ПОСІБНИК

Ініціатива «Модельні суди»

ОСОБИСТА БЕЗПЕКА СУДДІВ ТА ПРАЦІВНИКІВ АПАРАТУ СУДУ

ПРЯМУЄМО РАЗОМ

ПРОЕКТ ФІНАНСУЄТЬСЯ ЄВРОПЕЙСЬКИМ СОЮЗОМ

ПРАВО-JUSTICE

З М І С Т

I. ЗАГАЛЬНА ІНФОРМАЦІЯ

Кому адресований Посібник?

Цей Посібник адресований суддям та працівникам апарату суду, які не відповідальні за безпекові питання, однак їм потрібно знати, як влаштована та функціонує система безпеки суду та як діяти у надзвичайних ситуаціях.

Посібник має на меті підвищити обізнаність щодо питань безпеки в цілому, а також спонукати планувати щоденну діяльність з урахуванням міркувань особистої безпеки.

Наявні процедури та заходи безпеки не мають сенсу, якщо про них не знають або не дотримуються, саме тому суддям та працівникам апарату суду важливо розуміти, що вони є учасниками системи безпеки, а не лише бенефіціарами.

Безпека починається з кожного з нас!

Організація особистої безпеки. Як це працює?

Обізнаність з правилами безпеки в будівлі суду та діяльністю інституцій, які відповідальні за її створення – це інформаційний мінімум, який будь-який роботодавець повинен надати працівникові, проте важливо усвідомлювати і Вашу особисту роль у цьому процесі.

Потрібно розуміти, що більшості потенційно небезпечних ситуацій передують ознаки, які можна помітити та ідентифікувати, проявивши належну пильність, зокрема:

- нападу на початковому етапі передують **погрози** або **стеження**,
- для шантажу спочатку потрібно зібрати **компромат**,
- замах на безпеку інформації зазвичай має місце після **спроб отримати інформацію** через різні канали тощо.

Саме тут Ви, як працівники судової системи, стаєте мішенню, однак вже на цьому етапі можете виявити перші ознаки незвичайної ситуації чи неминучої загрози.

Ось чому володіння ситуацією є настільки важливим для раннього виявлення спроб заподіяння шкоди особистій безпеці суддів та працівникам апарату суду, їх майну, інформації та процесам у цій сфері діяльності.

Що Ви знайдете у цьому Посібнику?

- **Базова інформація про процес управління безпековими ризиками**

Даний розділ містить інформацію про те, як функціонує система управління ризиками та її складові елементи, як самостійно здійснити аналіз ситуації та потенційних загроз та як мінімізувати або уникнути їх наслідків.

- **Організаційні обов'язки щодо забезпечення безпеки судів**

Загальні рекомендації даного розділу допоможуть зорієнтуватись у разі виникнення надзвичайної ситуації, яка становить загрозу особистій безпеці, а також знайти відповіді на питання:

- Що таке фізичний і загальний контроль?
- У чому суть надзвичайних процедур і планів дій у надзвичайних ситуаціях?
- Для чого потрібно повідомляти про інциденти, що трапляються під час службової діяльності?

- **Володіння ситуацією та особиста безпека**

Розділі присвячено інформації про заходи, яких потрібно дотримуватись для контролю над ситуацією не залежно від місця перебування, а також порадам щодо моделі поведінки для зменшення загроз особистій безпеці.

Взаємозв'язок індивідуальних та організаційних обов'язків розкриває суть ефективного поєднання особистих обов'язків працівників суду та організаційних обов'язків роботодавця для встановленні надійної системи безпеки у суді.

Пропонуємо взяти участь у короткому опитуванні за цим посиланням

II. БАЗОВА ІНФОРМАЦІЯ ПРО ПРОЦЕС УПРАВЛІННЯ БЕЗПЕКОВИМИ РИЗИКАМИ

• Вступ до процесу управління безпековими ризиками

Процес управління безпековими ризиками – це щоденна діяльність, що стосується заходів безпеки і вимагає принаймні здорового глузду в діях кожного. По суті, це процес прийняття рішень щодо того, як безпечно досягти поставленої мети: знаючи, що ми хочемо зробити, ми оцінюємо спосіб та час, коли це безпечно зробити, залежно від ситуації. Наприклад, плануючи подорож, необхідно переглянути прогноз погоди (це оцінювання). Знаючи про ймовірність дощу, можна розглянути кілька можливих сценаріїв поведінки: скасувати поїздку (захід уникнення ризику) або взяти з собою парасольку (захід, спрямований на пом'якшення, зменшення наслідків).

Процес управління безпековими ризиками – це необхідна оцінка викликів, пов'язаних із безпекою, яких вимагає будь-який вид діяльності, задля вжиття незалежних заходів безпеки. Можливість застосування будь-яких заходів безпеки повинна розглядатись лише за результатами оцінки ризику безпеки кожної конкретної ситуації, та за умови наявності загрози завдання шкоди працівникам, їх майну, інформації чи діяльності.

Процес управління ризиками безпеки

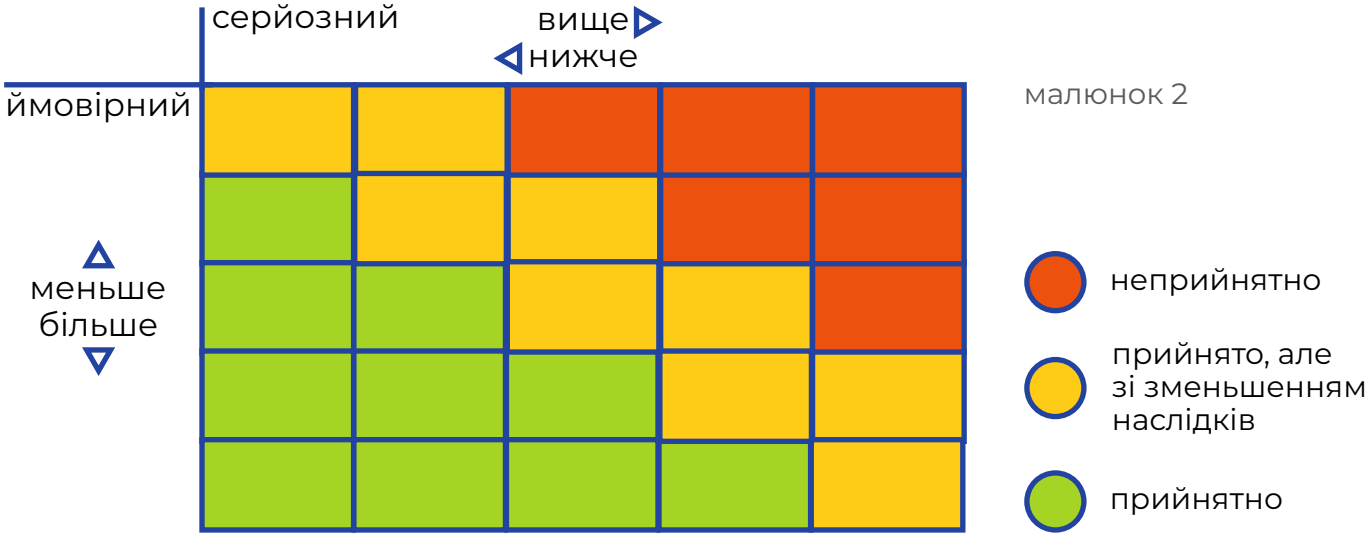
малюнок 1

Розглядаючи управління ризиками, застосовують такі терміни, як запобігання та пом'якшення наслідків. Профілактичні заходи покликані знизити ймовірність виникнення події, тоді як заходи з пом'якшення наслідків – зменшують наслідки шкідливої події. Використовуючи спеціальну матрицю, можна належним чином оцінити та скерувати ризик.

Більш детально про терміни та етапи управління ризиками безпеки за посиланням.

• Оцінка безпекових ризиків

Конкретні загрози для суду та його працівників встановлюються шляхом **оцінки безпекових ризиків**, що є процесом визначення ймовірності настання шкідливої події (загрози) та її **наслідків/тяжкості**, якщо вона відбудеться. Рівні ризику, можуть визначатися за матрицею (малюнок 2), яка встановлює їх перелік у зв'язку із виявленими загрозами. Рівень ризику варіюється залежно від імовірності виникнення небезпечної ситуації та наслідків/тяжкості, якщо вона настане.



малюнок 2

Низький рівень ризику є наслідком меншої ймовірності виникнення загрози та незначних наслідків/тяжкості у разі настання випадку. Відповідно, більш висока ймовірність виникнення та серйозніші наслідки/тяжкість означатимуть вищий рівень ризику. Саме тому, перед усіма установами постає завдання адаптувати заходи безпеки на основі оцінки ризику, переконавшись у тому, що вони містять плани дій та процедури, спрямовані на подолання високого рівня ризику, і які застосовуватимуться, поки не зменшиться ймовірність його виникнення та не мінімізуються наслідки/тяжкість.

Ризик можна:

- **Контролювати** шляхом застосування пом'якшувальних заходів для його зменшення до прийнятного рівня.
- **Приймати**, якщо ймовірність його настання або наслідки є не дуже шкідливими.

- **Уникати**, тобто не вчиняти певних дій за певних обставин, наприклад, чекати на інший час чи умови.

- **Перенести** – на практиці означає надання іншим можливості виконати цю роботу; тим, хто може мати інший підхід до цієї діяльності або іншу вразливість перед загрозою.

Контрольовані ризики – це ті, щодо яких є заходи, розроблені для зменшення ймовірності виникнення або тяжкості/наслідків. Саме це і пропонують установам фахівці з безпеки – заходи, спрямовані на контроль за ризиками шляхом зменшення ймовірності їх виникнення або мінімізації наслідків за умови настання такої ситуації.

Більш детально за QR-кодом

• Стратегії та заходи щодо управління безпековими ризиками

Стратегія управління безпековими ризиками є процесом вибору заходів та процедур, спрямованих на зниження рівня ризику виявлених загроз до прийнятної відмітки. Стратегії залежать від наявних коштів, доступності ресурсів і матеріалів, рівня знань в аспекті можливості реагування осіб, відповідальних за безпеку тощо. Після узгодження заходів, які мають бути реалізованими, визначаються пріоритети, розробляється план закупівель та навчання осіб, відповідальних за безпеку суду.

Стратегія управління безпековими ризиками реалізується в Плані безпеки та містить стандартні процедури, мінімальні операційні стандарти безпеки, плани дій у надзвичайних ситуаціях та план евакуації. **Реалізація заходів безпеки** повинна зменшити ризики до **прийнятного рівня**.

Прийнятні ризики – це ризики, зменшені до рівня, який установа вважає допустимим. Інша назва цьому – це схильність до ризику, тобто фактична демонстрація того, наскільки далеко установа готова піти, толеруючи ризики до моменту їх контролю.

Періодично цей процес потребує **перегляду** заходів безпеки, у зв'язку з виявленням нових загроз (викликів), або у зв'язку з поліпшенням **ситуації** з безпеки, адже це може дозволити припинити вжиття певних заходів.

Відповідний цикл процесу управління безпековими ризиками, який проводиться спеціалістами при прийнятті рішення щодо вжиття заходів безпеки, необхідних для захисту конкретної особи зображений на малюнку 1.

ВАЖЛИВО ПАМ'ЯТАТИ!

Усі ми щодня проводимо різні оцінки та ухвалюємо рішення на їх основі. Розуміння процесу оцінювання професійних ризиків не тільки допоможе визначити потенційні ризики безпеки, але й покращить способи прийняття рішень, а, отже, сприятиме досягненню нашої мети, а саме кращому володінню ситуацією навколо.

III. ОРГАНІЗАЦІЙНІ ОБОВ'ЯЗКИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СУДІВ

• Фізичний і загальний контроль

Законодавством передбачений обов'язок роботодавця забезпечити належні та безпечні умови праці своїм працівникам. Саме тому важливо, наскільки ефективними є заходи безпеки, розроблені для забезпечення потреб організації, та закріплені в план безпеки, який містить масив інформації щодо заходів, ресурсів, стандартних процедур з організації безпеки та плану дій у надзвичайних ситуаціях.

Фізична безпека приміщення, залежно від оцінки безпеки, покликана забезпечити безпеку шляхом застосування контролю, який повинен стримувати, виявляти (ідентифікувати загрозу) та затримувати ворожу чи небезпечну подію за рахунок заходів безпеки.

Комплексний захист – це загальне поняття, яке застосовується в контексті безпеки. Комплексний захист стосується використання кількох рівнів безпеки та заходів, які протилежна сторона повинна подолати, щоб отримати доступ до захищеної території. У контексті безпеки, комплексність, яка означає певну надмірність, досягається за рахунок того, що вимагає від протилежної сторони вчинення певних додаткових дій. Наприклад, за умови будь-якого розвитку подій, перш ніж отримати можливість вчинити замах на крадіжку чи диверсію, необхідно подолати кілька послідовних заходів безпеки. Щоб переконатися в наявності такої комплексності, заходи розробляються за рівнями безпеки, ніби оточуючи охоронювану територію. Комплексність передбачає кілька рівнів захисту. Більш детально про організаційні заходи безпеки судів за цим посиланням.

На практиці, окрім фізичної охорони з боку працівників Служби судової охорони, Національної поліції чи Національної гвардії та застосовуваних ними процедур щодо захисту працівників суду та будівлі, існує також охоронне обладнання, призначене для контролю доступу та переміщень в приміщеннях з обмеженим доступом.

Додатково пропонуємо переглянути відео вебінару «Особиста безпека суддів та працівників апарату суду» за QR-кодом

• Надзвичайні процедури та плани дій у надзвичайних ситуаціях

Наведені приклади планів дій у надзвичайних ситуаціях можуть бути впроваджені, протестовані та відпрацьовані залежно від оцінки безпеки в аспекті ймовірності настання наслідків та відповідного попереднього досвіду.

Евакуація з будівлі

Необхідно підготувати план евакуації для кожної конкретної будівлі як частину планування безпеки. План евакуації з будівлі – це робочий документ, з яким всі співробітники повинні ознайомитися, знати його положення та виконувати процедури. Він містить керівні принципи та опис обов'язків різних суб'єктів для успішного проведення евакуації з будівлі.

Опинившись на місці події першим, потрібно оцінити ситуацію та вирішити, чи має ситуація ознаки надзвичайної і чи потрібно повідомити про неї.

У випадку надзвичайної ситуації потрібно повідомити інших осіб в будівлі про неї, увімкнувши сигналізацію (за наявності), покликати на допомогу, зателефонувати або в інший спосіб поширити інформацію про небезпеку.

«Блокування» (локдаун) як засіб захисту від нападу

Ця процедура застосовується, коли є підстави вважати, що правопорушник знаходиться у приміщенні або здійснює безпосередній напад на будівлю. «Блокування» передбачає вибір внутрішньої кімнати або кімнат у будівлі, де немає вікон (або вони захищені), і переховування там. Такі заходи мінімізують ризик конфронтації осіб, які перебувають у будівлі, з правопорушником.

Блокування необхідно реалізувати негайно, як тільки сталася надзвичайна подія, і воно вимагає оперативного реагування та втручання з боку правоохоронних органів. Такий план дій дозволяє пом'якшити ризики, зменшивши тяжкість надзвичайної події, а також час повернення до роботи після блокування. Цей процес повинен бути децентралізованим, щоб будь-який працівник, який наражається на невідворотну небезпеку для життя, мав можливість запустити процедуру блокування.

План дій у випадку виявлення підозрілого пакунку

Планування дій за умови виявлення підозрілих пакунків має проводитися за результатами оцінки безпеки в певній місцевості. Інформація про попередні інциденти, а також характер злочинів у цій місцевості вкажуть на те, коли такі плани мають бути підготовлені у певній локації.

Варто взяти до уваги, що вибухові речовини можна замаскувати так, щоб вони були схожі на буденні предмети, такі як листи та/або посилки, або заховати у відносно невеликі сумки, валізи тощо.

Розроблений план дій повинен встановлювати чіткі процедури поводження з будь-яким підозрілим пакунком (листи, речі без нагляду), щоб працівник суду міг оцінити та визнати за зовнішнім виглядом, місцезнаходженням та обставинами можливу загрозу та діяти відповідно. Такий план має бути чітким, зрозумілим та враховувати специфіку будівлі конкретного суду.

Відповідальність за дії в цьому випадку покладається на того, хто виявляє пакунок, або тих, хто навчений/має обов'язок реагувати.

План дій у випадку наявної загрози вибуху

Сьогодні загроза вибуху є цілком імовірною, і її не слід сприймати легковажно. Деякі правопорушники попереджають установу про закладання бомби, можливо, тому що бажають пошкодити майно, а не заподіяти шкоду життю та здоров'ю людей, або бомби немає, а метою є зрив нормального порядку роботи установи.

Інстинктивною реакцією на загрозу може стати заклик до евакуації, проте, це не завжди найкращий варіант. Постійна евакуація підриває впевненість у здатності керівництва забезпечувати безпечне та сприятливе робоче середовище. Це також може призвести до появи наслідувачів: незадоволений працівник може спробувати таким чином отримати вільний від роботи час, сторонні особи можуть отримати вигоду із перспективи зриву діяльності установи, або відповідне повідомлення може бути способом здійснити напад на працівників, коли вони знаходяться за межами будівлі.

Усі працівники суду повинні знати, як діяти, якщо вони отримують дзвінок із погрозою вибуху.

Рекомендації у випадку отримання повідомлення про загрозу вибуху (бомбу)

Якщо надійшло повідомлення про загрозу вибуху/бомбу, потрібно:

а) Під час дзвінка:

- зберігати спокій;
- за можливості повідомити найближчому колезі про надзвичайну ситуацію (подати знак та вказати на телефон);

- не відключатися і не класти слухавку, адже абонент має закінчити своє повідомлення, не будучи перерваним;

- спробувати зібрати якомога більше інформації;

- звернути увагу на будь-які відмінні риси голосу абонента, такі як стать, акцент, тембр голосу, манера розмови;

- запитати додаткову інформацію, де і коли була розміщена бомба та коли вона вибухне;

- спробувати записати точне формулювання повідомлення (диктофон, папір, відео);

- звернути увагу на те, як суб'єкт описує, місцезнаходження бомби, щоб зрозуміти, наскільки добре він/вона знає будівлю.

б) Після дзвінка:

- негайно попередити керівництво суду та представників Служби судової охорони;

- записати детальну інформацію, якщо не було можливості зробити це під час дзвінка;

- залишатися на зв'язку, як єдиний свідок події.

в) Додаткові дії при отриманні письмового повідомлення про загрозу вибуху /бомбу:

- записати час та спосіб отримання повідомлення;

- якщо повідомлення було вручене особисто, занотувати, як виглядав кур'єр (за можливості);

- якомога менше чіпати конверт та пакунок;

- негайно помістити повідомлення (конверт, пакунок) у чистий прозорий пластиковий пакет;

- якщо повідомлення з погрозою надійшло електронною поштою, не видаляти його (з заголовка повідомлення можна зібрати багато інформації) та повідомити керівництво суду та представників Служби судової охорони.

Рекомендації у випадку загрози від мін, саморобних вибухових пристроїв, вибухонебезпечних предметів

Як правило, у більшості місць ймовірність того, що працівники суду постраждають від мін, пасток-«розтяжок», саморобних вибухових пристроїв або вибухонебезпечних предметів, є дуже низькою, але в деяких особливих регіонах необхідно і важливо мати детальні знання про цей тип загрози та бути в курсі того, як зменшити супутні ризики.

Наголошуючи на необхідності зберігати пильність, спеціалісти вважають, що в районах, де виявлено ризик натрапити на вибухові пристрої, працівники повинні бути в змозі **розпізнати та ідентифікувати місця**, де раніше могли використовуватися міни, саморобні вибухові пристрої, вибухонебезпечні предмети або закладатися мінні поля.

Такі плани розробляються у співпраці зі спеціалізованими підрозділами поліції та військовими, і необхідним є проведення практичної спеціалізованої підготовки, щоб персонал ознайомився з процедурами, якщо в місцевості, де вони працюють, раніше траплялися подібні інциденти.

Рекомендації у випадку небезпеки від «активного стрільця»

Хвиля інцидентів з активними стрільцями та активними нападниками підкреслює непередбачуваний характер подібних подій, а також важливість ухвалення певних захисних заходів безпеки для пом'якшення потенційних наслідків. Історія випадків стрілянини є дуже динамічною, і жоден перелік процедур чи рекомендацій не може охопити всі аспекти. Більшість випадків скоїв один нападник, але деякі вчиняли організовані групи, або вони були складовою комплексної атаки (потім слідували вибухи), або як спосіб уразити слабку ціль, якій бракує ґрунтовних оперативних та матеріально-технічних можливостей, для підготовки захисту від масштабної атаки.

Враховуючи те, що стрілянина може відбуватися в приміщенні суду чи навколо нього, такі події напряму пов'язані з евакуацією з будівлі або планами дій «блокування/локдаун» (про що зазначалося вище). На певному етапі будь-який із цих планів дій у надзвичайних ситуаціях передбачає найкращий спосіб захисту життя людей, допоки не прибудуть сили збройного реагування у складі представників правоохоронних органів та інших силових структур.

Рекомендації у випадку прямих особистих погроз

Будь-хто може стати жертвою цькування, настирливої чи недоречної поведінки з особистих причин, проте працівники суду перебувають у зоні такого ризику через конкретні службові функції, або можуть стати «випадковим» адресатом більш масштабної погрози, спрямованої на судову систему.

Ці загрози можуть включати випадкові хуліганські телефонні дзвінки, часті безглузді дзвінки, дзвінки і мовчання, нецензурні дзвінки або прямі погрозливі повідомлення з використанням будь-яких засобів зв'язку, в тому числі, електронної пошти, поштової кореспонденції, повідомлень в соціальних мережах. Метою є встановлення реального значення конкретного інциденту, ідентифікація джерела загрози, встановлення конкретної мети та цілей, а також важливо оцінити реальність загроз та наслідків, щоб є основою для розробки правильної стратегії реагування.

Рекомендації у випадку небезпеки захоплення заручників

У ситуаціях із захопленням заручників з урахуванням вимог національного законодавства, можуть використовуватися різні терміни, зокрема такі як: незаконне позбавлення волі або викрадення людини, незаконне утримання або захоплення заручників.

Детальніше про особливості управління кризовими ситуаціями у випадку захоплення заручників за цим посиланням.

У всіх є спільна риса - люди позбавлені свободи пересування, але характер та/або мотиви викрадачів можуть будуть різними. Для цілей безпеки зазначені ситуації мають тактичні відмінності при виборі стратегії і плану, оскільки при викраденні людини її місцезнаходження не відоме, і переговори з викрадачами є основним інструментом вирішення ситуації. В той же час при захопленні заручників їх місцезнаходження, як і місце знаходження правопорушників відоме органам правопорядку. У зв'язку з цим стратегії управління кризовими ситуаціями будуть відрізнятися.

Більше інформації про переговори в кризових ситуаціях можна знайти, переглянувши відео вебінару року «Особиста безпека суддів та працівників апарату суду» за QR-кодом

Демонстрації/Несанкціонований вхід/незаконне зайняття приміщень

Демонстрація – це форма ненасильницьких дій групи людей, викликаних політичними або іншими міркуваннями, які зазвичай виражається у формі маршу та/або зустрічі (мітингу) для виступу з промовами. Такі дії, як блокування, також можуть називатися демонстраціями. Ці рекомендації стосуються демонстрацій, які є абсолютно або принаймні відносно мирними.

Проте мирні дії демонстрантів можуть перетворитися на протест чи бунт, і передбачити спалах насильства у такій ситуації неможливо. Саме тому ймовірність раптового виникнення насильства має бути складовою постійного моніторингу та аналізу ситуації.

Детально про рекомендації щодо заходів безпеки під час демонстрацій та інших загроз при порушенні громадського порядку за QR-кодом

Ці рекомендації також можуть застосуватися до наступних подій – «мирний» несанкціонований вхід чи незаконне зайняття приміщень. В таких випадках учасники вище вказаних заходів не становлять прямої загрози фізичній безпеці працівників, навіть коли їхнє ставлення є досить ворожим. Необхідно відрізняти ці випадки від ситуацій із вторгненням озброєних зловмисників або інших видів прямих атак, для яких відповідне реагування прописано в плані дій у разі блокування або евакуації з будівлі.

Невідкладна допомога

Надати першу невідкладну допомогу, щоб врятувати чиєсь життя, знаючи загальні принципи надання першої допомоги та за наявності базового обладнання – це ті знання та навички, якими повинні володіти працівники суду.

Надання першої допомоги – це практична навичка, тому необхідно регулярно проходити практичні навчання. Метою такого навчання є не створення довідкового посібника про надання першої допомоги чи будь-якого виду медичного лікування, а уточнення плану дій, якого слід дотримуватись у надзвичайних ситуаціях, коли потрібна невідкладна медична допомога.

Наразі перелік дії на випадок надзвичайних ситуацій не є вичерпним, і його слід доповнити спеціальними навчаннями, заснованим на оцінці безпеки діяльності у відповідній місцевості та специфіці кожної конкретної будівлі, де розташований суд.

• Повідомлення про інциденти

Повідомлення про інцидент є одним з найбільш важливих заходів, відповідальність за виконання якого несуть працівники.

Навіщо повідомляти?

Важливо, щоб кожен співробітник усвідомлював, що відсутність повідомлення про інцидент призведе до цілої низки негативних наслідків:

- статистика буде помилковою, оскільки не відображатиме реальну кількість інцидентів;
- ресурсів, що виділяються на вирішення конкретних видів ситуацій, буде недостатньо, оскільки здаватиметься, що в них немає потреби;
- виникне імовірність, що інші співробітники стануть жертвам аналогічних ситуацій, оскільки не будуть вживатися потрібні заходи чи проводитися розслідування;
- допомога конкретній особі не буде надана, оскільки не буде інформації що вона потрібна, в той час як сама особа не буде знати, що може її отримати.

Повідомлення про інцидент зазвичай може здійснюватися за допомогою двох різних каналів залежно від потреб: невідкладно, коли допомога потрібна терміново, і «для запису» – здебільшого у ситуаціях, що не потребують негайних дій.

- Офіційний канал – це тип повідомлення, коли інформація офіційно повідомляється компетентним правоохоронним органам та реєструється, разом із діями щодо реагування.
- Неофіційний канал – це тип повідомлення про підозрілу діяльність працівнику охорони в будівлі або працівнику поліції на вулиці.

Про що необхідно повідомляти?

- необхідно повідомляти про всі підозрілі дії;
- потрібно оцінити тяжкість інциденту: чи може він стосуватись інших працівників? Як він може загостритися? Чи може він скомпрометувати вашу організацію?

Що важливо під час підготовки повідомлення про інцидент?

Під час підготовки повідомлення, слід не забувати про зазначення: **часу і дати, хто, що, де, коли, чому [+як] – послідовність подій, опис зовнішності всіх причетних і свідків**.

Повідомлення про інциденти, пов'язані з безпекою, потрібно регулювати на рівні, що забезпечить правильне реагування у разі виникнення надзвичайних ситуацій. Такі процедури вимагають затвердження стандартної операційної процедури, яка регулює порядок комунікації між працівником, який повідомляє, керівництвом і працівником, відповідальними за забезпечення безпеки та відповідне реагування.

IV. ВОЛОДІННЯ СИТУАЦІЄЮ ТА ОСОБИСТА БЕЗПЕКА СУДДІВ ТА ПРАЦІВНИКІВ АПАРАТУ СУДУ

- **Володіння ситуацією та особиста безпека працівників суду**

- Володіння ситуацією вимагає обізнаності про те, що відбувається навколо і як це може негативно вплинути, зокрема, на:

- постійне усвідомлення власності або доступу до певного майна;

- розуміння загроз майну;

- усвідомлення особистих уразливих сторін у контексті загроз;

- усвідомлення свого оточення.

Підтримка належного рівня володіння ситуацією дозволяє вжити відповідних заходів для запобігання та зменшення ризиків, що викликають найбільше занепокоєння. Важливо повідомляти Службу судової охорони або керівництво суду про інциденти або про підозрілу діяльність.

Особиста безпека суддів та працівників апарату суду залежить від:

- управління ризиками безпеки, за якою основним активом є людина, а також майно суду, до якого наявний доступ або воно знаходиться у розпорядженні.

- розуміння власних активів, до яких належить безпосередньо життя та здоров'я людини, її родина, дім та майно, всі вони вразливі перед загрозами та іншими випадковими небезпеками.

- усвідомлення, що робота в суді може потенційно збільшити загрозу для такого працівника, а також збільшити кількість активів, за захист яких цей працівник несе відповідальність.

Для забезпечення особистої безпеки необхідно дотримуватися наступних рекомендацій:

- слід пам'ятати, що особиста безпека – це, перш за все, персональна відповідальність особи;

- розуміти, що працівник, який є частиною судової системи потенційно зазнає більшого ризику;

- уникати передбачуваності в пересуванні та обирати відповідні альтернативні маршрути;

- ставитись підозріло до всіх, хто запитує інформацію про місце роботи та службові (посадові) повноваження;

- не оприлюднювати особисту інформацію або інформацію, пов'язану з колегами по роботі, через соціальні мережі, електронні засоби комунікації;

- уникати втрат інформації, пов'язаної з роботою, або документів, які посвідчують особу/забезпечують контрольований доступ;

- пам'ятати, що анонімність – це першочергова лінія захисту;

- повідомляти про будь-які особисті підозри та переживання щодо власної безпеки, оскільки відсутність інформації виключить можливість надати відповідну своєчасну допомогу, що може призвести до збільшення кількості жертв.

Додаткова інформація про заходи особистої безпеки працівників суду у за цим посиланням.

У випадку користування громадським транспортом слід пам'ятати про три аспекти:

1. Існування загрози з боку інших людей (в т.ч. застосування сили, вчинення крадіжки, залякування, антисоціальна поведінка).

З метою мінімізації ризиків особистій безпеці у транспорті потрібно дотримуватись наступних основних рекомендацій:

- залишити вдома цінні речі, а особисті речі тримати поруч і в полі зору;

- документи і гроші тримати біля себе;

- завчасно підготувати суму без здачі;

- детальніше за посиланням.

2. Питання безпеки, пов'язані із постачальниками послуг перевезень:

- самостійно вивчити маршрут, потенційні загрози, типи пасажирів та повсякденні дії;

- перевірити наявність найближчого виходу, пожежного виходу, сигналізації;
- перевірити якість обслуговування за відгуками та репутацію постачальника.

3. Особисті афективні аспекти (емоційний стан: впевненість і манера тримати себе):

- у разі появи некомфортного відчуття краще вийти;
- продумувати заздалегідь сценарій відносно того, що може піти не так і як вирішити ситуацію;
- бути готовим покликати на допомогу у доступний спосіб;
- детальніше за посиланням.

Більше інформації можна знайти, переглянувши відео вебінару «Особиста безпека суддів та працівників апарату суду на транспорті» за QR-кодом

Основні рекомендації щодо фізичного контролю безпеки:

- потрібно завжди зберігати пильність, спостерігати та усвідомлювати те, що відбувається навколо;
- повідомляти про підозрілі дії (особи, які отримають цю інформацію, зможуть більше знати або зрозуміти по-іншому, що відбувається);
- мати при собі посвідчення особи в приміщеннях, де перебуває багато відвідувачів та різні зони мають різний рівень доступу. Це допоможе оперативно відрізнити працівників від інших людей у випадку виникнення небезпеки;
- не викидати непотрібні документи, вони мають бути знищені аби уникнути використання їх зловмисниками як компромату;
- зберігати паролі у безпечному місці, розголошення іншим особам може призвести до негативних наслідків;

- захищати особисті мобільні пристрої та ноутбуки, не залишати їх без нагляду;

- пам'ятати, що пристрої, підключені до мережі Інтернет, легко перетворити на засоби спостереження, за допомогою яких можна отримати доступ до всієї інформації, а також визначити місцезнаходження, зображення та оточуючий звук;

- ознайомитись з планами дій та процедурами у надзвичайних ситуаціях, оскільки ефективність таких процедур напряму залежить від обізнаності суб'єктів.

Для того, щоб забезпечити фізичний контроль, який надає можливість зменшити ризики безпеки для інформації з обмеженим доступом, потрібно:

- зберігати документи у папках, щоб запобігти випадковій демонстрації;

- дотримуватись «Правила чистого столу» – систематично прибирати усі документи та предмети наприкінці робочого дня;

- зберігати документи та файли у замкнених шафах;

- не залишати особистий кабінет з відчиненими дверима;

- дотримуватись встановленого режиму зон з обмеженим доступом та не допускати сторонніх осіб до зон із обмеженим доступом;

- зберігати конфіденційні документи у робочих приміщеннях, якщо відсутній дозвіл на їх переміщення та заходи безпеки для віддаленої роботи, а для їх знищення використовувати шредери (слід пам'ятати, що не всі шредери роблять свою роботу належним чином);

- використовувати електронну систему відстеження ключів для забезпечення безпеки ключів від кабінету;

- переносити із собою якомога менше інформації, оскільки випадкова втрата є значним ризиком, про настання якого необхідно оперативно повідомляти відповідальних осіб;

- свідомо користуватись засобами зв'язку, усвідомлюючи можливість несанкціонованого відстеження та фіксації.

• Інформаційна безпека суддів та працівників апарату суду

Інформаційна безпека розглядає інформацію як актив у процесі управління ризиками. Ця категорія активів є найбільш вразливою, оскільки не завжди очевидно, коли на неї здійснюється атака. Рівні захисту інформації визначаються на основі оцінки важливості інформації, її чутливості, а також наслідків чи тяжкості шкоди, що може бути нанесена внаслідок її розкриття. Більш детально про значення інформаційної безпеки за цим посиланням.

У питанні інформаційної безпеки важливим є електронний контроль, який допомагає зменшити ризик викрадення інформації, саме тому необхідно дотримуватись наступних рекомендацій:

- використовувати якісні паролі, що містять мінімум вісім і більше символів та літерно-цифрових символів;
- змінювати періодично пароль від робочого столу або входу до персонального комп'ютера (ноутбука), а також використовувати різні паролі для різних типів рахунків;
- вимикати комп'ютер (ноутбук) наприкінці дня (для оновлень та безпеки);
- зберігати файли у мережевих папках, а не на робочому столі та уникати збереження інформації на USB або інших переносних носіях;
- з обережністю надсилати інформацію електронною поштою;
- використовувати затверджене шифрування та ліцензійне програмне забезпечення, щоб мінімізувати ймовірність несанкціонованого розкриття інформації;
- не відкривати вкладені файли та посилання з невідомих електронних листів або з невідомих джерел, що видаються підозрілими (за формою, написанням, темою, дизайном тощо);
- намагатись не підключатися до службової мережі з публічних комп'ютерів та точок Wi-Fi;
- пам'ятати, що громадські бездротові підключення не є безпечними;
- не завантажувати конфіденційні документи зі службової мережі на загальнодоступний комп'ютер і не вмикати опцію автоматичного заповнення «збереження пароля»;

- використовувати особисту, а не службову адресу електронної пошти, щоб зареєструватися на онлайн-сервісах або оформити підписки, які не пов'язані з роботою;

- під час друку конфіденційних (вразливих) документів, не залишати їх та знаходитись біля принтера, непотрібні або пошкоджені документи підлягають знищенню у порядку, визначеному вище;

- не залишати без нагляду ноутбуки та/або документи;

- дотримуватися інших заходів захисту персональних даних та інформаційної безпеки.

Додаткову інформацію про заходи інформаційної безпеки та електронного контролю можна дізнатись переглянувши відео вебінару «Цифрова безпека: як не потрапити в пастку інформаційних технологій» за QR-кодом

Для оцінки рівня особистої інформаційної безпеки пропонуємо взяти участь у короткому опитуванні за цим посиланням.

- **Взаємозв'язок індивідуальних та організаційних обов'язків забезпечення безпеки**

Обов'язком роботодавця є забезпечення належних умов праці працівникам, а безпека є невід'ємною складовою цього процесу. Про запроваджені заходи безпеки працівників повинні повідомляти під час інструктажів із безпеки, навчальних занять та таких заходів, як тренувальна евакуація.

На індивідуальному рівні від кожної працівника вимагається обізнаність із питань безпеки, а також здатність самостійно виявити ознаки потенційно небезпечної ситуації. Усе починається з того, що суддів та працівники апарату суду не завжди звертають увагу на перші ознаки підозрілої поведінки, що вимагає пильності та відповідного навчання, щоб набути здатності реагувати у разі настання певної ситуації.

Рекомендації щодо поінформованості з питань безпеки:

- необхідно систематично працювати над підвищенням розуміння процедур та протоколів безпеки у робочому (службовому) середовищі;
- цікавитись наявними тренінгами з конкретних тем, що стосуються професійної сфери діяльності;
- розвивати відчуття безпеки та орієнтуватися на нього у всіх своїх діях;
- дотримуватись правил і просити оточуючих робити те саме – передусім правила існують для забезпечення особистої безпеки;
- відпрацьовувати найбільш реальні сценарії з відповідальними за безпеку особами для спільного розуміння дій, які слід зробити у випадку настання небезпечної ситуації.

Існує чітка взаємозалежність між тим, що організація зобов'язана надавати, і тим, що вимагається від особи, і обов'язки обох сторін потрібно регулярно відпрацьовувати та забезпечувати їхнє функціонування в залежності від конкретних потреб, які були з'ясовані під час оцінювання ситуації у сфері безпеки.

Організація може вжити найкращі заходи безпеки в будівлі, але якщо співробітник тримає двері для евакуації відкритими, для власних потреб, усі умови, створені на центральному вході опиняються під загрозою. Те саме з дезактивацією детектора диму в офісі або з проханням не проходити перевірку на вході, оскільки працівника давно і добре знають тощо.

Можна запроваджувати та інвестувати в найкращі механізми реагування на безпеку персоналу, але якщо працівник не знає про існування цих інструментів, то всі інвестиції будуть марними і не виконуватимуть свого призначення.

Важливо бути обізнаним у питаннях забезпечення безпеки,

Найвищий рівень безпеки – це Ваше розуміння реальності!

Цю публікацію створено в рамках Проєкту ЄС "Право-Justice" та за фінансової підтримки Європейського Союзу. Її зміст є відповідальністю Проєкту ЄС "Право-Justice" та не обов'язково відображає офіційну позицію Європейського Союзу.

ПРЯМУЄМО РАЗОМ
ПРОЕКТ ФІНАНСУЄТЬСЯ ЄВРОПЕЙСЬКИМ СОЮЗОМ

ПРАВО-JUSTICE