ILG Investment Lawyer Group

ПРОДУКТ

АРХІТЕКТУРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Проведення аудиту, проектування систем, нормативний супровід організацій

+34%

Зросла кількість успішних атак з використанням технічний вразливостей систем у 2025

Джерело: Verizon DBIR 2025

$4.4M

Середня вартість одного кіберінциденту у 2025

Джерело: IBM Cost of a Data Breach 2024

72%

Компаній в світі зазначили значний ріст загроз від кіберінцидентів у 2025 році

Джерело: World Economic Forum — Global Cybersecurity Outlook 2025

ILG Investment Lawyer Group

Реальна практика: хроніка глобальних кіберінцидентів

2021 **Colonial Pipeline**

Кібератака паралізувала постачання пального на Східному узбережжі США. Угрупування DarkSide застосувало шифрувальник, що спричинило масштабний дефіцит пального.

Збитки: $4.4M за один день + $40M операційна шкода

2023 **MGM Resorts**

Методом примітивної соціальної інженерії (vishing) була повністю знищена інформаційна інфраструктура гіганта комерційної нерухомості. Атакуючі отримали повний контроль над системами.

Збитки: $100M за один день + операційна шкода. Угрупування: Scattered Spider

2024 **Change Healthcare**

Атака шифрувальника на найбільший медичний сервіс США. Колапс системи тривав 3 тижні. Паралізовано виплати страхових компенсацій та обробку рецептів по всій країні.

Збитки: $22M за один день + $872M операційні витрати. $2 млрд — сума для повного відновлення

Реальна практика: інциденти 2025 року, включаючи Україну

2025 **Jaguar Land Rover**

Атака деструктивним шифрувальником на промислового гіганта призвела до повної зупинки виробництва на 5 тижнів. Стався злив виробничих та службових таємниць. Операційні збитки: $2.4 млрд + злиття виробничих та службових таємниць. Угрупування: Scattered Lapsus$ Hunters

2025 **Приватна фінансова установа (Україна)**

Відсутність сегментації мережі та застаріла автентифікація дозволили зловмисникам компрометувати внутрішню інфраструктуру методом Credential Stuffing. Прямі збитки перевищили $2M, відновлення — понад 3 тижні. НБУ ініціював перевірку відповідності Постанові №143.

2025 **Обленерго**

Кібероперація призвела до каскадного відключення підстанцій, фізичного знищення контролерів та примусового переходу на ручне керування об'єктом. Був реальний ризик повного знищення системи автоматизації та спроба знищення електросистеми регіону. 12 годин тривав параліч системи автоматизації. Операція підрозділу № 74455 ГРУ РФ «Sandworm»

2025 **AgroProsperis**

Компрометація системи холдингу, попри формально вчасну реакцію на інцидент. Угрупування FIN7 здійснило цілеспрямовану атаку на агропромисловий сектор. Загальний збиток: $1M. Угрупування: FIN7

Це підтверджується практикою: коли приватні фінансові установи та об'єкти КІІ зазнають мільйонних збитків — держава реагує посиленням регуляторного тиску. Відповідність вимогам — вже не вибір, а зобов'язання.

ILG Investment Lawyer Group

Критичні проблеми систем інформаційної безпеки

01 ⚠ **Окремі сегментовані рішення**

В кращому випадку реальна безпека інформації більшості організацій утримується антивірусними програмами, мережевими системами та фізичним контролем доступу. Статистика твердо констатує: стала архітектура безпеки знищена — не здатна протидіяти реальним загрозам.

02 ⚙ **Відсутність системи управління**

Відсутність контролю, документованості, структурності. Як наслідок — хаотичність процесів та операційна залежність від окремих людей та рішень.

03 👤🛡 **Кадрова залежність**

Відсутність контролю над системою, відсутність можливості зміни ключових спеціалістів. Фактично система «живе» поки присутній спеціаліст, що операційно керує нею на свій розсуд.

Регуляторний тиск зростає паралельно із загрозами.

Ми також спостерігаємо глибші процеси:
— зростаючу поляризацію світових сил
— послаблення інституцій міжнародного права
— стрімкий розвиток технологій штучного інтелекту
Держава реагує на зростання кіберзагроз посиленням вимог до захисту інформації:
— Постанова НБУ №143 — обов'язкові вимоги до ІБ для всіх фінансових установ
— Постанова КМУ №712 + Закон про захист інформації в ІКС — для об'єктів КІІ
— Обов'язкова авторизація у Держспецзв'язку для об'єктів критичної інфраструктури

Невідповідність несе не лише технічні ризики — санкції регулятора, зупинка ліцензії, публічні перевірки. Організація без задокументованої системи безпеки вразлива вдвічі: і до атак, і до регулятора.

ILG Investment Lawyer Group

Критична інфраструктура

Аудит, розробка та супровід профілю кібербезпеки інформаційних систем

Критична інфраструктура: профіль кібербезпеки та авторизація у Держспецзв'язку

Аудит, розробка та супровід профілю кібербезпеки

Формуємо галузевий профіль кібербезпеки та повністю супроводжуємо авторизацію інформаційної системи у Держспецзв'язку — від підготовки пакету документів до отримання офіційного статусу. Щорічна реавторизація перестає бути проблемою.

Проведемо аналіз контексту та меж діяльності — точно визначимо вимоги держави та регулятора. Сформуємо галузевий профіль кібербезпеки відповідно до вимог авторизації.

Приводимо систему безпеки до відповідності Постанові КМУ №712 та Закону «Про захист інформації в ІКС». Аудит IT/OT-інфраструктури: реальний стан захисту, критичні вузли, поверхня атаки — все у зрозумілому стратегічному документі.

Проектуємо та впроваджуємо СУІБ і ВНД під специфіку Вашої галузі. Адаптуємо рішення до реального контексту та наявної інфраструктури — баланс між відповідністю вимогам регулятора, операційною безперервністю та захистом критичних активів.

Наші фахівці в співпраці з Вами спроектують та впровадять прозору систему управління інформаційною безпекою, розробимо та інтегруємо внутрішню нормативну документацію відповідно до потреб Вашої діяльності.

Ми адаптуємо рішення під Вас, Ваш контекст, вимоги та ризики, наявну IT систему та масштаб діяльності організації. Представимо оптимальну стратегію балансу системи безпеки між відповідністю державним вимогам, функціональною безпекою та продуктивністю бізнес-процесів.

Критична інфраструктура: користь для Вашої компанії (1/2)

Продукт «Архітектура інформаційної безпеки»

Захист від зупинки та фінансових втрат:

- **зупинка підстанції, водозабору або транспортного вузла через кібератаку коштує в десятки разів більше за вартість захисту — архітектура ІБ є вашим страховим полісом;**
- задокументована СУІБ є пом’якшуючою обставиною для НБУ при перевірці — мінімізує штрафи, обмеження ліцензії та зупинку діяльності навіть у разі інциденту;
- **система фіксує всі дії в OT/IT-середовищі — при атаці РФ-угруповань маєте доказову базу для розслідування, відшкодування збитків і захисту в суді.**

Контроль, прозорість та масштабування:

- **керівник бачить реальний стан захисту без залежності від слів IT-відділу — чіткі KPI, відповідальні особи, зрозумілі звіти без технічного жаргону;**
- **кожен новий об'єкт, вузол або сегмент підключається за типовою задокументованою архітектурою — розширення мережі без хаосу та «латання дір»;**
- **єдина архітектура безпеки розгортається на всіх об'єктах мережі — жодного різнобою між підрозділами, жодних прихованих точок входу для атак.**

Критична інфраструктура: користь для Вашої компанії (2/2)

Продукт «Архітектура інформаційної безпеки»

Кадровий суверенітет та безперервність:

- **новий ІБ-спеціаліст входить у роботу за тиждень, а не за місяці — вся архітектура, процеси та відповідальності задокументовані без «чорних ящиків»;**
- **заміна ключового IT/OT-спеціаліста не зупиняє роботу об'єкта — знання зафіксовані в документах, а не тримаються в голові однієї людини;**
- **регламентована діяльність об'єкта триває навіть при відсутності IT-спеціаліста — чіткі інструкції для персоналу на кожен сценарій, включаючи позаштатний.**

Авторизація та захист критичних активів:

- **авторизація у Держспецзв'язку «під ключ» — від аудиту до офіційного статусу без бюрократичних затримок; щорічна реавторизація стає плановою процедурою, не авральним завданням;**
- підтверджений рівень ІБ є обов’язковою умовою при due diligence для міжнародних партнерств, кредитних ліній та залучення іноземних інвестицій — банки і інвестори вже питають про СУІБ на першій зустрічі.

ILG Investment Lawyer Group

Опис продукту

Що входить до «Архітектури інформаційної безпеки»

Що входить до «Архітектури інформаційної безпеки» (1/2)

1 Комплексний аудит інформаційної системи

- Комплексний аудит інформаційної системи передбачає всебічне дослідження організації як інтегрованого середовища функціонування інформаційних, технологічних та операційних процесів. Об'єктом аналізу виступає не лише IT-інфраструктура, але й пов'язане з нею фізичне середовище, мережеві сегменти, віддалені точки доступу, хмарні сервіси та взаємодія з зовнішніми системами.
- У межах аудиту здійснюється ідентифікація активів, визначення поверхні атаки, оцінка архітектури мереж, рівня сегментації, захищеності каналів зв'язку та наявності контролів безпеки. Окремо аналізуються фактори, що впливають на тійкість системи, включаючи залежності від провайдерів, географічну розподіленість інфраструктури та рівень захисту критичних вузлів.

2 Аналіз нормативно-правового контексту діяльності організації

- У межах аналізу здійснюється оцінка відповідності діяльності організації вимогам національного законодавства та міжнародних стандартів у сфері інформаційної та кібербезпеки. Перевіряється узгодженість внутрішніх документів із вимогами Закону України «Про захист інформації в інформаційно-комунікаційних системах», а також відповідність принципам ISO/IEC 27001, NIS2 Directive та NIST Cybersecurity Framework.
- Оцінюється повнота нормативної бази, коректність формалізації процесів, наявність політик, регламентів і процедур, а також їх фактичне застосування в операційній діяльності.

Що входить до «Архітектури інформаційної безпеки» (2/2)

3 Розробка та впровадження СУІБ та внутрішньої нормативної документації

- На основі результатів аудиту формується та впроваджується система управління інформаційною безпекою як інтегрована управлінська модель, що охоплює всі рівні організації. Визначаються інформаційні активи, їх критичність, ролі та відповідальність користувачів, встановлюється модель управління доступом, включаючи принципи мінімальних привілеїв та розмежування прав.
- Розробляється ієрархія нормативної документації, що включає політики, регламенти та процедури, які регулюють процеси управління ризиками, доступом, інцидентами, змінами та безперервністю діяльності. Особлива увага приділяється інтеграції технічних, організаційних та поведінкових контролів у єдину керовану систему.

4 Профіль кібербезпеки, регуляторна відповідність та авторизація

- Формується цільовий профіль кібербезпеки організації, який відображає поточний і бажаний рівень захищеності, а також ступінь відповідності регуляторним вимогам. Проводиться оцінка ризиків, визначаються критичні вразливості та фактори, що можуть впливати на стабільність функціонування системи або призводити до інцидентів безпеки.
- Окремо аналізуються механізми автентифікації та авторизації, управління ідентифікацією, контроль доступу до ресурсів та журналювання дій користувачів. Результати цього етапу дозволяють виявити обмеження та ризики, що можуть впливати на прийняття управлінських рішень, впровадження системи безпеки або запуск критичних бізнес-процесів.

ILG Investment Lawyer Group

Пакети послуг

Вартість та умови надання

ILG Investment Lawyer Group

Пакети послуг

ПАКЕТ 1

Аудит + ВНД

- Відповідність вимогам регулятора до СУІБ та ВНД
- Розробка галузевого профілю кібербезпеки (КМУ №712)
- Загальна архітектура кібербезпеки (IT / OT / IoT)
- Ефективність засобів захисту (EDR, SIEM, IDS/IPS)
- Управління доступами та привілеями (IAM, PAM)
- Мережевий периметр і сегментація
- Рівень логування та моніторингу подій безпеки
- Вразливості інфраструктури та вектори атак
- Готовність до інцидентів (IR-процеси, playbooks)

Строк проведення : 3 тижні

★ РЕКОМЕНДОВАНО

ПАКЕТ 2

Аудит + СУІБ + Профіль кібербезпеки

- Усі параметри базового аудиту
- Відповідність СУІБ та ВНД (ISO 27001, NIST, нац. вимоги)
- Аналіз та вибір стратегії відповідності держвимогам
- Процеси управління ризиками та їх імплементація
- Governance-модель: ролі, відповідальність, контроль
- Розробка та інтеграція СУІБ та ВНД
- Розробка профілю кібербезпеки за вимогами регулятора
- Супровід авторизації систем та галузевих експертиз

Строк проведення : за результатами аудиту

ILG Investment Lawyer Group

З ПОВАГОЮ

АО «ІНВЕСТМЕНТ ЛОЙЄР ГРУП»

Архітектура інформаційної безпеки

Аудит · Проектування систем · Нормативний супровід

+38 063 204 26 25
+38 063 641 50 30

info@investlaw-group.com

investlaw-group.com

Київ, Берестейський провулок, 5а