Львівської області Тип: Лінійний об’єкт інженерно-транспортної інфраструктури Код ДКБС: 2112.5 Майдани, тротуари та пішохідні зони Вид будівництва: Капітальний ремонт Примітка до періоду будівництва: не вказано	Показник	Значення	Примітка	За чергами і п.к.
	Тривалість будівництва, міс	2		
	Довжина проектованої ділянки, м	66.22		
	Мінімальний радіус, м	6	Мінімальний радіус в плані	
	Загальна площа покриття, в тому числі, м^2	153		
	Поздовжній ухил проїзної частини, ‰,	77		
	у тому числі:	106	Площа покриття тротуару	

	у тому числі:	47	Площа покриття поширення проїзної частини	
	Ширина, м	1.5	Ширина тротуару	

Показники		Од. вим.	Вартість
Загальна кошторисна вартість будівництва у поточних цінах станом на «18» червня 2025р. складає всього:		тис. грн.	1 039,082
у тому числі:	- будівельні роботи	тис. грн.	790,222
	- устаткування	тис. грн.	-
	- інші витрати	тис. грн.	248,860

2. Контроль за виконанням даного рішення покласти на виконавчий комітет Солонківської сільської ради.

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 494

від 21 липня 2025 року

Про внесення змін до складу робочої групи з питань забезпечення детінізації економіки Солонківської сільської ради

Керуючись Законом України "Про місцеве самоврядування в Україні», рішення виконавчого комітету Солонківської сільської ради від 08.02.2022 року №44 «Про створення робочої групи з питань забезпечення детінізації економіки Солонківської сільської ради та затвердження Положення про робочу групу» у зв'язку із змінами в штаті,

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ВИРІШИВ:

1. Внести зміни до складу робочої групи з питань забезпечення детінізації економіки Солонківської сільської ради (далі Робоча група) згідно з додатком 1.
2. Скликати засідання Робочої групи за результатами моніторингу податкової заборгованості в розрізі категорій місцевих податків та зборів.
3. Контроль за виконанням цього рішення покласти виконавчий комітет.

Сільський голова **Богдан ДУБНЕВИЧ**

Додаток 1
до рішення виконавчого комітету
Солонківської сільської ради
від 21.07.2025 року № 494

СКЛАД
робочої групи з питань забезпечення детінізації економіки
Солонківської сільської ради

№ п/п	Прізвище, ім'я та по батькові	Посада
1.	Кечур Оксана Дмитрівна	Секретар ради, голова робочої групи
2.	Зайльо Марія Ярославівна	Керуюча справами виконавчого комітету, заступник голови робочої групи
3.	Світлик Наталія Ярославівна	Головний спеціаліст фінансового відділу, секретар робочої групи
Члени робочої групи:		
4.	Ширій-Ярема Ірина Ігорівна	Начальник юридичного відділу
5.	Гавриляк Руслана Григорівна	Начальник фінансового відділу
6.	Гладковська Оксана Іванівна	Начальник ЦНАПУ
7	Лещук Богдан Йосипович	Начальник земельного відділу
8.	Баркит Богдан Володимирович	Староста Поршнянського старостинського округу
9.	Бучок Андрій Степанович	Староста Зубрянського старостинського округу
10.	Домбровська Галина Зіновіївна	Староста Жирівського старостинського округу
11.	Нагірний Петро Євгенович	Староста Вовківського старостинського округу
12.	Скіп Тетяна Степанівна	Староста Раковецького старостинського округу
13.	Приступа Ольга Василівна	Головний спеціаліст відділу міжнародного територіального співробітництва та економічного розвитку громади

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 495

від 21 липня 2025 року

Про виготовлення проектно-кошторисної документації на «Благоустрій території біля будинків №58–59 по вул.Центральна в с. Раковець Львівського району Львівської області (Капітальний ремонт)»

Відповідно до ст.31 Закону України «Про місцеве самоврядування в Україні», «Про архітектурну діяльність», «Про регулювання містобудівної діяльності», заслухавши інформацію головного спеціаліста відділу капітального будівництва, ЖКГ, транспорту та благоустрою Рихліцький В. В. щодо необхідності виготовлення проектно-кошторисної документації на «Благоустрій території біля будинків №58–59 по вул. Центральна в с. Раковець Львівського району Львівської області (Капітальний ремонт)»,

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ВИРІШИВ:

1. Надати дозвіл на виготовлення проектно-кошторисної документації на «Благоустрій території біля будинків №58–59 по вул. Центральна в с. Раковець Львівського району Львівської області (Капітальний ремонт)».

2. Звернутися в сертифіковану проектну організацію з питанням виготовлення проектно-кошторисної документації.

3. Надати дозвіл сільському голові на укладання договору на проектно-кошторисні роботи.

4. Контроль за виконання даного рішення покласти на виконавчий комітет Солонківської сільської ради.

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 496

від 21 липня 2025 року

Про виготовлення проектно-кошторисної документації на «Благоустрій території біля громадського простору по вул. Стрийська в с.Деревач Львівського району Львівської області (Капітальний ремонт)»

Відповідно до ст.31 Закону України «Про місцеве самоврядування в Україні», «Про архітектурну діяльність», «Про регулювання містобудівної діяльності», заслухавши інформацію головного спеціаліста відділу капітального будівництва, ЖКГ, транспорту та благоустрою Рихліцький В. В. щодо необхідності виготовлення проектно-кошторисної документації на «Благоустрій території біля громадського простору по вул. Стрийська в с. Деревач Львівського району Львівської області (Капітальний ремонт)»,

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ ВИРІШИВ:

1. Надати дозвіл на виготовлення проектно-кошторисної документації на «Благоустрій території біля громадського простору по вул. Стрийська в с.Деревач Львівського району Львівської області (Капітальний ремонт)».

2. Звернутися в сертифіковану проектну організацію з питанням виготовлення проектно-кошторисної документації.

3. Надати дозвіл сільському голові на укладання договору на проектно-кошторисні роботи.

4. Контроль за виконання даного рішення покласти на виконавчий комітет Солонківської сільської ради.

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 497

від 21 липня 2025 року

На виконання ключових законодавчих актів України у сфері кібербезпеки, а саме законів України «Про інформацію», «Про захист інформації в інформаційнокомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», Указу Президента України від 26.08.2021 №447/2021 «Про Стратегію кібербезпеки України», а також наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.01.2025 № 54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту», доручення начальника Львівської обласної військової адміністрації від 16.07.2025 № 39/0/6-25ВА щодо підвищення стану кіберзахищеності територіальних громад Львівської області, листа заступника голови ЛОДА з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO) Олександра Кулепіна від 18.07.2025 року №01-01/1278 «Щодо підвищення стану кіберзахищеності територіальних громад Львівської області»

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ВИРІШИВ:

1. Затвердити Політику інформаційної безпеки Солонківської сільської ради (додаток 1).
2. Затвердити бланк Плану реагування на кіберінциденти (додаток 2).
3. Інспектору з інформаційних технологій:

3.1. До 30.09.2025 забезпечити підключення органу місцевого самоврядування до платформи обміну індикаторами компрометації MISP CERT-UA та адаптованого програмного продукту MISP-UA.

3.2. Провести оцінку та визначення поточного профілю кіберзахисту Солонківської сільської ради відповідно до Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту, затверджених наказом Адміністрації

Держспецзв’язку від 30.01.2025 № 54
3.3. До 30.09.2025 забезпечити проведення самодіагностики профілю кіберзахисту, шляхом заповнення Google – форми за посиланням: https://forms.gle/7nbaz8xsCQxdVbRE9 .
3.4. До 15.10.2025 проінформувати управління з питань цифрового розвитку Львівської обласної державної адміністрації про виконання заходів кіберзахисту.
4. Секретарю виконавчого комітету:
4.1. Довести дане рішення до відповідальних осіб за інформаційну безпеку Солонківської сільської ради шляхом отримання підпису.
4.2. Оприлюднити дане рішення на офіційному сайті сільської ради.
5. Відповідальним особам за інформаційну безпеку ознайомити підлеглих з «Політикою інформаційної безпеки Солонківської сільської ради»
6. Контроль за виконанням даного рішення покласти на виконавчий комітет.

Сільський голова **Богдан ДУБНЕВИЧ**

Додаток 1
до рішення виконавчого комітету
Солонківської сільської ради
від 21.07.2025 року №479

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ

Зміст

1. Загальні положення

Політика інформаційної безпеки Солонківської сільської ради (далі – Політика) визначає загальні вимоги до інформаційної безпеки у Солонківській сільській раді (далі – СР), основні принципи, цілі та завдання управління інформаційною безпекою СР.

Дана Політика є обов'язковим документом для ознайомлення при прийомі на роботу та є доступною для ознайомлення будь-якому співробітникові СР або третій стороні.

Ця Політика є офіційно прийнятою Керівництвом СР системою поглядів на проблеми забезпечення інформаційної безпеки, встановлює принципи побудови процесів управління інформаційною безпекою на основі систематизованої розробки та впровадження політик, положень, регламентів, стандартів, інструкцій та інших нормативних документів в області інформаційної безпеки.

Метою даної Політики є:

- Забезпечення захисту інформаційних ресурсів СР від зовнішніх і внутрішніх загроз;
- Безперервність роботи всіх служб і сервісів СР;
- Мінімізація ризиків операційної діяльності СР;
- Створення позитивної репутації СР при взаємодії з третіми сторонами;
- Відповідність законодавству України та вимогам контролюючих органів в області інформаційної безпеки та захисту персональних даних.

Дана Політика поширюється на всі процеси діяльності СР та є обов'язковою для виконання всіма співробітниками СР. Порушення вимог Політики тягне за собою дисциплінарну відповідальність та відповідальність згідно з чинним законодавством України.

2. Терміни та визначення

Власник ІА – співробітник СР, який несе відповідальність за: забезпечення належної класифікації інформації та активів, пов'язаних із засобами обробки інформації; визначення та періодичний перегляд обмежень доступу і класифікацій; управління конкретними ризиками, пов'язаними з активом, і визначення пов'язаних потреб в безпеці.

Внутрішній аудит – аудит ІБ, що проводиться співробітниками СР, відповідно навченими та незалежним від контролюючої особи.

Вплив – величина збитку, який можна очікувати в результаті наслідків несанкціонованого розкриття інформації, несанкціонованої зміни інформації, несанкціонованого знищення інформації або втрати інформації або порушення доступності інформаційної системи.

Доступність – властивість інформації, яка полягає в тому, щоб бути доступною та використовуватися на вимогу користувача і/або процесу.

Загроза – можлива небезпека, яка може використовувати уразливість в інформаційній системі для порушення цілісності, конфіденційності, доступності системи.

Інформаційна безпека (ІБ) – це практика забезпечення захисту інформаційних активів від загроз, які можуть на них вплинути. Вона включає в себе вичерпний набір засобів управління, які охоплюють різні фактори (людські, фізичні, екологічні та технічні) протягом життєвого циклу інформаційних і технологічних активів, включаючи розробку, створення і впровадження нових систем, підтримка даних і систем, моніторинг використання таких активів, виявлення та реагування на потенційні загрози, дотримання чинних законів і положень про кібербезпеку і конфіденційність, а також виведення з експлуатації ІТ-систем і знищення даних.

Інформаційна система – комп'ютерні системи, програмне забезпечення, телекомунікаційне і периферійне устаткування.

Інформаційний актив (ІА) – обладнання, програмне забезпечення, дані, а також співробітники, які беруть участь в процесах діяльності СР, які визначені і управляються як єдине ціле, щоб його можна було зрозуміти, спільно використовувати, захищати та ефективно керувати. Інформаційні активи мають керовану цінність, ризики, контент і життєві цикли.

Інцидент – це подія, яка не є частиною звичайних операцій і порушує робочі процеси. Інцидент може включати відмову функції або послуги, які повинні були бути надані, або будь-які інші

типи збою операції.
Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.
Користувач – особа або СР, які взаємодіють з інформаційними системами.
Оцінка ризиків – процес виявлення, визначення пріоритетів та аналіз ризиків. Процес включає визначення ступеня, в якому несприятливі обставини або події можуть вплинути на Організацію. Даний процес використовує результати оцінок загроз і вразливостей для виявлення ризиків для діяльності СР і оцінює ці ризики, з точки зору ймовірності виникнення і впливу. Результатом оцінки ризику є список передбачуваних потенційних впливів і явних вразливостей. Оцінка ризиків є частиною процесу управління ризиками.
Політика інформаційної безпеки – набір задокументованих управлінських рішень, створений для захисту інформації СР та пов'язаних з нею ресурсів.
Ризик – ймовірність впливу на діяльність СР (включаючи місію, функції, імідж, репутацію), її активи (ресурси) і співробітників в результаті експлуатації вразливостей інформаційної системи і залежно від потенційного впливу, реалізація загрози і ймовірність її реалізації.
Уразливість – недолік в інформаційній системі, який може бути використаний суб'єктом загрози (наприклад, зловмисником) для виконання несанкціонованих дій в системі і порушення цілісності, конфіденційності, доступності або спостережливості.
Цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.
Шифрування – процес перетворення відкритого тексту в зашифрований з метою безпеки або конфіденційності.
Шкідливе ПЗ – програмне забезпечення, яке вживлюється в систему, як правило, таємно, з метою порушення конфіденційності, цілісності та/або доступності даних, додатків або операційної системи користувача або іншим чином шкодити або заважати роботі користувача.
SMTPS – Simple Mail Transfer Protocol Secure.
Політика інформаційної безпеки

3.1. Управління інформаційною безпекою

Для забезпечення ІБ, необхідно слідувати формальним загальним правилам та процедурам наведеним далі, що покривають відповідне використання ІА СР.
Співробітники СР та відповідні треті сторони (які мають доступ до інформації та/або ресурсів СР) повинні бути проінформовані про необхідність дотримання цієї Політики.
Для забезпечення постійної придатності, адекватності та ефективності ця Політика повинна переглядатися Відповідальною особою за інформаційну безпеку через заплановані проміжки часу – щонайменше раз в рік, якщо впроваджуються суттєві зміни або за рішенням Керівництва СР.
Суттєвими змінами можна вважати:
- Зміни в процесах діяльності СР;
- Зміни в організаційній структурі;
- Зміни в ІТ-інфраструктурі СР тощо.

Відповідно до сфери діяльності СР необхідно також враховувати наступні моменти:
- Законодавство, що регулює сферу діяльності СР та договірні зобов’язання;
- Відповідальність за порушення Політики;
- Обов’язки Керівництва СР та інших осіб щодо безпеки систем та інформації СР.

3.2. Розподіл обов’язків з інформаційної безпеки

Загальна відповідальність за ІБ СР покладається на Керівництво.
Конфліктні обов’язки та сфери відповідальності повинні бути розділені, щоб зменшити можливості для несанкціонованих або ненавмисних змін чи зловживання ІА СР.

Формальне розподілення відповідальності Керівництвом СР забезпечує стратегічну прозорість та вплив на практику забезпечення ІБ.
Керівництво відповідальне за:
- Визначення критичних операційних процесів для діяльності СР;
- Прийняття рішень щодо розвитку ІБ СР;
- Затвердження та поширення правил і вимог ІБ в СР;
- Затвердження відповідальності за порушення правил та вимог ІБ;
- Функцію перевірки та контролю виконання в СР правил та вимог ІБ. Додатково

відповідальні та їх обов'язки описані нижче в тілі цієї Політики.

3.3. Безпека людських ресурсів

Перевірка кандидатів перед працевлаштуванням, співробітників чи третіх сторін повинна чітко враховувати чутливість інформації, до якої кандидати отримають доступ, та передбачувані ризики при визначенні характеру та строків цих перевірок.
Призначення на посади та звільнення з посад повинно виконуватися відповідно до державних нормативно-правових актів.
Кожен співробітник СР та третьої сторони, якому надано доступ до систем та/або даних СР, несе відповідальність за безпечне використання систем і даних для цілей діяльності СР та дотримання її політик.
Співробітники та треті сторони несуть відповідальність за повідомлення Керівнику про будь-які сумніви щодо ефективності процесів безпеки, про будь-яку подію чи інцидент щодо несанкціонованого або неправильного використання активів СР.
Обов’язок Керівництва СР вимагати від всіх співробітників та третіх сторін дотримання вимог ІБ СР, відповідно до встановлених політик та процесів, а також контролювати процес їх дотримання.
Припинення трудової діяльності здійснюється згідно з чинним трудовим законодавством України.

3.4. Навчання та обізнаність

Всі співробітники, які є користувачами внутрішньої мережі повинні бути ознайомлені з внутрішніми вимогами щодо роботи з інформаційними активами СР та нести персональну відповідальність за їх дотримання.
Усі співробітники та відповідні треті сторони повинні проходити відповідну підготовку з підвищення обізнаності та регулярно отримувати інформацію про оновлення організаційних політик та процедур відповідно до їх робочих функцій.
Програма обізнаності повинна забезпечувати, щоб усі співробітники досягали та підтримували принаймні базовий рівень розуміння питань ІБ, таких як загальні зобов’язання згідно з різними політиками, стандартами, процедурами, керівними принципами, законами, нормативними актами, контрактними умовами, а також загальноприйнятими стандартами етики та прийнятної поведінки.

3.5. Класифікація та управління інформацією

Інформацію слід класифікувати, визначати та оцінювати ризики відповідно до її конфіденційності, цілісності, доступності та спостережливості, незалежно від носія, на якому вона зберігається і/або обробляється. Чутлива інформація повинна визначатися відповідно до її конфіденційності, цілісності, доступності та спостережливості. Вся інформація, окрім публічної, має визначатися як чутлива.
Незалежно від рівня конфіденційності, вся інформація СР повинна використовуватися належним чином та тільки для дозволених цілей.
Розкриття інформації з обмеженим доступом може здійснюватися лише у законний спосіб зацікавленим особам органів влади, а також фізичним та юридичним особам за згодою СР, з

дотриманням вимог чинного законодавства України та вимог відповідних Договорів.

3.6. Обробка, передача та зберігання даних

Чутливі дані повинні збиратися та зберігатися лише в системах, де є обґрунтована ділова чи технічна потреба. Чутливі виробничі дані повинні бути захищені при зберіганні і/або використанні у системах, і надійно видалятись, коли вони більше не потрібні.

Чутливі дані ніколи не повинні збиратися або використовуватися для цілей, відмінних від тих, для яких дані були зібрані спочатку. Усі параметри збереження даних (періоди, цілі тощо) повинні бути законними та відповідати місцевому та міжнародному законодавству та нормам щодо захисту даних.

3.7. Використання особистих пристроїв

СР може дозволяти співробітникам та іншим авторизованим користувачам своїх систем, послуг та ресурсів використовувати власні пристрої для виконання посадових обов'язків та завдань, які необхідні для забезпечення її безперервної діяльності.

СР повинна розробити та встановити вимоги ІБ щодо використання власних робочих пристроїв та довести їх до відома усіх співробітників та відповідних третіх сторін. Особисту відповідальність має нести кожен співробітник та третя сторона, що використовує персональний пристрій для доступу до систем, послуг та ресурсів СР, щоб забезпечити відповідне використання всіх протоколів безпеки та усіх заходів безпеки.

Кожен пристрій, який використовується для виконання посадових обов'язків та завдань, які необхідні для забезпечення безперервної діяльності СР, тобто для доступу до внутрішньої інформації, повинен використовуватися відповідально та лише в робочих цілях.

3.8. Парольна політика

Відповідно до Парольної політики, для забезпечення надійного захисту інформаційних систем паролем, мають бути встановлені наступні параметри:

- Мінімальна довжина: 4 символи;
- Пароль повинен відповідати вимогам складності: так;
- Повинен містити символи верхнього та (або) нижнього регістру, числа, також може містити неалфавітні символи;
- Не використовувати будь-які персональні дані;
- Не містить у собі загальновживані слова;
- Мінімальний термін дії пароля: 1 день;
- Максимальний термін дії пароля: 30-90 днів;
- Безпечне зберігання паролів: паролі не слід зберігати або передавати у відкритому тексті.

3.9. Використання електронної пошти

Доступ до електронної пошти надається співробітникам СР для виконання своїх службових обов'язків. Використання електронної пошти співробітниками СР в особистих або інших цілях, не пов'язаних з діяльністю СР, заборонено.

В СР заборонено:

− Надсилати повідомлення, що містять чутливу інформацію, а також дані, що містять чутливу інформацію не для виконання своїх службових обов'язків. Забороняється надсилати по електронній пошті логіни, паролі та іншу чутливу інформацію;

− Використовувати електронну пошту для особистих цілей;

− Використовувати електронну адресу для підписки на маркетингові електронні листи без попереднього узгодження з Відповідальною особою за ІБ;

− Відкривати будь-яке вкладення, посилання чи додаток до електронної пошти, де співробітник не має ґрунтовних підстав вважати, що інформація, до якої очікується доступ, надійшла з надійного джерела;

− Надсилати масові розсилки (понад 10) на зовнішні адреси без згоди Керівника співробітника та Відповідальної особи за ІБ;

− Надсилати по електронній пошті матеріали, що містять шкідливе програмне забезпечення чи

інші програми, призначені для порушення, знищення або обмеження функціональних можливостей будь-якого комп'ютерного чи телекомунікаційного обладнання чи інформаційних систем та послуг;
− Надсилати електронною поштою програми, які забезпечують несанкціонований доступ;
− Розповсюджувати за допомогою електронної пошти матеріали, які захищені авторським правом і зачіпають будь-який патент, торгову марку, комерційну таємницю, авторські права або будь-які інші права власності. та/або авторські права або пов'язані з ними права третіх сторін;
− Поширювати через електронну пошту інформацію, заборонену міжнародним та українським законодавством, включаючи матеріали, що є шкідливими, загрозливими, нецензурними, а також інформацію, що порушує честь та гідність інших. Також забороняється надсилати матеріали, що розпалюють національну ворожнечу, підбурюють до насильства, закликають до незаконних дій, включаючи матеріали, що містять інструкції щодо використання вибухових речовин, зброї тощо.
Доступ колишнього співробітника до облікових записів електронної пошти СР повинен бути негайно відключений та деактивований.

3.10. Безпека мережі

Наступні вимоги обов'язкові до виконання:

− Вимоги до конфігурації безпеки повинні бути визначені для всього мережевого обладнання;
− Вимоги до контролю аутентифікації та доступу повинні бути визначені та повинні бути впроваджені;
− Вимоги до систем та механізмів моніторингу безпеки мережі повинні бути визначені, впровадженні, необхідним чином управлятися;
− Усі оновлення повинні вчасно встановлюватись;
− Зміни можуть бути внесені лише адміністратором систем або відповідним авторизованим користувачем;
− Процес резервного копіювання мережевих пристроїв (наприклад, системного програмного забезпечення, даних конфігурацій, файлів баз даних) повинен відбуватися регулярно;
− Вимоги до конфігурування безпеки Wi-Fi мереж:

- Зміна паролів за замовчуванням;
- Вимкнення WPS;
- Вимкнення SSID Broadcast;
- Своєчасне оновлення прошивки;
- Обмеження можливості під'єднання пристроїв до локальної мережі.

Протоколи безпечного зв'язку

Щоб захистити інформацію в системах та додатках СР, необхідно належним чином управляти та контролювати мережі.
Використання протоколів безпечного зв'язку гарантують конфіденційність, цілісність, доступність та спостережливості інформації, що передається. Наступні протоколи найбільш прийнятні для використання:
− SSH2;
− SFTP;
− TLS 1.2-1.3;
− HTTPS;
− WSS;
− SMTPS;
− DNS-over-HTTPS.

3.11. Використання робочих пристроїв

СР повинна встановити вимоги щодо безпеки пристроїв, змінних носіїв під час їх використання.
Обов'язкове блокування екрану на пристроях після встановленого часу бездіяльності повинне бути налаштоване на всіх робочих пристроях.
Захист робочих пристроїв шляхом шифрування жорстких дисків та паролів для розблокування повинен бути реалізованим за необхідності.
Персонал несе відповідальність за забезпечення фізичної безпеки робочих пристроїв при їх використанні за межами приміщень СР (обмеження фізичного доступу третіх сторін, слідування вимогам блокування екрану).
Забезпечення виконання вимог щодо безпечного використання робочих пристроїв має бути автоматизовано за допомогою відповідних програмних інструментів. Політики налаштування таких інструментів повинні регулярно переглядатись на відповідність даній Політиці та іншим цільовим політикам СР.

3.12. Встановлення безпечних оновлень

СР повинна встановити вимоги щодо встановлення оновлень на всіх ІА, з яких надається доступ до інформації/послуг/ресурсів СР.
Режим автоматичного оновлення виправлень або можливість зробити це вручну має бути забезпечена адміністратором систем. Антивірусне програмне забезпечення та інші компоненти безпеки повинні регулярно перевірятись та оновлюватись до останньої версії.
Якщо операційна система – Windows, інструмент управління виправленнями повинен бути налаштований таким чином, щоб він автоматично завантажував останні виправлення безпеки Microsoft. Перевірка та застосування виправлень повинна проводитись за необхідності.

3.13. Обмеження встановлення програмного забезпечення

Правила до встановлення програмного забезпечення користувачами повинні бути визначені та впроваджені СР.
СР повинна створити та застосовувати правила щодо дозволеного для встановлення програмного забезпечення та контролю, базуючись на принципі мінімальних привілеїв. Відповідальна особа за ІБ та адміністратор систем мають створити списки дозволеного та забороненого для встановлення програмне забезпечення.
Встановлення програмного забезпечення повинно бути обмежене для всіх користувачів, проте можливі винятки, які повинні бути схвалені адміністратором систем та Відповідальною особою за ІБ.
Функція контролю закріплена за Відповідальною особою за ІБ та Керівництвом, щоб забезпечити належний рівень контролю та розділення привілеїв.

3.14. Захист від шкідливого ПЗ

Попереднє тестування програмного забезпечення та перевірка файлів до їх встановлення на пристроях, з яких існує доступ до корпоративної інформації/систем/ресурсів повинні забезпечуватись адміністратором систем.
Лише програмне забезпечення, затверджене адміністратором систем та Відповідальною особою за ІБ, дозволено встановлювати на системи СР.
Сканери проти шкідливого ПЗ необхідно налаштувати на автоматичне сканування відповідних компонентів відразу після випуску оновлень.
СР має налаштувати антивірусне програмне забезпечення на: сканування під час завантаження, сканування файлових та поштових серверів принаймні один раз на день та будь-яких інших серверів – принаймні раз на тиждень, сканування файлів при відкритті, сканування вкладень вхідної та вихідної електронної пошти, веб сканування вмісту при синхронізації із скануванням портативних пристроїв, де це можливо.
Управління та перегляд журналів антивірусного програмного забезпечення має здійснюватися адміністратором систем.
Для захисту програмного забезпечення від шкідливих програм СР повинно здійснюватися: ручне/автоматичне та планове сканування, видалення заражених файлів, розміщення заражених

файлів на карантин, які неможливо видалити, можливість автоматичного та запланованого оновлення, реєстрація випадків шкідливого програмного забезпечення та забезпечення можливості аналізу логів, централізоване управління та ведення логів.
Комп'ютери, у яких виявлено шкідливе програмне забезпечення, та комп'ютери без антивірусного програмного забезпечення заборонено під'єднувати до внутрішньої мережі СР.
Відповідальність за контроль дотримання захисту від шкідливого ПЗ покладено на Відповідальну особу за ІБ.

3.15. Логування та моніторинг

Інформація, яку слід збирати з власних систем має включати в себе:
- Дату та час події;
- Ідентифікатор користувача;
- Тип запиту/дії;
- Статус запиту (успішний чи невдалий);
- Події, що включають зміни, можуть вказувати на початок та кінцевий стан тощо.

СР повинна визначити необхідність проведення ручного збору логів в тих системах, де це неможливо автоматично або, якщо автоматичний аудит логів не містить необхідної інформації.
Для реалізації неможливості зміни/видалення журналів логів адміністратором систем, в СР мають бути впроваджені додаткові засоби контролю та рішення для реєстрації дій. Якщо критично важливі системи не мають функції реєстрації дій адміністратора систем, потрібно перейти на версії або нові платформи з наявною такою функцією або здійснити затвердження таких винятків Керівництвом СР. У разі неможливості зміни систем чи сервісів, такі винятки повинні бути погоджені з Керівництвом.

3.16. Віддалений доступ

Інтернет-ресурси СР мають використовуватися для дистанційного виконання робочих завдань, інформаційно-аналітичної роботи в інтересах СР, обміну поштою із третіми сторонами.
Інше використання Інтернет-ресурсів слід розглядати як порушення.
Підключення до мережі Інтернет в СР повинно здійснюватися адміністратором систем у порядку надання прав доступу. При переміщенні співробітника (звільненні, переведенні в інший підрозділ) його безпосередній Керівник повинен подати заяву на скасування прав доступу.
Віддалене підключення до інформаційних активів СР має здійснюватися за допомогою визначених адміністратором систем та Відповідальною особою за ІБ ресурсів.
З'єднання веб-зустрічей/віддаленого управління (наприклад, TeamViewer, AnyDesk) не повинні використовуватися в мережі СР для надання віддаленого доступу третім сторонам за замовчуванням. Цей тип підключень дозволений лише для технічного обслуговування та усунення несправностей систем після належної авторизації.

3.17. Резервне копіювання

Резервне копіювання повинно здійснюватися регулярно.
Критично важлива інформація, програмне забезпечення та системи, що підлягають резервному копіюванню, повинні бути визначені.
Періодичність створення резервних копій та частота їх тестування повинні бути чітко визначені.
Тип резервного копіювання (повне, інкрементне, диференційоване) повинен бути визначений адміністратором систем для кожної системи.
Резервні копії повинні зберігатися окремо від основних копій та повинен бути забезпечений належний рівень безпеки, а доступ до резервних копій повинен бути обмежений на тому ж рівні, що і для основних копій.
Доступ до резервних копій повинні мати лише визначені співробітники СР.
Відповідальність за здійснення резервного копіювання покладається на Відповідальну особу за ІБ.

3.18. Безпека комунікацій

СР повинна визначити дозволені методи для зв'язку (передачі корпоративної інформації)

всередині СР та з третіми сторонами.
Обов'язковою є перевірка вкладень з поштових скриньок та інших месенджерів перед завантаженням.
Заборонений доступ до ресурсів СР за прямим посиланням.
Під час обміну інформацією повинні використовуватись лише захищені протоколи передачі даних.
В СР повинен бути впроваджений та підтримуватись процес електронного спілкування, включаючи питання безпеки, відповідно до рівня конфіденційності переданої інформації. Там, де це необхідно, повинні бути впроваджені додаткові засоби захисту (цифровий підпис, шифрування тощо).

3.19. Управління ризиками

Управління ризиками є невід'ємною частиною діяльності на всіх рівнях СР. Метою управління ризиками є надання Керівництву СР інформації, необхідної для прийняття обґрунтованих рішень щодо зміни пріоритетів діяльності для управління областями неприйнятно високого ризику.
СР має здійснювати оцінку ризиків, оскільки це процес ідентифікації, вимірювань та визначення пріоритетів ризиків ІБ.

3.20. Управління інцидентами

СР повинна регулярно проводити навчання та підвищення обізнаності персоналу в сфері управління інцидентами. Підтримувати та розвивати процес реагування на всі типи інцидентів ІБ, відповідно до Політики управління інцидентами кібербезпеки (Додаток 1).
Кожен співробітник несе відповідальність за повідомлення Відповідальної особи за ІБ, коли він або вона дізнаються про те, що стався або міг статися інцидент ІБ, який міг поставити під загрозу безперервність діяльності СР.
Співробітники та треті сторони можуть намагатися вирішити інциденти ІБ лише за вказівками та з прямого дозволу Відповідальної особи за ІБ.
З міркувань безпеки та технічних міркувань СР залишає за собою право відстежувати, записувати та реєструвати все використання своїх інформаційних активів і діяльність у мережі СР.

3.21. Безперервність діяльності

СР повинна забезпечити наявність необхідних ресурсів для безперервної діяльності та швидкого відновлення критичних систем у разі непередбачуваних ситуацій.
Керівники підрозділів несуть відповідальність за визначення вимог щодо захисту доступності систем/сервісів/даних і несуть остаточну відповідальність за їх виконання. Вимоги мають базуватися на аналізі ризиків, критичності активів і враховувати нормативні вимоги. Керівництво несе відповідальність за забезпечення необхідного фінансування для їх реалізації. Відповідальна особа за ІБ повинен забезпечувати та підтримувати безперервність систем на випадок непередбачених обставин.

4. Перегляд, оновлення та розповсюдження

Політика буде опублікована у формі, яку неможливо легко змінити, і у формі, яка є актуальною, доступною та зрозумілою для цільового читача. Політика зберігається та є легкодоступною для персоналу та третіх сторін (за необхідності) для подальшого використання.
Політика буде розповсюджена в електронному вигляді. Нова копія Політики буде поширена разом із новою версією будь-якого компонента Політики. Нова копія матиме збільшений номер версії.
Персонал, який отримує електронну копію, оновлює власну паперову версію Політики та зберігає її.
Відповідальність за керування та оновлення Політики покладено на Відповідальну особу за ІБ. Оновлена Політика подається до Керівництва СР для остаточного затвердження. Політика переглядається щорічно для забезпечення її адекватності та відповідності потребам і цілям СР

або частіше, якщо це необхідно (під час внесення суттєвих змін).

5. Перелік відповідальних осіб за інформаційну безпеку Солонківської сільської ради

Роль	ПІБ	Підпис
Відповідальна особа за інформаційну безпеку Вовківського старостинського округу	Нагірний Петро Євгенович	
Відповідальна особа за інформаційну безпеку Жирівського старостинського округу	Домбровська Галина Зіновіївна	
Відповідальна особа за інформаційну безпеку Зубрянського старостинського округу	Бучок Андрій Степанович	
Відповідальна особа за інформаційну безпеку Поршнянського старостинського округу	Баркит Богдан Володимирович	
Відповідальна особа за інформаційну безпеку Раковецького старостинського округу	Скіп Тетяна Степанівна	
Відповідальна особа за інформаційну безпеку Відділу ЦНАП	Гладковська Оксана Іванівна	
Відповідальна особа за інформаційну безпеку Відділу бухгалтерського обліку та звітності	Кучерепа Уляна Іванівна	
Відповідальна особа за інформаційну безпеку Фінансового відділу	Гавриляк Руслання Григорівна	
Відповідальна особа за інформаційну безпеку Відділу земельних відносин	Лещук Богдан Йосифович	
Відповідальна особа за інформаційну безпеку Відділу архітектури та містобудування	Дідюк Андрій Васильович	
Відповідальна особа за інформаційну безпеку Юридичного відділу	Ширій-Ярема Ірина Ігорівна	
Відповідальна особа за інформаційну безпеку Відділу капітального будівництва, ЖКГ, транспорту та благоустрою	Копач Олег Богданович	

Відповідальна особа за інформаційну безпеку Відділу міжнародного територіального співробітництва та економічного розвитку громад	Войтович Володимир Васильович	
Відповідальна особа за інформаційну безпеку Відділу у справах ветеранів та соціального захисту населення	Богун Леся Романівна	
Відповідальна особа за інформаційну безпеку апарату управління та працівників поза відділами сільської ради	Зайльо Марія Ярославівна	
Відповідальна особа за інформаційну безпеку Служби у справах дітей	Гичка Галина Григорівна	
Відповідальна особа за інформаційну безпеку Відділу освіти, культури, туризму, молоді та спорту	Монастирський Роман Теофілійович	
Відповідальна особа за інформаційну безпеку КНП «ЦПМСД»	Метко Олександра Степанівна	
Відповідальна особа за інформаційну безпеку КП «Амарант»	Пташник Юрій Богданович	
Адміністратор систем	Стасишин Андрій Тарасович	
Треті сторони	Представники підрядних організацій та ін.	
Керівництво	Войтович Володимир Васильович	

Сільський голова **Богдан ДУБНЕВИЧ**

Додаток 1
до Політики інформаційної безпеки
Солонківської сільської ради

Політика управління інцидентами кібербезпеки

1. Загальне

Політика управління інцидентами кібербезпеки (далі – Політика) визначає вимоги та послідовність дій щодо виявлення, аналізу та опрацювання інцидентів кібербезпеки (далі – КБ) у Солонківській сільській раді (далі – СР).

Метою Політики є забезпечення:

- Організація оперативного виявлення, оцінки та реагування на інциденти КБ;
- Мінімізації наслідків інцидентів КБ;
- Запобігання інцидентам КБ в майбутньому, поліпшення впровадження та використання захисних заходів КБ;
- Відповідності рівня КБ СР вимогам законів України, нормативно-правових актів України та міжнародних стандартів в області КБ;
- Захисту інформаційних систем СР від порушень конфіденційності, цілісності, доступності та спостережності.

1.1. Класифікація інцидентів

За наслідками інциденти КБ повинні класифікуватись за відповідно до таблиці, яка наведена у **пункті 2.2.3** даної Політики.

1.2. Види інцидентів

В цій Політиці визначені наступні види інцидентів:

- Порушення цілісності інформації;
- Порушення конфіденційності;
- Порушення доступності;
- Порушення спостережності.

2. Реагування на інциденти КБ

Етап реагування на інциденти КБ в інформаційних системах СР повинен включати наступні кроки:

- Підготовка;
- Виявлення та аналіз;
- Стримування;
- Усунення;
- Відновлення;
- Аналіз ефективності.

2.1. Підготовка

Для забезпечення готовності СР до оперативного реагування на інциденти КБ повинні бути розроблені плани реагування на окремі види інцидентів КБ, що є найбільш ймовірними для певної прикладної системи з урахуванням умов та режиму її функціонування виходячи з прогнозованих даних та експертних оцінок.

Розробка планів реагування на інциденти КБ є основою для системного підходу до процесу управління інцидентами КБ в СР.

2.1.1. Етап «Створення плану реагування на інцидент КБ»

Відповідальна особа за ІБ повинна проводити пошук інформації про аналогічні інциденти КБ, які відбувалися в минулому та для яких розроблено типовий план реагування.

Якщо для поточного виду інциденту КБ у базі знань існує типовий план реагування, то

Відповідальна особа за ІБ переходить до його реалізації.
Якщо подібних інцидентів КБ у базі знань немає, Відповідальна особа за ІБ повинна розробити комплекс заходів, який оформлюється у вигляді плану реагування на інцидент КБ та зберігається в базі знань.

2.2. Виявлення та аналіз

2.2.1. Етапи «Виявлення та інформування про інцидент. Збір та реєстрація інформації про інцидент КБ»

У разі виявлення інциденту або слабких місць КБ працівники СР або залучені треті сторони повинні повідомити про це Відповідальну особу за ІБ.
До основних ознак інциденту відносяться наступні (невичерпний перелік):

- Суттєве зниження продуктивності прикладних систем або недоступність прикладних систем;
- Повідомлення антивірусного ПЗ;
- Несанкціонована діяльність у мережі та прикладних системах СР;
- Стрімке збільшення мережевого трафіку;
- Численні повідомлення про помилки та збої;
- Зафіксовані спроби підбору паролів;
- Заздалегідь відома негативна подія безпеки;
- Подія безпеки, що зафіксована у неробочий час;
- Невідомі облікові записи;
- Відключені засоби забезпечення безпеки;
- Спроби застосування методів соціальної інженерії;
- Відсутність засобів захисту інформації;
- І т.д.

Працівник СР, який виявив можливі ознаки інциденту, повинен вказати у повідомленні наступну інформацію:

- Опис проблеми, що спостерігається;
- Час виникнення ознак інциденту;
- Інші суттєві дані щодо інциденту – у відповідь на запитання Відповідальної особи за ІБ

2.2.2. Етап «Аналіз інциденту»

Процедура повинна розпочинатись за фактом отримання Відповідальною особою за ІБ повідомлення про виникнення інциденту КБ.
Після отримання повідомлення про інцидент Відповідальна особа за ІБ повинна провести класифікацію інциденту, аналіз зібраної інформацію та прийняти рішення щодо підтвердження його статусу.

2.2.3. Етап «Оповіщення про інцидент»

В СР оповіщення зацікавлених сторін (голова СР, заступники голови, Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA, яка функціонує в складі Державної служби спеціального зв’язку та захисту інформації України, Служба безпеки України, Національний координаційний центр кібербезпеки при РНБО України, залучені треті сторони – відповідно до договірних вимог, тощо) повинно здійснюватися Відповідальною особою за ІБ визначеними засобами після маркування.
Маркування повинно проводитися відповідно до наступних значень:

Мітка (колір)	Значення
рівень 0, некритичний (білий)	Кіберінцидент/кібератака не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем.
рівень 1, низький (зелений)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно- комунікаційних систем, технологічних систем, але не загрожує захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.
рівень 2, середній (жовтий)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно- комунікаційних систем, технологічних систем, внаслідок чого створюються передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються, виникають передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою.
рівень 3, високий (помаранчевий)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно- комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Реагування на цьому рівні може потребувати залучення сил та засобів більше ніж одного основного суб’єкта національної системи кібербезпеки.
рівень 4, критичний (червоний)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох інформаційних, електронних комунікаційних, інформаційно- комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають реальні загрози для національної безпеки і оборони, стану навколишнього природного середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Кіберінцидент/кібератака може

	мати транскордонний вплив. Реагування на цьому рівні потребує залучення сил та засобів основних суб'єктів національної системи кібербезпеки.
рівень 5, надзвичайний (чорний)	Кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю громадян України. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує максимального залучення сил та засобів основних суб'єктів національної системи кібербезпеки та інших суб'єктів забезпечення кібербезпеки.

2.3. Стримування

2.3.1. Етап «Збір інформації для розслідування інциденту»

Відповідальна особа за ІБ відповідно до плану реагування повинна зібрати інформацію про інцидент для проведення подальшого розслідування.

У випадку, коли при реалізації збору інформації про інцидент КБ планується переривання роботи інформаційно-комунікаційної системи (далі ІКС), Відповідальна особа за ІБ, повинна погодити таке переривання з Керівництвом СР.

2.3.2. Етап «Зменшення впливу інциденту»

Відповідальна особа за ІБ повинна обрати методи та заходи, спрямовані на зменшення впливу інциденту на процеси діяльності СР, окремо для кожного конкретного інциденту, залежно від його виду, та у відповідності з розробленим, планом реагування.

Будь-які методи, дії та порядок їхнього використання або виконання повинні погоджуватися Керівництвом СР.

Відповідальна особа за ІБ повинна виконати оцінку можливого впливу запланованих дій на безперервність діяльності ураженої системи та проінформувати Керівництво СР. За необхідності допускається ізолювання системи або роз'єднання компонентів цієї системи на період проведення повного розслідування інциденту.

2.4. Усунення інциденту та відновлення функціонування інформаційно- комунікаційної системи

З метою відновлення нормального функціонування ІКС Відповідальна особа за ІБ повинна проводити заходи з усунення причин та наслідків інциденту.

Процедура усунення інциденту та відновлення функціонування залежить від виду інциденту та повинна визначатись для кожного інциденту окремо.

Після відновлення функціонування ІКС Відповідальна особа за ІБ має перевірити відсутність ознак повторення інциденту та повідомити про завершення робіт Керівництво СР.

2.5. Аналіз ефективності заходів з реагування на кіберінциденти/кібератаки

2.5.1. Етап «Розслідування інциденту»

Під час виконання робіт з розслідування інцидентів повинні використовуватись методи та засоби, що запобігають випадковому або навмисному внесенню змін в дані, що вивчаються та аналізуються.

Відповідальна особа за ІБ повинна з'ясувати причини інциденту та провести аналіз усіх виявлених у процесі розслідування небезпечних факторів, що призвели до відхилень:

- у діях працівників СР;
- у роботі інформаційних ресурсів та систем;
- відхилень від норм експлуатації програмного забезпечення і обладнання;
- відхилень від вимог політик ІБ із визначенням ступеня впливу цих відхилень на розвиток інциденту.

Відповідальна особа за ІБ повинна визначити:

- які нормативні вимоги були порушені або не виконані (з посиланням на відповідні статті, розділи, пункти нормативних актів);
- причетність до інциденту, якщо це мало місце, інших підприємств, організацій і установ із визначенням, наскільки це можливо;
- ступеня їх впливу на виникнення і перебіг інциденту.

2.5.2. Етап «Аналіз ефективності»

Після завершення розслідування Відповідальна особа за ІБ повинна підготувати звіт з описом всіх проведених процедур щодо управління інцидентами КБ та закриттям інциденту КБ та надати Керівництву СР, а також, за необхідності, зацікавленим сторонам.

Відповідальна особа за ІБ повинна внести інформацію про закриття інциденту в журнал реєстрації інцидентів.

3. Система внутрішнього контролю

Всі співробітники СР несуть відповідальність за своєчасність інформування Відповідальну особу за ІБ у разі виявлення ознак інцидентів КБ або можливості настання інциденту КБ.

4. Підтримка, оновлення та розповсюдження

Політика буде опублікована у формі, яку неможливо легко змінити, і у формі, яка є актуальною, доступною та зрозумілою для цільового читача. Політика зберігається та є легкодоступною для персоналу та третіх сторін (за необхідності) для подальшого використання.

Політика буде розповсюджена в електронному вигляді. Нова копія Політики буде поширена разом із новою версією будь-якого компонента Політики. Нова копія матиме збільшений номер версії.

Персонал, який отримує електронну копію, оновлює власну паперову версію Політики та зберігає її.

Відповідальність за керування та оновлення Політики покладено на Відповідальну особу за ІБ. Оновлена Політика подається до Керівництва СР для остаточного затвердження. Політика переглядається щорічно для забезпечення її адекватності та відповідності потребам і цілям СР або частіше, якщо це необхідно (під час внесення суттєвих змін).

Сільський голова **Богдан ДУБНЕВИЧ**

Додаток 2
до рішення виконавчого комітету
Солонківської сільської ради
від 21.07.2025 року

План реагування на інциденти кібербезпеки

Опис інциденту кібербезпеки

№	Назва інциденту	План дій щодо реагування на інцидент	Дата/час виконання дій з реагування	Очікувана дата завершення всіх дій з реагування	Технічні, програмні та фінансові ресурси	Місце збереження інформаційних підтверджень та доказів	Відповідальна за реагування особа (ПІБ,Посада)	Статус			Коментарі
								Не розпочато	У процесі	Завершено	

Приклади реагування на інцидент кібербезпеки

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
ФІШИНГ	Завдання: Визначити та впровадити кроки з розслідування інцидентів КБ, включаючи основні питання та стратегії фішингу. 1. Область та масштаб атаки 2. Аналіз повідомлень 3. Аналіз посилань та вкладень 4. Категоризація типу атак 5. Визначення критичності атаки	Спланувати заходи з усунення інцидентів у яких ці кроки запускаються разом (або скоординовано) з залученням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Визначити необхідний час і компромісні підходи для усунення наслідків. Завдання: Визначити тактичні та стратегічні кроки стримування фішингових атак.	Завдання: Визначити етапи проведення комунікацій під час фішинг атаки. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення після фішинг атаки. Визначити та вказати інструменти та процедуру для кожного кроку	Приклад: Дії користувача при ймовірній фішинговій атаці Завдання: Визначити кроки для користувачів, які мають підозру на фішинг.	

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
ПРОГРАМ И-ВИМАГАЧ І	Завдання: Визначити та впровадити кроки з розслідування атак/інцидентів, які відбулись за участі програм-вимагачів, зокрема основні питання та стратегії. 1. Визначити тип програм-вимагачів 2. Визначити область застосування 3. Оцінка впливу 4. Знайти інфікованого	Спланувати заходи з усунення інцидентів, у яких ці кроки запускаються разом (або скоординовано) з залученням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з усунення інциденту. Завдання: Визначити тактичні та стратегічні кроки стримування програм-вимагачів.	Завдання: Визначити етапи проведення комунікацій. Вказати інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру для кожного кроку. Не рекомендовано платити викуп: це не гарантує вирішення проблеми. Все може піти не так (наприклад, помилки можуть зробити дані неможливими для відновлення навіть за допомогою ключа). Крім того, оплата доводить, що програми-вимагачі працюють і можуть посилити атаки проти вас чи будь-кого іншого.	Приклад: Дії користувача при підозрі про наявність програми-вимагача Завдання: Визначити кроки для користувачів, які реагують на наявність програми-вимагача.	
АТАКА НА ВЕБСАЙТ	1. Негайно відключити зіпсований сервер для	Спланувати заходи з усунення проблем, у яких кроки зі стримування запускаються разом (або	Завдання: Визначити кроки проведення етапу комунікацій. Вказати	Завдання: Визначити кроки відновлення. Визначити та вказати інструменти та процедуру	Приклад: Дії користувача при атаці пошкодження веб-сайту Завдання: Визначити	Завдання: Поспілкуватись з іншими співробітниками, щоб переконатися, що всі розуміють

	РОЗСЛІДУВАН НЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
	подальшого дослідження. 2. Визначити джерело вразливості системи, яку використав зловмисник. 3. Зібрати будь- які підказки щодо того, ким є хакер або на яку організацію він працює. 4. Зібрати іншу важливу інформацію зі сторінки, яка була зіпсована.	скоординовано) з задіянням відповідних команд спеціалістів, готових реагувати на будь-які порушення. Розглянути час і компромісні підходи з усунення інциденту. Завдання: Визначити тактичні та стратегічні кроки стримування пошкодження веб-сайтів. 1. Створити резервну копію всіх даних, що зберігаються на веб-сервері. 2. Обов'язково тимчасово вимкнути сервер зіпсованої сторінки, поки триває розслідування. Після визначення джерела атаки	інструменти та процедуру (зокрема хто повинен бути залучений) для кожного кроку.	для кожного кроку.	кроки для користувачів, які реагують на атаку на веб- сайт.	наступні кроки та роблять свій внесок, де це можливо.

	РОЗСЛІДУВАННЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
		виконати необхідні кроки, щоб переконатися, що сценарій атаки більше не повториться				
ВТРАТА ДАНИХ	Забезпечити належний доступ до будь-якої необхідної документації та інформації, включаючи доступ у неробочий час, для наступного: - Процес управління інцидентами; - Схеми архітектури мережі; - Діаграми потоку даних; Визначити та отримати послуги стороннього провайдера. Переглянути останні	Завдання: Визначити та впровадити кроки з розслідування, зокрема основні питання та стратегії компрометації, ідентифікації та доступу.	1. Переконатись, що будь-які задіяні дані. 2. Проаналізувати будь-який підозрілий мережевий трафік. 3. Переглянути журнали безпеки та доступу, сканування вразливостей і будь-які автоматизовані результати інструментів. Проаналізувати будь-яку підозрілу активність, файли чи виявлені зразки ЗПЗ. 4. Зіставити будь- які нещодавні події безпеки або ознаки компрометації з підозрілою активністю в	Етап виправлення: - Містить технічний механізм порушення даних; - Усунення технічного механізму витоку даних; - Відновлення уражених систем і служб та приведення до звичайного стану.	На додаток до загальних кроків і вказівок у плані реагування на інцидент: 1. Відновити системи на основі аналізу впливу на діяльність і критичності діяльності. 2. Здійснити повне антивірусне та розширене сканування шкідливих програм усіх систем по всій організації 3. Повторно встановити облікові дані всіх задіяних систем і дані облікових записів користувач	Етап заходів після інциденту має такі цілі: - Заповнити Звіт про інцидент, включаючи всі деталі інциденту та дії. - Завершити процес управління інцидентами. - Опублікувати відповідні внутрішні та зовнішні повідомлення.

	РОЗСЛІДУВАН НЯ	ВИПРАВЛЕННЯ	КОМУНІКАЦІЯ	ВІДНОВЛЕННЯ	РЕСУРСИ	ЗАПОБІГАННЯ РИЗИКАМ
	кіберінциденти та їх результати		мережі. 5. Визначити джерело компрометації даних. 6. Визначити конкретний набір даних, який було зламано, а також спосіб його зламу. 7. Визначити методологію атаки та графік кіберінцидентів		ів. 4. Реінтегрувати раніше скомпрометован і системи. 5. Відновити будь-які пошкоджені або знищені дані. 6. Відновити усі призупинені служби. 7. Встановити моніторинг для виявлення подальшої підозрілої діяльності. 8. Координувати впровадження будь-яких необхідних виправлень або заходів з усунення вразливостей.	

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ

ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 498

від 21 липня 2025 року

Про затвердження зведеного кошторисного розрахунку вартості об'єкта будівництва «Реконструкція системи газопостачання адмінбудівлі за адресою: вул. Франка І., 6а с. Зубра Львівського району Львівської області»

Відповідно ст.31 Закону України "Про місцеве самоврядування в Україні", статті 7 Закону України «Про архітектурну діяльність», «Про регулювання містобудівної діяльності», ЗУ «Про публічні закупівлі» та Порядку затвердження проектів будівництва і проведення їх експертизи, затвердженого постановою Кабінету Міністрів України від 11.05.2011 № 560 та на підставі зведеного кошторисного розрахунку вартості об'єкта будівництва по проекту «Реконструкція системи газопостачання адмінбудівлі за адресою: вул. Франка І., 6а с. Зубра Львівського району Львівської області»,

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ ВИРІШИВ:

1. Затвердити зведений кошторисний розрахунок вартості об'єкта будівництва по проекту «Реконструкція системи газопостачання адмінбудівлі за адресою: вул.Франка І., 6а с. Зубра Львівського району Львівської області» загальною вартістю 30,76583 тис. грн, в тому числі:

   Будівельних робіт – 24,19882 тис. грн;
   Устаткування, меблі та інвентар – 0 тис. грн;
   Інші витрати – 6,56701 тис. грн.

2. Контроль за виконанням даного рішення покласти на виконавчий комітет Солонківської сільської ради.

Сільський голова **Богдан ДУБНЕВИЧ**

ВИКОНАВЧИЙ КОМІТЕТ
СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ЛЬВІВСЬКОГО РАЙОНУ ЛЬВІВСЬКОЇ ОБЛАСТІ

РІШЕННЯ № 499

від 21 липня 2025 року

Про затвердження зведеного кошторисного розрахунку вартості об'єкта будівництва «Реконструкція системи газопостачання адмінбудівлі за адресою: вул.Центральна, 61а с.Раковець Львівського району Львівської області»

Відповідно ст.31 Закону України "Про місцеве самоврядування в Україні", статті 7 Закону України «Про архітектурну діяльність», «Про регулювання містобудівної діяльності», ЗУ «Про публічні закупівлі» та Порядку затвердження проектів будівництва і проведення їх експертизи, затвердженого постановою Кабінету Міністрів України від 11.05.2011 № 560 та на підставі зведеного кошторисного розрахунку вартості об'єкта будівництва по проекту «Реконструкція системи газопостачання адмінбудівлі за адресою: вул. Центральна, 61а с. Раковець Львівського району Львівської області»,

ВИКОНАВЧИЙ КОМІТЕТ СОЛОНКІВСЬКОЇ СІЛЬСЬКОЇ РАДИ
ВИРІШИВ:

1. Затвердити зведений кошторисний розрахунок вартості об'єкта будівництва по проекту «Реконструкція системи газопостачання адмінбудівлі за адресою: вул. Центральна, 61а с. Раковець Львівського району Львівської області» загальною вартістю 27,48647 тис. грн, в тому числі:

   Будівельних робіт – 21,48228 тис. грн;
   Устаткування, меблі та інвентар – 0 тис. грн;
   Інші витрати – 6,00419 тис. грн.

2. Контроль за виконанням даного рішення покласти на виконавчий комітет Солонківської сільської ради.

Сільський голова **Богдан ДУБНЕВИЧ**