АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ПРАВОВІЙ, ОРГАНІЗАЦІЙНІЙ ТА ТЕХНОЛОГІЧНІЙ СФЕРІ

А. С. Азєєв, М. П. Чайковська
м. Одеса, Одеський національний університет
імені І. І. Мечникова

Однією з найбільш критичних проблем менеджменту сучасного інформаційного підприємства є забезпечення та управління інформаційною безпекою (ІБ). Побудова ефективної системи ІБ залежить від постійного моніторингу інформаційного середовища та своєчасного реагування, адаптації та оновлення систем захисту. Менеджмент організації найчастіше очікує від ІБ негайних вигід, однак безпека – це процес, а не результат. Побудова ефективної системи ІБ – це складний і безперервний процес, від уваги до якого залежить життєздатність та саме існування бізнесу.

Взаємовідносини між компаніями, державними органами та зловмисниками по лінії ІБ в 2018 р. знаходять нові форми й поглиблюються. Так 25 травня набуває чинності постанова GDPR [1], що встановлює вимоги до компаній з питань захисту даних громадян ЄС, обробці й зберіганню цієї інформації. Постанова стосується будь-яких організацій, у тому числі українських, які обробляють або збирають особисті дані громадян ЄС, незалежно від того, чи перебувають ці компанії в ЄС або за його межами. Це підвищує рівень складності керуванням інформаційними ресурсами компанії. З'явиться необхідність вирішувати перелік технологічних і фінансових проблем: відсутність поінформованості, збільшення видатків на управління даними, нестача кваліфікованих фахівців, відволікання уваги й інвестицій від інших важливих ініціатив.

Наступний важливий аспект ІБ пов'язаний з поведінкою регулюючих органів. Організації, які не ставляться серйозно до GDPR і в яких відбуваються інциденти, що провокують розслідування, одержать реальну небезпеку серйозного штрафу – 4% річного обороту або €20 млн. [1].

Незважаючи на актуальну природу загроз мережевої безпеки, менш відома, але не менш важлива, директива по безпеці мережевих і інформаційних систем (NIS) не одержала такої широкої популярності як GDPR. Директива повинна стати частиною національних законодавств у травні 2018 і вводить такі ж тверді санкції відносно компаній за її недотримання [2]. NIS зосереджена на створенні загального рівня кібербезпеки в ЄС. Впроваджується національний нагляд за безпекою в критичних секторах економіки, таких як енергетика, транспорт, водопостачання, охорона здоров'я, фінанси тощо, а також за постачальниками цифрових послуг (точки обміну інтернет-трафіком, системи доменних імен).

Мільйони підключених пристроїв практично не захищені від хакерів. Насправді, зловмисникам з кожним роком стає навіть легше одержувати доступ до безлічі Інтернет-пристроїв. Усе, що їм потрібно зробити, це купити комплект ботнета (Andromeda, Gamarue, Wauchos). Проблема в тому, що детально невідомі наміри роботи хакера, які контролюють боти-мережі. Можуть бути запущені атаки типу «відмова в обслуговуванні» (Ddos) або відправлена величезна кількість спама, можливо виникнуть нові, несподівані способи злочинної поведінки.

Виробники найчастіше абияк ставляться до проблем безпеки – в IT-сфері висока конкуренція, а дійсно якісний захист пристроїв вимагає більших витрат. Крім того, дуже складно виправляти виявлені вразливості – оновлення на більшість пристроїв просто технічно неможливо встановити.

Деякі з найбільших кібер-інцидентів 2017 року пов'язані з проблемами програм-шкідників, що самовідтворюються. Наприклад, Wannacry або Notpetya [3]. Можна чекати, що подібне шкідливе ПЗ продовжить свою роботу в 2018 році.

Однією з найтривожніших новин 2017-го було виявлення фундаментального недоліку поширеного протоколу безпеки Wi-Fi WPA2, який навряд буде усунутий на більшості пристроїв з підтримкою Wi-Fi у наступному році.

Критичні вразливості, нещодавно знайдені в процесорах – Meltdown і Spectre. Враховуючи широку поширеність таких

процесорів, величезна кількість користувачів опиняється під загрозою.

Помітною жертвою спалаху шкідливого ПЗ Wannacry на початку 2017 стала Національна служба охорони здоров'я Великобританії (NHS) [4]. Розвиток телемедицини та різнобічність збережених персональних даних і далі будуть приваблювати зловмисників. А впровадження IoT у якості медичних пристроїв, підключених до мережі, підсилює ризик подальших атак. Поки ця сфера не настільки актуальна для України, однак розвиток телемедицини посилюється.

Злочин-як-послуга (Caas) розширює інструменти й послуги. Злочинні організації продовжують свій постійний розвиток і стають усе більш витонченими. Комплексні ієрархії, партнерські відносини й співробітництво будуть сприяти їхньому виходу на нові ринки й комерціалізації діяльності на глобальному рівні. Деякі організації будуть мати коріння в існуючих кримінальних структурах, а інші будуть зосереджені винятково на кіберзлочинності. У результаті кібератаки стануть більшою мірою безперервними та руйнівними, ніж раніше [5, с. 74].

Програми, від самого початку розроблені з урахуванням загроз, почнуть поліпшувати безпеку автоматизованих систем управління (АСУ). Нагадаємо, що АСУ застосовується для керування різними процесами в рамках технологічного процесу в різних галузях промисловості, енергетиці, транспорті й т. п., тобто в галузях, критичних для людської життєдіяльності.

Недоліки в забезпеченні безпеки приводять до інцидентів, подібних атаці на українську енергосистему в 2015. Через рік відбулася друга й менш відома атака з використанням повністю автоматизованого шкідливого ПЗ, здатного нанести більш масштабний збиток за менший час. Подібні речі призводять до підвищеного усвідомлення проблем безпеки. Все більше розробників АСУ створюють ПЗ що враховує шкідливі способи впливу.

У 2018 році усе більше організацій усвідомлюють, що атаки не уникнути, вона відбудеться не «якщо», а «коли». Відповідно компанії почнуть приділяти більше уваги

результатам, а не заспокоюватися, перевіривши наявність усіх необхідних, як їм здається, інструментів.

За прогнозами Frost & Sullivan, нестача кваліфікованих фахівців в галузі безпеки може сягнути 1,5 мільйонів до 2020 року [5]. Це приводить до збільшення інвестування в альтернативні способи забезпечення безпеки. Очікуються інноваційні продукти, що здійснюють моніторинг і тестування ІБ систем на основі штучного інтелекту.

Аналізуючи методи, використані зловмисниками, важливо відслідковувати зміни, що відбуваються в їхній тактиці.

Необхідність змінити відношення до ІБ як додаткової опціональної послуги, яка не є обов'язковою умовою успішного бізнесу. Очікування топ-менеджерів перевершують реальні можливості системи. І невідповідність між ними виявляться при виникненні великого інциденту. Мало того, що організація зіштовхнеться з істотною проблемою, її наслідки також відіб'ються на особистій і колективній репутації всіх зацікавлених осіб компанії.

Інформаційне середовище росте та структурується й те, на що можна було раніше не звертати увагу, зараз не можливо ігнорувати. В цьому причина введення нових правових актів і появи нових регуляторів як державних, так і приватних. У цьому ж і причина ускладнення злочинного світу як за способами атак, так і за учасниками співтовариств. Безпека стає частиною структури організації та її продуктів. І на ринку залишаться лише ті компанії, які це усвідомили.

Список використаних джерел:

1. The General Data Protection Regulation (GDPR) (EU) 2016/679 [Електронний ресурс] – Режим доступу: eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
2. The Directive on security of network and information systems (NIS Directive) [Електронний ресурс] – Режим доступу: eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
3. Cisco 2017 Midyear Cybersecurity Report. – Cisco, 2017. – 90 p.
4. Internet Security Threat Report // Symantec – 2017. – 77 p.
5 Азєєв А. С., Чайковська М.П. Сучасні напрямки типологізації

інформаційних загроз та тренди ринку інформаційної безпеки// «Економіка та суспільство» # 13/2017. Електронне фахове видання. Мукачівський державний університет.- http://www.economyandsociety.in.ua/index.php/
6. 2017 Global Network Threat Protection Solutions Technology Leadership Award. – Frost & Sullivan, 2018. – 11 p.