**Тема 8. Політика інформаційної безпеки для установ, що здійснюють наукову діяльність**

План

1. Сфера застосування політики інформаційної безпеки

2. Документальне забезпечення політики інформаційної безпеки. Політика Due Diligence

3. Ролі та обов’язки політики інформаційної безпеки

Розширення ІТ інфраструктури та інформаційних технологій тягне з собою появу все більшої кількості ризиків і сфері інформаційної безпеки. Надійний партнер має усвідомлювати і задекларувати шляхом добровільної сертифікації рівень відповідальності за збереження конфіденційності не лише власних даних, а також і сторонніх інформаційних ресурсів.

Політика інформаційної безпеки – це сукупність правил і принципів, якими керується компанія в цій області, в тому числі і з метою виконання умов сертифікації.

Політика ІБ – це інструкція з використання оборонного щита, який вибудований на підприємстві, саме інструкція, бо щитом є система технічних засобів з інформаційної безпеки і самі користувачі, якщо вони добре поінформовані і правильно виконують свої функції.

Оскільки організація інформаційної безпеки має здійснюватися шляхом комплексного підходу, політика інформаційної безпеки має встановлювати відповідальність вищого керівництва, його цілі і принципи щодо дотримання інформаційної безпеки; є дієвим засобом успішного проходження процедури проведення сертифікації у цій сфері.

Крім того, політика містить загальне визначення інформаційної безпеки як можливості спільного використання інформації, законодавчий і правовий аспект питання, навчання персоналу з питань цієї сфери, протидії появі шкідливого програмного забезпечення, обов’язки персоналу, відповідальність за порушення власне політики безпеки, а також управління безперервністю бізнесу.

Відсутність правильно розробленої та впровадженої Політики інформаційної безпеки частіше за все стає причиною успішності зловмисників у випадках кібератак.

Концепція побудови системи інформаційної безпеки повинна будуватися на принципах, характерних для системи безпеки наукової установи, тобто кожен працівник повинен себе ідентифікувати при вході в систему, по аналогії з записом в журналі відвідувань, присвоювати різні ступені доступу інформації (такі як інформація з обмеженим доступом, чи конфіденційна інформація) аналогічно забороні доступу до певних приміщень, повинна бути заборона вчиняти певні дії, та багато іншого.

При розробці Політики ІБ потрібно балансувати на межі зниження ризиків і зручністю для користувача.

Також потрібно пам’ятати, що Політика ІБ – це лише загальний документ (свого роду Конституція ІБ), загалом же Інформаційна безпека повинна поділятися на рівні:

* Політика Інформаційної безпеки;
* спеціалізовані документи з різних напрямків інформаційної безпеки (Політика конфіденційності, Політика реагування на кіберінциденти);
* вузькопрофільні документи, які регулюють вчинення конкретних дій працівниками в рамках Політики інформаційної безпеки (Процедури, регламенти, Посадові інструкції осіб відповідальних за ІБ).

На сьогодні в Україні немає чітко врегулювання вимог до Інформаційної безпеки в закладах вищої освіти та наукових установах. При цьому є вимоги які ставляться до компаній, які працюють з персональними даними громадян Європейського союзу відповідно до вимог [General data protection regulation](https://legalitgroup.com/gdpr-novi-yevropejski-tendentsiyi/) (GDPR), та деяких інших нормативних актів.

Останні тенденції нормотворення, зокрема, проект Постанови НБУ «Про затвердження Положення про кіберзахист та інформаційну безпеку в платіжних системах та системах розрахунків», окремі норми Закону України «Про основні засади забезпечення кібербезпеки України» та деякі інші, вказують на те, що в близькому майбутньому нас чекає чітке законодавче регулювання з жорсткими вимогами до Політик інформаційної безпеки підприємств.

Для забезпечення достатнього рівня інформаційної безпеки наукової установи потрібно розробляти Політику інформаційної безпеки з урахуванням того, що вона є складовою системи її безпеки, і пам’ятати, що вона повинна бути орієнтованою на кожного працівника, а також не навантажувати головний документ інформацією, направленою на окремих працівників. Для цього потрібно розробляти документи нижчого рівня.

Розробка політики інформаційної безпеки є початковим етапом процедури проведення сертифікації та починається з аналізу ризиків у цій сфері, в тому числі і визначення оптимального рівня ризику. Досягнення такого цього рівня має стати визначальною віхою та метою розробки системи управління інформаційною безпекою.

Наступний етап розробки – аналіз інформаційних ресурсів, визначення їх цінності та побудова моделі  взаємозв’язків між ними. Отримана модель дає можливість обрати оптимальні способи протидії інформаційних ризикам та дотримуватися загальної схеми сертифікації системи управління.

Останній крок – розробка документації у сфері забезпечення інформаційної безпеки.

Результатом цих дій має бути створення документа, що вбирає в себе основні принципи і правила, яких дотримується компанія для забезпечення інформаційної безпеки – власне політики інформаційної безпеки.

Due Diligence – це процес отримання інформації про осіб, організації або компанії, з якими ви можете працювати з приводу:

Переконатися, що інформація є об’єктивною та надійною;

Збір важливих фактів і описової інформації, які є найбільш доречними для прийняття обґрунтованого рішення;

Оцінка того, як найкраще працювати чи співпрацювати з цією особою чи організацією в межах прийнятного ризику;

Є ключові всеохоплюючі сфери, які цікавлять під час проведення належної перевірки, зокрема:

– Управління та контроль

– Безпека

Розуміння дослідницької та інноваційної діяльності мають значну цінність, яка проявляється в різних аспектах, зокрема:

**Фінансовий,** що сприяє економічному зростанню країни через ліцензії, спін-аути та інші форми розвитку.

**Академічний,** що сприяє накопиченню знань у предметній галузі.

**Репутаційний,** підвищення поваги вашої дослідницької групи та установи в усьому світі.

**Стратегічний,** який створює технологічну, медичну або військову перевагу.

Тому захист наукових досліджень є важливим, і спільне дослідження може бути вразливим до зловживання окремими особами, організаціями та установами, чиї цінності відрізняються від наших власних

**Як допомагає Due Diligence?**

– Надає впевненість у тому, що дослідницька група зможе виконати дослідницький проект згідно з домовленістю.

– Надає можливість поділитися знаннями та системами або процесами, які вам можуть знадобитися для використання.

– Відповідати очікуванням спонсора або умовам, які вимагають проведення належної обачності.

– Відповідати очікуванням спонсора або умовам, які вимагають проведення належної обачності.

**Коли здійснюється Due Diligence?**

– на стадії початкових обговорень;

– на стадії застосування;

– на стадії нагородження;

– під час виконання проекту.

**Коли можна провести Due Diligence?**

* Коли працюєш з новими засновниками, партнерами, колабораціями;
* Коли працюєш з новою галуззю організації вперше;
* Якщо з моменту належної обачності минув певний період часу;
* Якщо були суттєві зміни щодо персоналу;
* Якщо були геополітичні зміни у зовнішньому середовищі;

Реалізація політики інформаційної безпеки певного об’єкта починається з проведення розрахунку фінансових втрат і вибору відповідних засобів для виконання цих задач. При цьому необхідно врахувати такі фактори як безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії. Також варто враховувати основні положення з безпеки інформації:

– економічна ефективність – вартість засобів захисту має бути меншою, ніж розміри можливого збитку;

– кожен користувач повинний мати мінімальний набір привілеїв, необхідний при роботі;

– простота системи захисту об’єкта – захист буде тим ефективніший, чим легше користувачу з ним працювати;

– відключення захисту при нормальному функціонуванні – захист не повинен відключатися, за винятком особливих випадків, коли співробітник із спеціальними повноваженнями може мати можливість відключити систему захисту;

– відкритість проектування і функціонування механізму захисту (для можливості адекватного реагування обслуговуючого персоналу на виникнення збоїв у системі);

– незалежність системи захисту від суб’єктів захисту – розроблювачами не повинні бути ті, кого вона буде контролювати;

– загальний контроль без будь-яких виключень з безлічі контрольованих суб’єктів;

– звітність і підконтрольність системи захисту;

– відповідальність осіб, що займаються інформаційною безпекою;

– об’єкти захисту доцільно розділити на групи так, щоб порушення захисту в одній групі не впливало на безпеку інших груп;

– відмова від замовчування – при збої засобів захисту доступ до обчислювальних ресурсів повинен бути заборонений;

– система захисту об’єкту має бути цілком специфікована, протестована та погоджена;

– система повинна допускати зміну своїх параметрів адміністратором;

– важливі критичні рішення повинні прийматися людиною, а не комп’ютером;

– система захисту об’єкта повинна проектуватися в розрахунку на вороже оточення і припускати, що користувачі мають найгірші наміри, будуть робити помилки і шукати шляхи обходу механізмів захисту;

– інформація про існування механізмів захисту повинна бути, по можливості, схована від користувачів, робота яких контролюється.

Кожен об’єкт повинен заздалегідь визначити набір адміністративних санкцій, застосованих до місцевих користувачів, які порушують політику інформаційної безпеки сторонньої організації чи об’єкта. Крім того, необхідно подбати про захист від відповідних дій сторонньої організації. При розробці політики інформаційної безпеки варто враховувати всі юридичні положення, які застосовуються до подібних ситуацій.

Політика безпеки об’єкта повинна мати процедури для взаємодії з зовнішніми організаціями, в число яких входять правоохоронні органи, інші організації, команди "швидкого реагування", засоби масової інформації. У процедурах повинно бути визначено, хто має право на такі контакти, і як саме вони відбуваються.

**Використані джерела:**

Використання Due Diligence в обґрунтуванні передінвестиційних рішень у секторах національної економіки: колективна монографія / Балджи М.Д., Доброва Н.В., Карпов В.А. [та ін.]; Одеський національний економічний університет. – Одеса: ПромАрт, 2018. – 335 с.

<https://biz.ligazakon.net/analitycs/220139_mnmzatsya-rizikv-dlya-nvestora-dlya-chogo-potrben-due-diligence>

<https://legalitgroup.com/informaciyna-bezpeka-v-kompanii/>

<https://atestor.ua/uk/poleznye-stati/politika-informaciinoyi-bezpeki/>