КОМУНАЛЬНИЙ ЗАКЛАД
«ДНІПРОРУДНЕНСЬКА ГІМНАЗІЯ «СОФІЯ»-
ЗАГАЛЬНООСВІТНЯ ШКОЛА І-ІІІ СТУПЕНІВ № 1»
ВАСИЛІВСЬКОЇ РАЙОННОЇ РАДИ ЗАПОРІЗЬКОЇ ОБЛАСТІ

НАКАЗ

Код ЄДРПОУ 25765436

18.12.2023 **м. Дніпрорудне** **№ 154 – од**

Про створення команди реагування та затвердження Порядку дій щодо раннього попередження та евакуації, Алгоритму дій учасників освітнього процесу в разі нападу або ризику нападу на заклад освіти

На виконання наказу Міністерства Внутрішніх Справ України, Міністерства освіти і науки України № 685/1013 від 18.08.2023, зареєстровано в Міністерстві юстиції України 07 вересня 2023 р. за № 1583/40639 «Про затвердження Порядку раннього попередження та евакуації учасників освітнього процесу в разі нападу або ризику нападу на заклад освіти», відповідно до листа Департаменту освіти і науки Запорізької обласної державної адміністрації від 18.12.2023 № 3905/03.2-18 «Про створення команд реагування закладу освіти», листа Дніпрорудненської міської військової адміністрації Василівського району Запорізької області від 18.12.2023 про проведену роботу щодо вищезазначених питань

НАКАЗУЮ:

1. Адміністрації закладу освіти:

1) Затвердити склад команди реагування закладу освіти:

Посада	Прізвище, власне ім'я, по батькові (за наявності)	Номер телефону	Електронна адреса
Заступник керівника закладу освіти	Бачурська Тетяна Анатоліївна	+380972563531	tetianabachurska@sofiya-dn.com
Заступник керівника закладу освіти	Амірзянов Владислав Нургазимович	+380966149610	vladyslavamirzianov@sofiya-dn.co
Заступник керівника закладу освіти	Коваленко Ольга Андріївна	+380989298010	olgakovalenko@sofiya-dn.com
Заступник керівника закладу освіти	Смішко Ольга Іванівна	+380975775613	olgasmishko@sofiya-dn.com
Заступник керівника закладу освіти	Сіра Рената Юріївна	+380977007729	renatasira@sofiya-dn.com
Заступник керівника закладу освіти	Цаприка Аліна Олександрівна	+380989802254	alinatsapryka@sofiya-dn.com
Соціальний педагог	Мовчан Валентина Петрівна	+380979534610	valentynamovchan@sofiya-dn.com

закладу освіти			
Вчитель початкових класів	Антоненко Олена Миколаївна	+380679897184	olenaantonenko@sofiya-dn.com
Вчитель біології	Міц Ольга Миколаївна	+380974805697	olhamits@sofiya-dn.com
Вчитель обслуговуючої праці	Качмар Ольга Олександрівна	+380977677657	olhakachmar@sofiya-dn.com
Вчитель математики	Куріпка Тетяна Іванівна	+380988449763	tetianakuripka@sofiya-dn.com
Вчитель іноземної мови	Овсієнко Юлія Миколаївна	+380979621600	yuliiaovsiienko@sofiya-dn.com
Вчитель української мови та літератури	Школова Юлія Володимирівна	+380974976754	yuliiashkolova@sofiya-dn.com
Вчитель предмету «Захист України»	Коломієць Станіслав Володимирович	+380962573267	stanislavkolomiets@sofiya-dn.com
Вчитель інформатики	Лобас Віталій Володимирович	+380975437054	vitallobas@sofiya-dn.com

2) Створити безпечні умови освітнього процесу з психологічною підтримкою фахівців (без фізичного та психологічного насильства).

2. Затвердити Порядок дій щодо раннього попередження та евакуації та Алгоритму дій учасників освітнього процесу в разі нападу або ризику нападу на заклад освіти та (додаток).

3. Працівникам закладу освіти:
1) Постійно проводити профілактичні та інформаційні заходи щодо попередження алгоритму дій у разі нападу на заклад освіти.
2) Захищати права, інтереси та свободи, життя і здоров’я людини та громадянина, суспільства та держави від протиправних посягань під час освітнього процесу.
3) Забезпечити інформаційну безпеку учасників освітнього процесу та проводити систематичну роз’яснювальну роботу серед здобувачів світи щодо захисту персональних даних, безпечного використання Інтернету для безпеки дистанційного навчання.

4. Заступнику директора з НВР Тетяні БАЧУРСЬКІЙ довести до відома працівників закладу освіти зміст даного наказу, Алгоритм дій учасників освітнього процесу в разі нападу або ризику нападу на заклад освіти та Порядок дій щодо раннього попередження та евакуації.

5. Контроль за виконанням даного наказу залишаю за собою.

Директор узгоджено в електронному виді Світлана ПРИТУЛА

З наказом ознайомлені

Всі працівники закладу освіти

Додаток до наказу

№ 154-од від 18.12.2023

Порядок дій щодо раннього попередження та евакуації

Засновник закладу освіти або уповноважений ним орган (особа) (далі – засновник закладу освіти) з метою створення умов безпечного освітнього середовища для навчання здобувачів освіти та роботи працівників закладу освіти (за згодою засновника закладу освіти):

- забезпечує впровадження інженерно-технічних заходів цивільного захисту закладу освіти;
- уживає заходів щодо встановлення в закладі освіти автоматизованої системи оповіщення, а в разі необхідності - технічних засобів охорони.

Керівник закладу освіти з метою створення умов безпечного освітнього середовища для навчання здобувачів освіти та роботи працівників закладу освіти:

1) організовує, забезпечує та контролює виконання заходів, спрямованих на створення безпечних умов перебування учасників освітнього процесу в закладі освіти;

2) розробляє та затверджує план евакуації, порядок оповіщення учасників освітнього процесу та алгоритми їх дій у разі нападу або ризику нападу на заклад освіти;

3) створює команду реагування закладу освіти, затверджує її склад (не менше ніж три працівники закладу освіти) та розподіляє між ними обов'язки щодо вжиття заходів реагування в разі нападу або ризику нападу на заклад освіти, у тому числі проведення евакуації учасників освітнього процесу;

4) забезпечує надання команді реагування закладу освіти, уповноваженому поліцейському, працівнику ДСНС інформації, яка міститься в паспорті безпеки закладу освіти, за формою, наведеною в додатку до цього Порядку, та її вчасне оновлення;

5) уживає заходів щодо унеможливлення доступу на територію закладу освіти сторонніх осіб, крім учасників освітнього процесу;

6) вносить пропозиції засновнику закладу освіти щодо необхідності забезпечення закладу освіти технічними засобами охорони та фізичною охороною (за потреби);

7) забезпечує проведення комплексного обстеження не рідше ніж один раз на шість місяців стану об'єктів фонду захисних споруд цивільного захисту, маршруту руху до них, вказівників, надійності охорони закладу освіти (запірні пристрої на вікнах та дверях, наявність ґрат на вікнах, засобів та систем протипожежного захисту, комплексу тривожної сигналізації з передаванням тривожних сповіщень на пункти централізованого спостереження охорони);

8) забезпечує ознайомлення учасників освітнього процесу з планом евакуації та порядком оповіщення в разі нападу або ризику нападу на заклад освіти;

9) забезпечує належне функціонування об’єктової системи оповіщення (гучномовці, шкільні дзвінки, сирени), системи протипожежного захисту закладу освіти;
10) контролює відповідність стану будівель, приміщень, інженерно-технічних комунікацій, устаткування, обладнання в закладі освіти чинним стандартам, правилам, нормам, не рідше ніж один раз на шість місяців організовує перевірку таких приміщень та території закладу освіти постійно діючими технічними комісіями закладу освіти із складанням акта;
11) організовує проведення щороку заходів (навчання, тренування, тренінги) щодо дій учасників освітнього процесу в разі нападу або ризику нападу на заклад освіти не рідше ніж чотири рази впродовж навчального року.

Команда реагування закладу освіти:

- розробляє та подає на затвердження керівнику закладу освіти алгоритм дій учасників освітнього процесу в разі нападу або ризику нападу на заклад освіти, а також плани евакуації учасників освітнього процесу;
- складає та оновлює паспорт безпеки закладу освіти, копія якого надається уповноваженому поліцейському, працівнику ДСНС та (за потреби) представникам інших органів державної влади;
- здійснює навчання (тренування, тренінги) учасників освітнього процесу згідно з алгоритмами дій у разі нападу або ризику нападу на заклад освіти, а також проведення їх евакуації;
- у разі нападу або ризику нападу на заклад освіти діє згідно з алгоритмом дій, затвердженим керівником закладу освіти.

Працівник закладу освіти в разі нападу або ризику нападу на заклад освіти:
1) негайно повідомляє членів команди реагування закладу освіти та керівника закладу освіти про відомі обставини нападу або ризику нападу;
2) роз’яснює здобувачам освіти алгоритми дій;
3) вживає заходів щодо проведення евакуації безпечним шляхом, визначеним командою реагування закладу освіти, у разі неможливості евакуації вживає заходів щодо залишення здобувачів освіти в місці їх перебування в закладі освіти;
4) виконує вимоги поліцейських та/або працівників ДСНС, які прибули в заклад освіти для реагування на напад або ризик нападу, сприяє в межах компетенції їх діяльності та за можливості інформує про перебіг евакуації, місця перебування учасників освітнього процесу;
5) за наявності постраждалих осіб надає їм домедичну допомогу;
6) обстежує приміщення закладу освіти з метою виявлення учасників освітнього процесу, яких не евакуювали;
7) бере участь у навчаннях (тренуваннях, тренінгах) щодо виконання дій згідно з алгоритмами в разі нападу або ризику нападу на заклад освіти, а також проведення евакуації.

Підставою для прийняття рішення про евакуацію учасників освітнього процесу є:

- перебування в закладі освіти або на його території чи безпосередньо поблизу них осіб, які скоїли напад, або наявні інші дані, що свідчать про намір скоєння нападу;
- надходження повідомлень в усній або письмовій формі про напад або ризик нападу на заклад освіти.

Для оповіщення про напад або ризик нападу на заклад освіти використовуються такі сигнали:

- перший сигнал – короткі, тривалістю 2-3 секунди, дзвінки, які повторюються п’ять разів із паузами, призначені для повідомлення учасникам освітнього процесу, що відбувається напад або є ризик нападу на заклад освіти;
- другий сигнал – довгий, тривалістю 10-15 секунд, дзвінок, призначений для повідомлення учасників освітнього процесу про проведення евакуації.

Алгоритм дій у разі нападу або ризику нападу на заклад освіти

1. Керівник закладу освіти координує та контролює дії членів команди реагування закладу освіти та працівників закладу освіти.

2. Команда реагування закладу освіти та/або працівник закладу освіти:

1) негайно викликають поліцію та (за необхідності) інші екстрені служби, вмикає систему оповіщення за першим сигналом та повідомляє керівнику закладу освіти про напад або ризик нападу на заклад освіти;

2) з'ясовує обставини нападу або виникнення ризику нападу (сутність загрози, кількість постраждалих від нападу, їх фізичний стан та місце перебування);

3) у разі неможливості евакуації, зокрема якщо проведення евакуації може бути небезпечним, уживає заходів щодо залишення учасників освітнього процесу в місці їх перебування в закладі освіти та блокування будь-яким способом дверей та вікон;

4) у разі проведення евакуації вмикає систему оповіщення за другим сигналом;

5) уживає заходів щодо проведення безпечної евакуації учасників освітнього процесу в безпечне місце;

6) організовує безпечне пересування учасників освітнього процесу до укриття або іншого безпечного місця;

7) перевіряє приміщення, будівлю закладу освіти на відсутність у них учасників освітнього процесу;

8) виконує вимоги поліцейських та/або працівників ДСНС, які прибули в заклад освіти для реагування на напад або ризик нападу, та сприяє в межах компетенції їх діяльності та за можливості інформує про перебіг евакуації, місця перебування учасників освітнього процесу;

9) у разі наявності постраждалих від нападу організовує надання їм домедичної допомоги, у тому числі із залученням екстрених служб;

10) за можливості оповіщає батьків, інших законних представників про переміщення здобувачів освіти в укриття;

11) погоджує повернення учасників освітнього процесу до навчання після завершення заходів, вжитих у разі нападу або ризику нападу на заклад освіти, а також перевіряє кількість здобувачів освіти.

Рекомендації педагогічним працівникам для безпеки дистанційного навчання

Закон України «Про основні засади здійснення кібербезпеки України» зазначає, що розвиток безпечного, стабільного і надійного кіберпростору має полягати в тому числі і завдяки «підвищенню цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту». В сучасних закладах освіти комп'ютерні технології використовуються майже при вивченні всіх навчальних предметів. Саме тому, необхідно вдосконалювати сучасну професійну підготовку педагогів у сфері інформаційних

технологій, а отже, і у сфері кібербезпеки. Кіберзагрози існують скрізь, де застосовуються інформаційні технології, отже, педагог може у своїй професійній діяльності зіткнутися зі спамом, з вірусами, зі зломом комп'ютера та з багатьма іншими проблемами, на які потрібно не тільки оперативно реагувати, а й вміти запобігати їх появі, а значить постійно згадувати в контексті уроку різні аспекти організації інформаційної безпеки. Педагог повинен мати уявлення про сучасний рівень розвитку інформаційних цифрових технологій.

Міжнародний союз електрозв'язку визначає такі рекомендації для викладачів. Насамперед необхідно слідкувати за безпекою та надійністю як домашніх так і робочих пристроїв, які ви використовуєте для проведення дистанційного навчання.

Для цього:

− переконайтеся в тому, що всі пристрої надійно захищені та на них встановлено пароль. Учителі настільки ж вразливі перед кібератаками, шкідливими програмами, вірусами та зламами, як і всі інші. Важливо, щоб усі пристрої, які ви використовуєте, захищалися надійним паролем. Онлайн-генератор надійних паролів – сервіс 2ip.ua (https://2ip.ua/ua/services/useful-service/password-generator)

− блокуйте пристрої, завершуйте сеанс і виходьте з облікового запису, коли не використовуєте їх (наприклад, якщо виходите з кімнати або класу);

− встановіть антивірусне програмне забезпечення та брандмауер й регулярно їх оновлюйте.

Також дотримуйтеся визначеної закладом освіти політики щодо використання мобільних технологій та інших електронних пристроїв. Важливо, щоб при використанні пристроїв ви подавали учням приклад правильної поведінки. Забезпечте фільтрацію та моніторинг даних, що передаються через шкільне під'єднання до Інтернету (під час дистанційного навчання вдома – через домашнє під'єднання до Інтернету). Здобувачі освіти не повинні отримувати доступу до шкідливого або неприйнятного контенту через ІТ-системи закладу освіти або домашнє технічне обладнання. Системи фільтрації мають щонайменше блокувати доступ до незаконного контенту, а також контенту, який вважається неприйнятним або шкідливим. Необхідно пам'ятати про власну онлайн-репутацію та цифровий слід, який залишаєте, про те, що ваші слова та дії в Інтернеті можуть вплинути як на вашу власну репутацію, так і на репутацію закладу освіти. Також розповідайте дітям про важливість онлайнової репутації й про те, як правильно її формувати. Між приватним та професійним життям педагогів завжди має бути чітка межа, зокрема, й у цифровому середовищі. Для будь-яких контактів між співробітниками закладу освіти та здобувачами освіти або батьками завжди необхідно використовувати корпоративну електронну пошту. Комунікаційна політика закладу освіти може забороняти будь-які контакти, не пов'язані з освітньою діяльністю, та контакти на платформах, що не мають стосунку до закладу освіти. На випадок проведення відеоконференцій або занять у віддаленому режимі, заклади освіти мають установлювати чіткі приписи як для співробітників, так і для учнів (наприклад, що бажано підготувати місце для віддаленого заняття/сеансу зв'язку та подбати про тих, хто перебуває поруч – чи то вдома, чи то в класі). Викладачі мають розуміти, чим Інтернет може бути для учнів небезпечний і чим корисний. З рекомендаціями щодо захисту дітей в мережі інтернет можна докладно ознайомиться у Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі, розробленими Міжнародним союзом електрозв'язку (МСЕ) та робочою групою авторів із провідних установ, що працюють у індустрії інформаційнокомунікаційних технологій (ІКТ) і переймаються проблемами захисту дитини (в цифровому середовищі), зокрема за посиланням https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiativi-mintsifripidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP-Guidelinesfor-Parents-Educators-UAfin.pdf

Для безпеки педагогів експерти радять створити окремий обліковий запис або окремого користувача, якщо ділите вдома чи на роботі свій пристрій ще з кимось, і також розмежувати ваші власні електронні скриньки для особистого користування та для робочих питань. Необхідно також звертати особливу увагу на пересилання персональної інформації (власної або здобувача освіти) через соціальні мережі, різноманітні месенджери, електронною поштою.

Поміркуйте, чи дійсно необхідно надсилати персональні дані у повідомленні. Якщо це все ж необхідно, потрібно ретельно перевірите, чи правильно вказана адреса адресата.

Рекомендації для батьків

Захист персональних даних – це спільна робота педагогів, батьків та учнів. Тому чималу роль у тому, чи буде дистанційне навчання успішним, якісним та безпечним для дитини, відіграють батьки. Просимо вас розповісти дітям про персональні дані, про небезпеку їхнього поширення і правила поводження з ними.

Для батьків Міжнародний союз електрозв'язку визначає такі рекомендації.

1. Насамперед спілкуйтеся зі своїми дітьми, цікавтеся, що вони люблять переглядати в Інтернеті, спробуйте організувати спільно з ними будь-яку онлайнову діяльність.

2. Визначте, які технології, пристрої та послуги використовуються у вас вдома.

3. Встановіть на всіх пристроях брандмауер та антивірусну програму. Поміркуйте над тим, чи будуть корисними та чи підходять для вашої родини програми фільтрації, блокування або відстеження. Розгляньте можливість використання контент-фільтрів, що досить часто називаються системами батьківського контролю, і безпечних пошукових систем або обмежень доступу, щоб фільтрувати контент, який діти можуть переглядати в Інтернеті.

4. У колі родини домовтеся про умови використання Інтернету й особистих пристроїв, приділяючи особливу увагу питанням конфіденційності, вікової відповідності змісту сайтів, додатків та ігор, булінгу, кількості проведеного перед екраном часу та небезпеки з боку незнайомців.

5. Поясніть дітям, що перш ніж публікувати світлини або відео в Мережі, слід отримати згоду людей, які там зображені. Батькам також варто звертати увагу на те, якою інформацією про своїх дітей вони діляться в соціальних мережах і в Інтернеті загалом, зокрема, це стосується особистих історій про дітей або їхніх світлин. Пам'ятайте про недоторканність приватного життя вашої дитини!

6. Поясніть дітям, що не можна повідомляти свої паролі доступу друзям або братам і сестрам. Звертайте їхню увагу на те, коли і де вони повідомляють свою персональну інформацію – наприклад, навчайте, що в загальнодоступному профілі краще використовувати деперсоніфіковані зображення як фотографії профілю і вказувати мінімум персональної інформації, такої як вік, школа та місце проживання.

7. Зверніть увагу на вік «цифрової згоди». У деяких країнах діють закони, що встановлюють мінімальний вік, починаючи з якого компанії або вебсайти можуть просити дітей повідомити персональну інформацію без попереднього отримання підтвердженої згоди батьків. Вік «цифрової згоди» зазвичай варіюється в межах 13-16 років. На багатьох вебсайтах, призначених для дітей молодшого віку, потрібна згода батьків для реєстрації нового користувача.

8. Дізнайтеся, як повідомити про проблему на платформах, якими користуються ваші діти, і як видалити профіль або змінити зазначену в ньому інформацію.

9. Розкажіть про важливість персональної інформації. Поясніть дітям, що їм слід ділитися тільки тією інформацією, яку, на вашу і на їхню думку, дозволено побачити стороннім. Їм не слід ділитися інформацією, що дозволяє встановити їхню особистість або 65 Умовні позначення Зміст курсу особистість інших. Нагадайте дітям, що в них є онлайн репутація, за якою необхідно стежити, а після того, як контент опубліковано, його може бути складно змінити або скорегувати.

10. Переконайтеся, що діти розуміють, що означає публікація світлин та відео в Інтернеті, в тому числі їхніх власних та їхніх друзів. Поясніть дітям, що фотографії та відео можуть розкривати безліч персональної інформації. Діти повинні розуміти ризики, пов'язані з використанням камер та опублікуванням контенту. Бажано, щоб світлини інших людей не викладалися без їхньої згоди. Це також стосується і батьків, які роблять та публікують знімки своїх дітей. Крім того, важливо, щоб діти розуміли, що іноді інформацію може розкрити хтось із їхніх друзів або членів сім'ї, тому їм варто поговорити про це зі своїми друзями та родичами і розповісти про небезпеку надмірного розкриття інформації. Порадьте своїм дітям не

викладати власні фото та відео або фото та відео друзів, на яких є елементи, що легко піддаються ідентифікації, наприклад, таблички з назвами вулиць, автомобільні номери або назва заклади освіти на толстовках тощо.

Всі учасники освітнього процесу повинні з повагою ставтеся один до одного, адже безпека як очного, так і дистанційного навчання залежить від педагогів, батьків, здобувачів освіти.

Заступник директора з НВР Тетяна БАЧУРСЬКА

Голова ради трудового колективу Ольга СМІШКО

Директор Світлана ПРИТУЛА