ABOUT THE AUTHOR
Studinska Galina - Doctor of Economic Sciences
Senior researcher at the State Research Institute of Informatization and Economic Modeling of the Ministry of Economic Development and Trade
Ave. Druzhby narodiv, 38, Kyiv, Ukraine
e-mail: Studinska.galina@gmail.com

УДК 330:004 https://doi.org/10.31470/2306-546X-2021-48-76-91

КОНФІДЕНЦІЙНІСТЬ ТА ШАХРАЙСТВО В ІНТЕРНЕТ-СФЕРІ

Шульга О. А.

Мета роботи *– розглянути теоретичні та практичні аспекти шахрайства в інтернет-сфері та на підставі цього визначити шляхи забезпечення конфіденційності та кібербезпеки приватних користувачів і комерційних організацій.*

Методологічною основою роботи є застосування загальнонаукових та спеціальних методів наукового пізнання. Методи поєднання аналізу та синтезу, індукції та дедукції були застосовані при визначенні різних видів шахрайства в інтернет-сфері. Методи узагальнення, логічний та емпіричний були використані при визначенні напрямів розвитку національної системи кіберзахисту та забезпечення конфіденційності.

Основні результати роботи: *Виділено найпоширеніші способи шахрайства із використання банківських платіжних карт, серед яких: вдаване опитування у соцмережах з розіграшем призів; телефонний дзвінок з метою отримати секретні дані; заміна SIM-карти для доступу до онлайн-банкінгу; платежі онлайн на незахищених сайтах; фішинг; копіювання даних карти при передачі у руки; незахищені мережі WI-Fi; комп'ютери у громадських місцях; скіммінг для крадіжки даних карти; несанкціоноване проведення мікроплатежів; шахрайство з використанням банкомату; використання шкідливих програм (вірусів), підроблених сайтів з метою компрометації реквізитів електронних платіжних засобів та/або логінів/паролів доступу до систем інтернет/мобільного банкінгу; розповсюдження (продаж, розповсюдження) інформації щодо скомпрометованих даних; шахрайство у термінальній мережі; шахрайство у системах дистанційного обслуговування; соціальна інженерія. Визначено основні правила безпеки з метою запобігання шахрайства. Проаналізовано досвід європейських країн у сфері кібербезпеки. Окреслено напрями адаптації чинного законодавства про кібербезпеку до стандартів ЄС та визначено напрями розвитку національної системи кіберзахисту.*

Практичне значення отриманих результатів полягає у поглибленні розуміння сутності та механізму реалізації різних видів шахрайства в інтернет-сфері. Запропоновані у роботі рекомендації можуть скласти методологічну та теоретичну основу для розробки економічної політики держави щодо забезпечення конфіденційності та кібербезпеки приватних користувачів і комерційних організацій.

Висновки. *Держава має створити ефективний наглядовий орган у сфері захисту персональних даних, однак при цьому заходи безпеки та онлайн-обмеження повинні відповідати міжнародним стандартам. На законодавчому рівні не повинно заборонятися використання шифрування, оскільки такі обмеження знижують можливості громадян із захисту себе від незаконних втручань у приватність. Крім того, політика держави у інтернет-сфері має бути спрямована на сприяння розвитку та функціонуванню безпечних інтернет-технологій і формування механізмів захисту від сервісів та протоколів, які ставлять під загрозу технічне функціонування інтернету від вірусів, фішингу тощо.*

Ключові слова: *інтернет, інформаційні технології, шахрайство, кібербезпека, державно-приватне партнерство, цифрова економіка.*

КОНФИДЕНЦИАЛЬНОСТЬ И МОШЕННИЧЕСТВО В ИНТЕРНЕТ-СФЕРЕ

Шульга О. А.

Цель работы – рассмотреть теоретические и практические аспекты мошенничества в интернет-сфере и на основании этого определить пути обеспечения конфиденциальности и кибербезопасности частных пользователей и коммерческих организаций.

Методологической основой работы является применение общенаучных и специальных методов научного познания. Методы сочетание анализа и синтеза, индукции и дедукции были применены при определении различных видов мошенничества в интернет-сфере. Методы обобщения, логический и эмпирический были использованы при определении направлений развития национальной системы киберзащиты и обеспечения конфиденциальности.

Основные результаты работы: Выделены наиболее распространенные способы мошенничества по использованию банковских платежных карт, среди которых: притворный опрос в соцсетях с

розыгрышем призов; телефонный звонок с целью получить секретные данные; замена SIM-карты для доступа к онлайн-банкингу; платежи онлайн на незащищенных сайтах; фишинг; копирования данных карты при передаче в руки; незащищенные сети WI-Fi; компьютеры в общественных местах; скимминг для кражи данных карты; несанкционированное проведение микроплатежей; мошенничество с использованием банкомата; использование вредоносных программ (вирусов), поддельных сайтов с целью компрометации реквизитов электронных платежных средств и/или логинов/ паролей доступа к системам интернет/мобильного банкинга; распространение (продажа, распространение) информации о скомпрометированных данных; мошенничество в терминальной сети; мошенничество в системах дистанционного обслуживания; социальная инженерия. Определены основные правила безопасности с целью предотвращения мошенничества. Проанализирован опыт европейских стран в сфере кибербезопасности. Определены направления адаптации действующего законодательства о кибербезопасности со стандартами ЕС и направления развития национальной системы киберзащиты.

Практическое значение полученных результатов заключается в углублении понимания сущности и механизма реализации различных видов мошенничества в интернет-сфере. Предложенные в работе рекомендации могут составить методологическую и теоретическую основу для разработки экономической политики государства по обеспечению конфиденциальности и кибербезопасности частных пользователей и коммерческих организаций.

Выводы. Государство должно создать эффективный надзорный орган в сфере защиты персональных данных, однако при этом меры безопасности и онлайн-ограничения должны соответствовать международным стандартам. На законодательном уровне не должно запрещаться использование шифрования, поскольку такие ограничения снижают возможности граждан по защите себя от незаконных вмешательств в приватность. Кроме того, политика государства в интернет-сфере должна быть направлена на содействие развитию и функционированию безопасных интернет-технологий и формирования механизмов защиты от сервисов и протоколов, которые ставят под угрозу техническое функционирование интернета от вирусов, фишинга и тому подобное.

Ключевые слова: *интернет, информационные технологии, мошенничество, кибербезопасность, государственно-частное партнерство, цифровая экономика.*

CONFIDENTIALITY AND SCAM IN THE INTERNET

Shulga Olga

The purpose of the work is to consider the theoretical and practical aspects of fraud in the Internet sphere and on this basis to identify ways to ensure the confidentiality and cybersecurity of private users and commercial organizations.

The methodological basis of the work is the use of general and special methods of scientific knowledge. Methods of combining analysis and synthesis, induction and deduction have been used to identify different types of fraud in the Internet. Generalization methods, logical and empirical, were used in determining the directions of development of the national cyber defense system and ensuring confidentiality.

The main results of the work: The most common methods of fraud with the use of bank payment cards are identified, among which: a fake poll on social networks with a prize draw; a phone call to obtain classified information; SIM card replacement for access to online banking; online payments on unsecured sites; phishing; copying card data when handed over; unsecured WI-Fi networks; computers in public places; skimming for card data theft; unauthorized micropayments; ATM fraud; use of malicious programs (viruses), fake sites in order to compromise the details of electronic payment instruments and/or logins/passwords for access to Internet/mobile banking systems; dissemination (sale, dissemination) of information on compromised data; terminal network fraud; fraud in remote service systems; social engineering. Basic security rules are defined to prevent fraud. The experience of European countries in the field of cybersecurity is analyzed. The directions of adaptation of the current legislation on cybersecurity to the EU standards are outlined and the directions of development of the national system of cybersecurity are defined.

The practical significance of the results is to deepen the understanding of the nature and mechanism of various types of fraud in the Internet. The recommendations proposed in the paper can form a methodological and theoretical basis for the development of economic policy of the state to ensure the confidentiality and cybersecurity of private users and commercial organizations.

Conclusions. *The state should establish an effective oversight body in the field of personal data protection, but security measures and online restrictions should comply with international standards. The use of encryption should not be prohibited at the legislative level, as such restrictions reduce the ability of citizens to protect themselves from illegal intrusions into privacy. In addition, the state policy in the Internet should be aimed at promoting the development and operation of secure Internet technologies and the formation of mechanisms to protect against services and protocols that threaten the technical functioning of the Internet from viruses, phishing and more.*

Key words: *Internet, information technologies, fraud, cybersecurity, public-private partnership, digital economy.*

JEL Classification: C100, E440

Вступ. В умовах формування інформаційного суспільства важливу роль у розвитку країн відіграє цифрова економіка, яка виступає продуктивним підґрунтям розвитку суспільства на платформі інформаційно-

комунікативних технологій. Наразі інформаційні технології застосовуються у процесі вирішення завдань забезпечення національної, військової та економічної безпеки. Відповідно до цього кожна держава намагається вживати всіх можливих заходів для забезпечення максимального доступу своїх громадян до інтернету, зокрема, проводити політику, щоб інтернет був доступним, відкритим та надавався за помірну плату для всіх груп населення. Однак ключовими умовами для цього є доступ громадян до інформації про технології та їх цифрова грамотність.

Водночас одним з фундаментальних наслідків глобальної інформатизації стало виникнення кіберпростору. Використання Інтернету та інформаційних технологій не тільки відкриває перед людством безмежні можливості, а й створює нові серйозні загрози. Все більше інформації переміщується в онлайн, на серверах збираються мільярди гігабайт різної інформації. За таких умов виникає необхідність формування «правил гри» у такій економіці.

Дослідженням особливостей цифрової економіки та її впливу на розвиток суспільства присвячені праці В. Апалькової, С. Коляденко, Г. Карчевої, Н. Краус, А. Маслова, К. Семячкова та ін. Проблеми кібербезпеки та результати запровадження європейського досвіду у систему захисту національної безпеки України знайшли своє відображення у працях таких вчених, як: О. Баєв, Г. Бєляков, Дж. Блумбекер, О. Манжай, В. Марков, О. Орлов, В. Черней та ін. Не зважаючи на наявність великої кількості публікацій з проблем розвитку цифрової економіки, не вирішеними залишаються ряд питань, які, через їх складність, вимагають подальшого поглибленого вивчення. Зокрема, залишається недостатньо дослідженою проблема впливу цифрової економіки на розвиток фінансового ринку та пошук ефективних методів запобігання ризиків, які пов'язані з бурхливим запровадженням цифрових фінансових технологій.

Мета статті – розглянути теоретичні та практичні аспекти шахрайства в інтернет-сфері та на підставі цього визначити шляхи забезпечення конфіденційності та кібербезпеки приватних користувачів і комерційних організацій. Методологічною основою роботи є застосування загальнонаукових та спеціальних методів наукового пізнання. Методи поєднання аналізу та синтезу, індукції та дедукції були застосовані при визначенні різних видів шахрайства в інтернет-сфері. Методи узагальнення, логічний та емпіричний були використані при визначенні напрямів розвитку національної системи кіберзахисту та забезпечення конфіденційності.

Виклад матеріалу. Право на доступ до інтернету базується на таких принципах [5]:

1) інклюзивність і недискримінація. Доступ має надаватися за розумну ціну і бути недискримінаційним. Взаємодія в інтернеті має бути вільною від дискримінації за такими ознаками, як стать, раса, національність, мова, віросповідання, стан здоров'я, політичні переконання, соціальне походження, майновий стан, вік або сексуальна орієнтація. Держава має сприяти просуванню культурної та мовної різноманітності онлайн, а також створювати технічні умови доступу до інтернету для вразливих груп.

2) мережева нейтральність. Користувачі повинні мати можливість вільно обирати систему, застосунки, програмне забезпечення. Архітектура інтернету, комунікаційні системи і формати мають ґрунтуватися на відкритих стандартах, які забезпечують інтероперабельність, інклюзивність і рівні можливості – вільний обмін інформацією.

3) безпека. Держава повинна гарантувати безпечність інтернету. Водночас технічні стандарти, пов'язані з його інфраструктурою, не мають застосовуватися для цензури чи незаконного нагляду. Технічні характеристики, які створюють можливості для віддаленого доступу силовиків до обладнання (як це, наприклад, пропонується в Україні), суперечать демократичним цінностям.

4) якість сервісу. Гарантований доступ до інтернету має відповідати рівню розвитку та поширенню технологій.

У той же час, кожен має право вільно висловлювати свої погляди, шукати, отримувати та поширювати інформацію онлайн. Реалізація права на свободу вираження поглядів традиційно охоплює декілька принципів, а саме:

1. Ніхто не має бути змушений діяти чи висловлюватися всупереч своїм переконанням.
2. Право шукати й отримувати інформацію означає не лише те, що держава не повинна чинити перешкод тоді, коли особа сама шукає інформацію онлайн, але й в окремих випадках має сприяти доступу до такої інформації, наприклад відповідати на інформаційні запити громадян.
3. Право поширювати інформацію та ідеї. Це право містить у собі не лише поширення нейтральної інформації, але й висловлювань, які можуть ображати, шокувати чи непокоїти. Але лише за умови, що вони не порушують інших прав і свобод, а також не є незаконними.

Поряд з цим, можливість отримувати та поширювати інформацію часто пов'язана з ризиками, а тому має охоплювати також право на анонімність або використання псевдоніму. Інтернет створив безпрецедентні можливості для обміну інформацією. Водночас такий доступ до знань неминуче пов'язаний із серйозними ризиками і загрозами, такими як, наприклад, погрози насильством та мова ворожнечі, а також координовані кампанії з поширення дезінформації, використання тролів і ботів. Усе це загалом ускладнює доступ до справді цінної інформації та підриває довіру до ЗМІ. Інша сторона питання – спроби держав протидіяти цим загрозам шляхом блокування та фільтрування онлайн-контенту.

Разом з тим, до епохи інтернет-комунікацій закритість приватного життя для сторонніх завжди були однією з важливих цінностей суспільства і культури. Однак технологічний розвиток вніс корективи і тепер на зміну уявленням про повну недоторканність приватного життя, приходить нове уявлення про можливості для

громадян контролювати обробку їх персональних даних і приймати рішення щодо цього, яке лягло в основу сучасного законодавства щодо захисту персональних даних.

Боротьба за право видалення даних про себе з пошукових систем, стала однією з перших спроб відстояти приватність особистої інформації. Вирішальною віхою тут став виграш судового процесу проти Google в Європейському суді у 2014 році за позовом, поданим іспанським комерсантом Маріо Костех Гонсалесом, якому вдалося домогтися видалення посилання з Google. Позитивне рішення Європейського суду по цій справі спричинило хвилю подібних виступів, спрямованих проти діяльності Google і в інших європейських країнах. Постанова Європейського суду стала важливим етапом у розвитку законодавства про захист персональних даних, позначивши наростаючий конфлікт між правом кожного на вільний доступ до інформації та правом на недоторканність приватного життя, в тому числі і у формі видалення з «пошукачів» посилань на ресурси з небажаною для людини інформацією.

Однак, як виявилося, на ділі реалізувати право на конфіденційність зовсім не так просто, адже за кожною з цих позицій можна виявити безліч різних інтересів як з боку IT-бізнесу, так і з боку національних держав і користувачів. Тим більше, що на порядку денному для законодавства, крім традиційних проблем безпеки, кіберзлочинності, електронного нагляду і стеження, вже стоять і виклики, пов'язані з цифровою економікою, заснованої на Big Data. Обробка величезних масивів таких даних стала новим економічним драйвером економічного розвитку. Бізнес-модель, заснована на використанні таких даних про клієнтів, набуває все більшого поширення у страховій, банківській справі, медицині, електронної комерції, транспорті та логістиці та багатьох інших сферах. Користувачі фактично оплачують безкоштовні на перший погляд інтернет-послуги своїми персональними даними, наприклад, заповнюючи різні форми на сайтах і при здійсненні платежів або дозволяючи користуватися файлами-cookie своїх браузерів про історію відвідин сайтів.

Все більшою мірою сферою використання Big Data стає сфера державного управління, де збільшується кількість електронних сервісів. За допомогою таких технологій можна налагодити логістику, транспортного та медичного обслуговування у великих містах, превентивно виявляти і попереджувати злочини, набагато швидше реагувати на виникнення і поширення епідемій і багато іншого. Не менш важливо й використання таких даних в інтересах державної безпеки, при боротьбі з тероризмом і злочинністю.

У найближчому майбутньому виросте кількість даних, отриманих в результаті взаємодії самих «розумних пристроїв» між собою і візуально-звукових даних. Триватиме і кіборгізація людини, тобто вбудовування технологій у людське тіло – від технологій інвазивних інтерфейсів «мозок-комп'ютер» до найрізноманітніших нейропротезів і імплантантів. Як наслідок, обсяги найрізноманітніших даних, у тому числі і візуально-звукових, біометричних, будуть стрімко збільшуватися, стаючи джерелом нових правових колізій.

Технології великих даних, таким чином, одночасно стали як стимулом для нової економіки 4.0 та частиною державного управління, так і перетворилися в серйозний виклик для правового регулювання. Сформовані практики збору даних укупі з їх вільної передачею підірвали існуючі механізми захисту даних. Законодавство про регулювання захисту персональних даних у нових технологічних умовах має тривалу історію, але зараз від законодавців потрібні чималі зусилля, щоб створити систему правових заходів для захисту права на конфіденційність.

Тим часом експерти вважають, що цілі і технології Великих даних суперечать базовим принципам існуючого законодавства про персональні дані, таким, як: відповідність цілей обробки персональних даних цілям, заздалегідь визначеним і заявленим при зборі персональних даних, обмеження обсягу зібраних і оброблюваних даних мінімально необхідним обсягом, здійснення обробки даних на основі інформованої згоди. Деперсоналізація/знеособлення персональних даних, що перетворює їх в ті знеособлені індустріальні дані, які власне потрібні бізнесу, не виправдовує покладених на нього сподівань. Адже вони можуть бути відновлені.

На пошук нових законодавчих рішень намагається вплинути IT-бізнес, чиї інтереси відстоює могутнє лобі (бізнес- і торгові асоціації, консалтинг, експерти і т. д.). У той же час поступово формується, і призначена для користувача інформаційна культура і активними учасниками пошуку правових рішень, які відстоюють права громадян на контроль за персональною інформацією, стають великі медіа- і споживчі асоціації, рух за персональну демократію, правозахисні організації (неолуддизм, техноаскетизм і ін.).

Право і законодавство відповіло на виклики нового етапу інформаційної економіки появою нових законів щодо захисту персональних даних. Перш за все це європейський регламент «Про захист персональних даних і про вільне переміщення таких даних» – General Data Protection Regulation (GDPR), який вступив у дію з 23 травня 2018 року – регулятивний інструмент, заснований на великих штрафах, який орієнтований, насамперед, на таку жорстку для бізнесу міру як значні грошові штрафи за порушення при обробці персональних даних, якщо про це не буде повідомлено регулятору протягом 72 годин. У кожній компанії повинен бути проведений моніторинг організації роботи з персональними даними та призначений спеціальний співробітник із захисту даних, що контролює дотримання нових вимог законодавства.

Європейські користувачі мають право запросити у компанії підтвердження факту обробки їх даних, а також уточнити, кому і яка інформація передається, дізнатися джерело отримання даних, вимагати припинення обробки своїх даних. Право на забуття дає змогу видаляти свої особисті дані за запитом, щоб уникнути їх розповсюдження або передачі третім особам. При виявленні порушень в процесі обробки і зберігання персональних даних громадяни ЄС можуть написати заяву і звернутися у національні регуляторні

органи для розслідування. Згода на обробку персональних даних має бути виражена у формі ствердження і активних дій користувача, а не за замовчуванням у формі бездіяльності.

У GDPR також введено нове право на портабіліті: на вимогу суб'єкта даних, компанії зобов'язані надавати безкоштовно електронну копію персональних даних іншої, обраної користувачем компанії, хоча на практиці цим поки найчастіше важко скористатися через технічні відмінностей між інформаційними системами та відсутності для цього функціоналу.

Так, у вересні 2018 року від злому мережі Facebook постраждали 50 млн. користувачів, 5 млн. з яких виявилися жителями ЄС. У той же час Facebook зробив ряд кроків щодо виконання нових вимог. Зокрема, виконуючи вимогу GDPR про портабіліті, Facebook і його дочірня компанія Instagram надали користувачам можливість вивантажувати історію пошуку, оновлення статусів і дзвінків, теги розташування й ін. Для недопущення використання персональних даних у рекламних цілях без згоди користувачів були внесені зміни в політику конфіденційності і створені додаткові механізми роботи з персональними даними користувачів. Були внесені зміни в налаштування приватності: щоб посилити контроль користувачів над контентом, додано нове діалогове вікно з проханням дати згоду на обробку тієї чи іншої інформації (в тому числі в маркетингових цілях). Однак ці нововведення вже зазнали критики як незадовільні.

Постраждали від штрафів і менш великі компанії, наприклад, у 2018 році був сплачений штраф у розмірі 20 тис. євро чат-додатком для знайомств Knuddels, а португальська лікарня Barreiro Hospital була оштрафована на 300-400 тис. євро за уразливість системи зберігання персональних даних пацієнтів. Таким чином, GDPR грунтовно вплинув на законодавство інших країн, не дивлячись на значні відмінності у правових традиціях та системах, і багато визначив у напрямках розвитку законодавства щодо захисту персональних даних інших країн. Так, деякі принципи GDPR, зокрема, штрафні санкції як засіб регулювання захисту персональних даних, було використано у прийнятому в Каліфорнії (США) законі «Про захист даних інтернет-користувачів», відповідно до якого користувачі отримали право запросити у компаній інформацію про те, які саме персональні дані про них були зібрані, як і чому вони використовуються, перелік третіх осіб, яким ця інформація стала відома, мету збору персональних даних та їх джерела. Користувач може зажадати видалити інформацію про себе з серверів компанії і третіх осіб і заборонити їм продаж цієї інформації Користувач має право подати до суду на організацію, яка неправомірно скористалася його персональними даними або не виконала його запиту у термін. На компанію-порушника за таким позовом може бути накладено грошовий штраф до 750 доларів.

У зв'язку з цим, досить актуальним нині є питання, що стосується видів шахрайства із використання банківських платіжних карт. Розглянемо його більш детально.

Шахрайства із використанням пластикових платіжних карток стають все більш масовим явищем, як в Україні, так і у світі. Вказана тенденція пов'язана із широким розповсюдженням даного виду платіжних засобів, що, у свою чергу, є результатом діяльністю держави, спрямованої на поступове обмеження операцій із готівковими платежами.

Шахрайство із кредитними картами можна визначити, як незаконне заволодіння чужими коштами з використанням карт-дублікатів, або отриманих шляхом обману даних. Схема такого шахрайства з банківськими картами полягає у використанні платіжної карти для виконання злочинного задуму, результатом якого є заволодіння чужими коштами у вигляді готівки або для оплати товару або послуги через мережу інтернет. Важливо те, що даний процес відбувається без насильства і людина сама віддає дані або переводить деяку суму шахраям.

Можна виділити такі найпоширеніші способи шахрайства із використання банківських платіжних карт [2]:

1. Вдаване опитування у соцмережах з розіграшем призів. Цей спосіб шахрайства в інтернеті вперше з'явився у 2019 році. У соціальних мережах та групах, створених у популярних месенджерах, почали з'являтись повідомлення про опитування з розіграшем грошових призів від імені великого банку або відомої компанії. Після участі в розіграші шахраї надсилали людям повідомлення про виграш великої суми і прохання надіслати дані кредитної карти для отримання грошового переказу. Люди називали номер карти, CVC-код, та пароль, який з SMS, що прийшов на телефонний номер, після чого з їх карти були вкрадені гроші.

2. Телефонний дзвінок з метою отримати секретні дані. Шахрай дзвонять жертві і представляється співробітником банку і повідомляє про підозрілу транзакцію, яку заблокував банк. Він просить назвати персональні дані і цифри з карти для «перевірки». Потім він «надсилає» SMS з разовим кодом, який просить повідомити. Насправді шахраї проводять платіж в інтернет-магазині, вказавши дані карти, і їм не вистачає лише разового коду для проведення платежу, який банк надсилає на фінансовий номер.

3. Заміна SIM-карти для доступу до онлайн-банкінгу. Відомі випадки, коли шахраї звертались до мобільного оператора, щоб замінити «загублену» SIM-карту, видаючи себе за її власника. Це можливо зробити, вказавши номер телефону і 2-3 контакти з телефонної книги (якщо вона була не іменна, без контракту). Замінивши SIM-ку, шахраї отримували доступ до банківського акаунту жертви, збільшували кредитний ліміт і знімали всю готівку у банкоматі без використання самої карти, або розраховувались за товари в інтернеті.

4. Платежі онлайн на незахищених сайтах. Інтернет-шахраї, які володіють знаннями про цифрові технології передачі даних, можуть легко викрасти незашифровану інформацію, підключившись до комп'ютерної мережі. Щоб інформація не потрапила в руки шахраїв, її необхідно шифрувати.

Шифроване підключення до сервера, на якому розміщений веб-сайт, захищає інформацію про кредитну карту при передачі від комп'ютера користувача до серверу. Якщо адреса сайту починається тільки з 4 букв

HTTP, це означає, що веб-майданчик використовує застарілу технологію передачі даних без шифрування і передавати через нього платіжну інформацію небезпечно.

5. Фішинг – підробка веб-сторінок та електронних листів. Дуже небезпечний і поширений вид шахрайства, який полягає у тому, що спеціально для крадіжки інформації шахраї створюють веб-сторінки або відправляють електронні листи на email від імені відомих веб-ресурсів, послугами яких жертва часто користується.

6. Копіювання даних карти при передачі у руки. Такий вид шахрайства поширений у деяких країнах, куди приїжджає багато туристів. Продавці або офіціанти у ресторанах беруть у клієнтів картки для оплати і непомітно записують, або фотографують їх номери та CVV коди. Випадок викрадення даних карти був зафіксований у Бразилії під час проведення Олімпійських ігор 2016.

7. Незахищені мережі WI-Fi. Серед людей, які теж підключились до Wi-Fi мережі, може знаходитись шахрай, або хакер, який полює за конфіденційною інформацією. Такі мережі можна використовувати лише для перегляду звичайних сторінок веб-сайтів, або для обміну неконфіденційною інформацією. Не варто ризикувати, оплачуючи онлайн покупки, чи заходити до власного банківського акаунту, використовуючи мережу Wi-Fi в публічних місцях.

8. Комп'ютери в громадських місцях. У бібліотеках або інформаційних центрах часто встановлюють комп'ютери для доступу в інтернет. Такі комп'ютери можуть бути обладнані спеціальним програмним забезпеченням для відстежування дій користувачів, запам'ятовування інформації, введеної з клавіатури. Шахраї можуть скористатись такими комп'ютерами, щоб вкрасти логіни та паролі для входу в персональний обліковий запис. Безпечність публічних (чужих) комп'ютерів не завжди можна перевірити, тому держіть інформацію про свою кредитку подалі від таких мереж.

9. Скіммінг для крадіжки даних карти. Скіммери використовують спеціальне обладнання для крадіжки даних карти. Спеціальні накладки на картридж для картки та на клавіатуру для введення пін-коду можуть виглядати гармонійно (як і має бути), навіть якщо їх добре видно.

Крім того, слід остерігатись прихованих відеокамер для запису інформації з карти, прикріплених шахраями. Безпечніше користуватись банкоматами, що знаходяться у відділеннях банку чи у великих супермаркетах.

10. Несанкціоноване проведення мікроплатежів. Даний вид фінансових втрат по кредитці на завжди відноситься до шахрайства. Деякі цілком легальні та авторитетні веб-ресурси, на яких користувачі добровільно прив'язують карту для оплати послуг, можуть бути налаштовані для автоматичного списання коштів раз на місяць. Попередження користувача може бути відсутнім, непомітнім або незрозумілим. Цей спосіб використовується деякими платформами для фрілансу, онлайн бібліотеками, сховищами для зберігання файлів, або соціальними мережами. Списання відбувається тоді, коли закінчується період безкоштовного пробного або платного використання послуг.

11. Шахрайство з використанням банкомату: зняття готівки з використанням «білого» пластику; використання інструментів для скімингу (копіювання даних платіжних карт, у т. ч. з магнітної смуги, записів ПІН-коду і т.д.); зняття коштів з використанням банкомату без відображення цієї операції на рахунку; зняття готівки власником платіжної картки без її фізичного отримання; фізичні атаки на банкомати.

12. Інтернет шахрайство: використання шкідливих програм (вірусів), підроблених сайтів з метою компрометації реквізитів електронних платіжних засобів та/або логінів/паролів доступу до систем інтернет/мобільного банкінгу; розповсюдження (продаж, розповсюдження) інформації щодо скомпрометованих даних.

13. Шахрайство у термінальній мережі: здійснення операцій з використанням підробленої/викраденої/втраченої платіжної картки; отримання готівки через касу банку з використанням підроблених документів і платіжної картки; проведення дублюючих операцій касиром/оператором; проведення несанкціонованого/неточного списання (коли сума на чеку і сума, яку включено в розрахунок, відрізняються); компрометація касиром даних платіжної картки при розрахунках в торгово-сервісній мережі з метою її подальшого несанкціонованого використання; використання накладок (скімерів) на термінальному обладнанні, які дозволяють при здійсненні розрахунку зчитувати і передавати дані платіжної карти (протиправна домовленість з касирами); установка шкідливих програм, які пошкоджують програмне забезпечення терміналів.

14. Шахрайство у системах дистанційного обслуговування (ДБО). Несанкціоноване втручання та/або установка шкідливих програм (вірусів), які пошкоджують програмне забезпечення персональних комп'ютерів і перехоплюють паролі доступу до рахунків, інформацію з секретних ключів/токенов тощо.

15. Соціальна інженерія. Виманювання шахраями, які входять у довіру до власників рахунків/утримувачів карток, їх персональних даних, реквізитів платіжних карток або спонукання власників рахунків до здійснення переказу коштів на користь шахраїв.

Як бачимо, способи шахрайства з банківськими картами досить різноманітні, тому варто ознайомитися з основними правилами безпеки [7].

1. Дуже важливо стежити за тим, щоб Пін-код карти не став відомий третім особам. Варто пам'ятати про те, що ні працівники банку, і ніхто інший не має права запитувати у вас код від карти та інші дані. Ніколи не пишіть на карті код і намагайтеся не показувати стороннім клавіатуру, коли його вводите. Помніть, що якщо співробітникам банку знадобляться якісь ваші дані або щось відбудеться з картою, вас обов'язково запросять у відділення. Ці дані ніколи не запитують по телефону.

2. Перш, ніж ви вставите карту у банкомат, огляньте його на предмет накладної клавіатури і інших неприродних для такого обладнання пристосувань. Самий вірний варіант – це користуватися банкоматом, установленим у відділенні банку або магазинах.

3. Шахрайство із кредитними картами в інтернеті найпоширеніший варіант афери, і щоб не попастися, найкраще користуватися перевіреними сайтами відомих компаній, які вже довгий час працюють на ринку. Пам'ятайте, що сумлінні компанії ніколи не приховують своїх даних, і вони завжди залишаються доступними відвідувачам сайту. Звичайно, найкраще буде, якщо є можливість оплачувати товар уже після його одержання.

4. Завжди ведіть облік руху коштів на вашій карті. Шахраї кредитні карти можуть знімати незначні суми, і при відсутності контролю ви можете цього не помітити. Намагайтеся зберегти всі виписки по операціях, а також установити на своєму телефоні функцію, яка у режимі онлайн дасть змогу відслідковувати картковий баланс.

5. Якщо ви помітили, що втратили карту або її украли, відразу ж зверніться до співробітників банку. Таким чином, імовірність того, що ви залишитеся зі своїми грішми набагато вища.

6. Ніколи не залишайте свою карту без нагляду і просіть співробітників ресторану або будь-якого іншого закладу проводити всі операції у вашій присутності.

7. Якщо ви часто проводите купівлю товару через інтернет, то радимо вам завести карту спеціально для таких операцій. Приміром, коли вам потрібно оплатити товар або послугу ви переводите на спеціальну карту рівно таку суму, яка потрібна для оплати. У найгіршому випадку, ви просто втратите цю суму, а інші ваші заощадження залишаться цілими.

8. Установите денний ліміт на зняття готівки.

Якщо все-таки шахраї банківські карти змогли заволодіти, то потрібно, якнайшвидше звернутися у відділення банку і описати ситуацію, з якої ви зіштовхнулися. Номер гарячої лінії можна знайти на звороті банківської карти. При розмові з оператором вам потрібно буде пройти ідентифікацію особи і відповісти для цього на кілька питань. Після цієї процедури оператор банку блокує карту, і кошти залишаються недоступними для зловмисників.

Таким чином, аналіз основних напрямів протидії шахрайствам із використанням банківських платіжних карток, свідчить про те, що перспективним напрямом такої діяльності є використання чіп-модулів на банківських платіжних картках, оскільки окремі показники безпеки інформації можуть бути досягнуті виключно із застосуванням додаткових механізмів технічного захисту інформації, яка зберігається на банківських платіжних картках. При цьому, чипові платіжні картки, які використовуються у Національній системі масових електронних платежів цілком відповідають зазначеним вимогам, а отже можуть розглядатися як один із перспективних платіжних механізмів в умовах активізації шахрайств у сфері карткових платежів.

Як бачимо з вищесказаного, актуальною проблемою на сьогодні є фішинг-атаки у хмарному середовищі. Фішинг – це один із різновидів інтернет-шахрайства, який дозволяє обманним шляхом отримувати різну цінну інформацію, маскуючи комунікації так, ніби вони надійшли з надійного джерела. Надалі інформація може бути використана для доступу до пристроїв або мереж.

Концепція фішингових атак вперше була визначена у 1987 році у документі, представленому на конференції Interex під назвою «Безпека системи: перспектива для хакера». З точки зору етимології, перше вживання слову «фішинг» зустрічається у хакерському інструменті AOHell у 1996 році.

Найбільш ранні відомі спроби фішингу, націлені на сектор фінансових послуг, були зафіксовані в 2001 році. Їхньою метою став сервіс «цифрової золотої валюти» E-gold. До жовтня 2003 року зловмисники кілька разів атакували BankofAmerica, CitiBank, PayPal, Lloyd'sofLondon і Barclays. За даними Робочої групи по боротьбі з фішингом (Anti-Phishing WorkingGroup), кількість унікальних фішингових атак, зафіксованих організацією у 2005 році, склала 173 тисячі. Але вже у 2015 році цифра збільшилася до рекордно високого рівня у 1,413 млн. Втім, у 2017 році це число зменшилося до 1,122 млн. [9].

Тобто фішинг – це схема, за якої хакери змушують користувачів передавати конфіденційну інформацію. Цей вид шахрайства, заснований на довірі та заволодінні злочинцем аккаунтом іншого користувача. Він, зазвичай, передбачає надсилання користувачу соціальної мережі повідомлення, яке ніби походить із довіреного джерела, наприклад від знайомого з проханням позичити електронних грошей, скачати контент або перейти за посиланням. Людина не може точно знати, хто відправив їй повідомлення – друг чи шахрай, який заволодів його сторінкою, і, як правило, вона, не замислюючись про це, виконує прохання [1].

Досить поширеним явищем у мережі є випадки, коли у повідомленні може бути посилання на віруси, черв'яки, троянські програми, що створені для зараження комп'ютера з метою його пошкодження, викрадення особистої інформації, шпигунства чи показу реклами. Найбільш простий спосіб захистити свій комп'ютер від мережевих атак – встановити на нього та належним чином налаштувати антивірусне програмне забезпечення та міжмережевий екран. Фармінг – це перенаправлення жертви за помилковою адресою, наприклад, це імітація сторінки авторизації у соціальну мережу з метою заволодіння логіном та паролем від облікового запису. Аби не потрапити у цю пастку необхідно уважно дивитися, за якими посиланнями та сторінками здійснюється перехід та використовувати механізм двофакторної аутентифікації у соцмережі.

Хмарне сховище даних – модель онлайн сховища, в якому дані зберігаються на багато чисельних серверах у мережі, які надаються для користуванням клієнтам третьою стороною. Якщо проаналізувати статистику втрат даних з хмарних сховищ, то можна виділити короткий перелік порад, які допоможуть підвищити безпеку даних.

Одна з причин, яка спричиняє заволодіння доступом до даних зловмисниками є нехтування правил безпеки по підбору пароля. Дуже часто, щоб не забивати голову різними паролями, люди використовують один пароль для найрізноманітніших сайтів. Зазвичай, це номер телефону, електронна пошта або логін (у залежності від сервісу). Далі, зловмисник зламавши профіль на сайті з низьким рівнем безпеки, може без перешкод зайти на інший сервіс простою підстановкою того ж пароля. Чим складніше буде пароль, тим важче його зламати. Але всі ці поради лише зменшать ризик і ніяк не зможуть повністю попередити їх втрату.

Якщо брати до уваги саме хакерські атаки, то найбільш поширеними видами атак є направлений фішинг та «WateringHoles». При фішингу, зловмисники можуть написати електронного листа легітимному працівнику від імені його колеги по роботі, де запитати персональні дані і отримати відповідь із правдивими даними. Дуже велика кількість користувачів інтернет-сервісів не мають мінімальних знань по безпеці у мережі, а саме, що сервіси не розсилають листів з проханнями повідомити у відповідь особисті дані (паролі, логіни, номера телефонів тощо).

Зазвичай зловмисники використовують наступні методи фішингу у своїх атаках [9]:

1. Обманні веб-посилання. Найбільш часто використовувана стратегія полягає в тому, що шахраї маскують зловмисне веб-посилання як вказівку на легітимне або довірене джерело. Ці типи фішингових атак можуть приймати будь-яку кількість форм, наприклад, застосування шахрайських URL-адрес, створення піддомену для зловмисного веб-сайту або експлуатація дуже схожих доменів.

2. Інтернаціональні доменні імена (IDN) також можуть використовуватися для створення заплутано схожих доменних імен, дозволяючи використовувати не-ASCII символи. Візуальні подібності між символами в різних сценаріях, які називаються гомогліфами, застосовують для створення доменних імен, що візуально неможливо диференціювати. Це спонукає користувачів приймати один домен за інший.

3. Клонування веб-сайтів, підробка та перенаправлення. Веб-сайти, вразливі до атак типу межсайтовий скриптинг (XSS), використовуються зловмисниками для запису власного контенту на інший веб-сайт. XSS-атака може застосуватися для перехоплення даних, введених на скомпрометованому сайті (включно з ім'ям користувача та паролем), які зловмисники використають пізніше.

Деякі фішингові атаки використовують XSS для створення вікон, що спливають, які походять з вразливого веб-сайту, але притому завантажують сторінку, що контролюється зловмисниками. Часто такий тип прихованого перенаправлення відкриває форму для входу з метою збору реєстраційних даних. Через поширення цього типу атаки більшість браузерів тепер показують адресний рядок у вікнах, що спливають.

4. Голосовий та текстовий фішинг. Для отримання інформації про обліковий запис зловмисники використовують телефонні дзвінки та текстові повідомлення. Спочатку вони надсилають клієнтам банків повідомлення, де стверджують, що їхній обліковий запис заблоковано. Це спонукає користувачів подзвонити на вказаний номер телефону або зайти на веб-сайт, що контролюється шахраями, і залишити конфіденційну інформацію.

Можна виділити наступні види атак з використанням фішингу [3]:

• Класичний фішинг. Фішингові листи, відправлені від імені відомих дійсно існуючих компаній, які практично не відрізняються від листів, які користувачі, зазвичай, отримують від цих компаній. Єдина відмінність може полягати у проханні пройти по посиланню, щоб виконати якусь дію.

• Цілеспрямована фішингова атака. Персоналізовані фішингові листи, спрямовані на конкретну людину. Такі листи містять ім'я, посаду потенційної жертви, а також будь-які інші особисті дані.

• Фішинг проти топ-менеджменту. Фішинг-листи націлені на отримання доступу до облікового запису глави компанії, генерального директора, технічного директора і т.д. Після отримання доступу до таких облікових записів фахівці з фішингу можуть продовжувати використовувати їх для зв'язку з іншими відділами, наприклад, підтверджувати шахрайські банківські перекази будь-якому фінансовій установі за власним вибором.

• Фішинг розсилки від Google і Dropbox. Відносно новий напрямок фішингових атак, метою яких є імена користувачів і паролі для входу в хмарні сховища даних.

• Фішингові листи з прикріпленими файлами. Фішинг-листи з вкладеннями, що містять віруси.

• Фармінг. Прихована переадресація на шахрайський сайт, виконаний за допомогою зміни кеша DNS на локальному комп'ютері або мережевому обладнанні.

На жаль, проти фішингових атак не існує надійних засобів. Адже майже всі подібні атаки значною мірою покладаються на соціальну інженерію, з метою переконати користувачів негайно вжити заходів і, тим самим, блокуючи можливість та бажання детального аналізу ситуації. Через це найкращим захистом від фішингу є навчання кінцевих користувачів правилам безпеки.

Крім того, виробники захисних рішень розробили спеціальні фільтри з метою виявлення фішингових атак в електронних листах. Утім, в деяких повідомленнях шахраї використовують зображення тексту замість звичайного текстового формату, щоб уникнути цих фільтрів в пошті. Крім того, фішингові веб-сайти часто покладаються на методи заплутування коду, щоб запобігти детектуванню зловмисної активності з боку систем захисту. Зазвичай фішингові атаки застосовують шифрування на базі алгоритмів AES-256 або Base64 у JavaScript, або ж інші методики, що ускладнюють аналіз базового вихідного коду.

До речі, нещодавно дослідники Proofpoint розкрили фішинговий інструментарій, який заплутує отримувача листа за допомогою шифру заміщення, який спирається на спеціальний шрифт. Цей інструментарій використовує незвичайну версію шрифту Arial з окремими транспонованими літерами; при

завантаженні фішингової сторінки контент виглядає нормально. Але коли користувач або програма намагаються прочитати вихідний текст на сторінці, він показується змішаним.

Оскільки фішингові атаки активно застосовують соціальну інженерію, навчання користувачів є найважливішою стратегією захисту компанії. Якщо їх навчити, як виявляти ознаки шахрайських електронних листів та час від часу проводити в компанії таємну імітацію фішингових атак з метою перевірки ефективності цього навчання, такі дії забезпечать набагато кращий захист, ніж спеціалізовані програмні рішення.

Не менш важливою є політика захисту працівників від мимовільного переказу коштів та заборона доступу до даних для нелегальних цілей. Взагалі, за думкою експертів, безпека починається саме з чітко визначених політик – підприємства повинні мати узгоджену політику для таких ситуацій і навчати своїх співробітників.

З технологічної точки зору, варто провести правильне налаштування клієнтів електронної пошти, таких як Microsoft Outlook, адже параметри за замовчанням не є оптимальними для безпеки. Крім того, інструменти для сканування повідомлень від сторонніх виробників можуть зменшити ефективність фішингових атак або навіть запобігти їхньому потраплянню до поштових скриньок користувачів.

Також сучасні веб-переглядачі включають так звані служби Безпечного перегляду, які увімкнені вже за замовчуванням. Вони здатні виявляти фішингові атаки й захищати від них користувачів.

Крім того, для боротьби проти фішингу розроблено багато методів: браузери, які попереджають про загрозу фішингу, посилена процедура авторизації, спам-фільтри, послуги моніторингу тощо. При WateringHoles хакери розміщують програми у коді сайту. У результаті таких дій, користувач, переходячи на сайт, може передати вірус у всю мережу підприємства, а хакер отримає доступ до даних цієї мережі.

Паралельно з цим, можна виділити такі основні методи боротьби з фішинговими сайтами та іншими видами онлайн-шахрайства [3]. Перший з них це використання одноразових паролів. Класичні паролі є багаторазовими: користувач вводить один і той же пароль кожного разу при проходженні процедури аутентифікації, не змінюючи його часом роками. Перехоплений зловмисником, цей пароль може неодноразово використовуватися без відома господаря. На відміну від класичного, одноразовий пароль використовується тільки один раз, тобто при кожному запиті на надання доступу користувач вводить новий пароль. Для цього використовуються, зокрема, спеціальні пластикові картки з нанесеним захисним шаром. Клієнт банку кожен раз стирає чергову смужку і вводить потрібний одноразовий пароль. Всього на картку стандартного розміру поміщається близько 100 паролів, що при інтенсивному використанні послуг телебанкінгу вимагає регулярної заміни носія. Більш зручними, але, правда, і дорогими представляються спеціальні пристрої – генератори одноразових паролів.

В основному розрізняють два типи створення: за часом, коли поточний одноразовий пароль відображається на екрані і періодично змінюється (наприклад, раз в дві хвилини); за подією, коли нове значення генерується кожен раз при натисканні користувачем на кнопку пристрою. Будучи більш безпечним, ніж класична парольна аутентифікації, такий метод, проте, залишає зловмисникові певні шанси на успіх. Наприклад, аутентифікація з використанням одноразових паролів не захищена від атаки «людина посередині». Суть її полягає у «вклинюванні» в інформаційний обмін між користувачем і сервером, коли зловмисник «представляється» користувачу сервером, і навпаки. Серверу передається вся інформація від користувача, в тому числі і введений нею одноразовий пароль, але вже від імені зловмисника. Сервер, отримавши правильний пароль, дозволяє доступ до закритої інформації. Не викликаючи підозр, зловмисник може дозволити користувачеві попрацювати, наприклад, зі своїм рахунком, пересилаючи йому всю інформацію від сервера і назад, але при завершенні користувачем свого сеансу роботи не розривати зв'язок з сервером, а зробити потрібні транзакції нібито від імені користувача.

Щоб не витрачати час в очікуванні завершення сеансу користувача, зловмисник може просто імітувати помилку зв'язку і не дозволяти легальному користувачеві працювати зі своїм рахунком. Залежно від використовуваного методу генерації перехоплений одноразовий пароль буде діяти або протягом короткого часу, або тільки для першого сеансу зв'язку, але в будь-якому випадку це дає зловмиснику можливість успішно провести крадіжку даних або грошей користувача. На практиці аутентифікація за допомогою одноразових паролів сама по собі використовується рідко, для підвищення безпеки застосовується встановлення захищеного з'єднання ще до аутентифікації, наприклад, з використанням протоколу SSL.

Другим відомим методом є одностороння аутентифікація користувача. Використання протоколу безпечних з'єднань SSL (SecureSocketsLayer) забезпечує захищений обмін даними між Web-сервером і користувачами. Незважаючи на той факт, що протокол дозволяє аутентифікувати не тільки сервер, але і користувача, на практиці найчастіше застосовується тільки одностороння аутентифікація. Для встановлення SSL-з'єднання необхідно, щоб сервер мав цифровий сертифікат, який використовується для аутентифікації. Сертифікат, зазвичай, видається і засвідчується третьою довіреної стороною, в ролі якої виступають центри сертифікації (ЦС). Роль ЦС полягає у тому, щоб підтверджувати оригінальність Web-сайтів різних компаній, дозволяючи користувачам, повіривши одному єдиному ЦС, автоматично мати можливість перевіряти справжність тих сайтів, власники яких зверталися до цього ж самого ЦС. Список довірених центрів, що засвідчують, зазвичай, зберігається в реєстрі операційної системи або в настройках браузера. Саме ці списки і піддаються атакам з боку зловмисника. Дійсно, видавши фішинговому сайту сертифікат від підробленого ЦС, що засвідчує, і додавши цей ЦС в довірені, можна, не викликаючи жодних підозр у користувача, успішно

здійснити атаку. Звичайно, такий спосіб потребує від шахраїв більше зусиль і відповідно витрат, але користувачі, на жаль, часто самі допомагають у крадіжці своїх даних, не бажаючи розбиратися в тонкощах і особливостях використання цифрових сертифікатів.

Справа в тому, що останнім часом почастішали випадки, коли сайти, заражені троянськими програмами, і самі трояни використовують протокол SSL з тим, щоб уникнути шлюзові системи фільтрації трафіку – адже шифровану інформацію ні антивірусне ядро, ні система захисту від витоку даних перевірити не в стані. Втручання в обмін між Web-сервером і призначеним для користувача комп'ютером дозволяє таким чином замінити сертифікат Web-сервера на виданий, наприклад, корпоративним СЦ і без видимих змін в роботі користувача сканувати трафік користувача при використанні протоколу SSL.

Третій та доволі ефективний метод протидії – це URL-фільтрація. У корпоративному середовищі фільтрація сайтів застосовується для обмеження нецільового використання мережі Інтернет співробітниками і як захист від фішерських атак. У багатьох антивірусних засобах захисту даний спосіб боротьби з підробленими сайтами взагалі є єдиним. Виявленням фішерських сайтів і внесенням їх у чорні листи займаються багато компаній – від виробників антивірусних рішень до банків, платіжних систем і правоохоронних органів. Зокрема, створюються спеціальні організації для боротьби з фішерами, такі як AntiPhishingWorkGroup (APWG – http://www.apwg.org).

Спільні заходи зацікавлених сторін у тісній співпраці з реєстраторами та хостингових компаній дозволяють оперативно закривати підроблені сайти. Спільні зусилля спрямовані на максимально швидке оновлення чорних списків і блокування роботи сайтів зловмисників. Однак далеко не всі виробники засобів антивірусного захисту можуть похвалитися такою високою оперативністю в оновленні баз, до того ж багато користувачів не використовують ніяких засобів захисту на своїх комп'ютерах або вводять номери кредитних карт і іншу конфіденційну інформацію з випадкових робочих місць.

Для захисту від загроз необхідно мати на увазі наступне:

- потрібно реєструватися тільки у тих соцмережах, які викликають довіру та пропонують надійні механізми аутентифікації і розмежування доступу до особистої інформації користувача;

- слід пам'ятати, що будь-яка інформація, розміщена в інтернеті, з великою імовірністю залишається там назавжди, навіть в разі її видалення автором, адже може бути збережена або поширена іншими користувачами;

- особливу увагу слід приділяти посиланням, які надходять від інших користувачів – вони можуть бути частиною фішингової чи фармінгової атаки.

Старі та перевірені методи шахрайства досі успішно працюють, але постійно модифікуються. Серед нових винаходів шахраїв можна виділити наступні схеми:

1. Схеми з працевлаштуванням. З'явилося два нових розповсюджених способи виманити кошти у тих, хто шукає роботу. Перший – кадрове агентство, яке обіцяє багато пропозицій від роботодавців. Але спочатку кандидат має зробити і надіслати селфі з паспортом. Другий – робота вдома, наприклад, набір тексту чи сортування кавових зерен, за яку аферисти просять заплатити завдаток, своєрідний гарантійний внесок.

За бажання працювати вдома доведеться заплатити, але один раз. Натомість, надсилаючи фото документу, ви ризикуєте отримати кілька кредитів у МФО, які дають позики онлайн, та довго сплачувати заборгованість.

2. Тенета для романтиків.Чим більше аферисти знають про людські слабкості та бажання, тим легше їм створювати нові приманки. Романтичне шахрайство прийшло до нас з Європи. Зловмисники шукають жертв у соціальних мережах та на сайтах знайомств. Потім розсилають їм романтичні електронні листи – і будь-яким способом виманюють гроші.

Набула популярності схема з кінотеатром. Самотня жінка чи чоловік спокушаються на запрошення незнайомця провести романтичний вечір разом. Аферист обирає на свій смак приватний кінотеатр для двох. Далі – прохає придбати квитки у кіно. Жертва оплачує їх за посиланням на шахрайському сайті, після чого «прекрасний» незнайомець чи незнайомка зникає. Часто зловмисники маніпулюють почуттями до близьких людей. Не втрачають дієвості фрази: «кохана, я в біді» або «мама, я в лікарні».

3. Онлайн-обмінники. Все більше товарів та послуг ми шукаємо і оплачуємо онлайн. Щоб перевірити сайт, достатньо за кілька хвилин почитати відгуки в інтернеті чи подивитися чорний список. На жаль, громадяни ігнорують заходи безпеки та купуються на зручність і легкість здійснення операцій. Тому часто кошти зникають на невідомих рахунках чи номерах мобільних телефонів.

4. Фальшиві інвойси. Новий вид шахрайства – схеми з інвойсами, тобто документами, які надсилає продавець покупцеві при оплаті товару. Інвойс містить інформацію про ціни та кількість товарів і послуг, які замовляє покупець. Шахраї, довідавшись про те, що жертва чекає певне замовлення, надсилають на пошту фальшиві листи з іншими реквізитами.

Останні два види шахрайства, пов'язані з обманом в електронних товарах. Справа у тому, що робити покупки через інтернет, а не бігати по магазинах, сьогодні воліють все більше людей. Такий вид торгівлі має низку переваг, зокрема значно економить, час, сили та гроші покупця. Але й тут є свої «підводні камені».

Не поодинокими зараз є випадки шахрайства в інтернеті, такі як:

1. Ви оплатили товар – товар не отримали – гроші повертати не збираються.

2. Товар назад не приймають протягом 14-ти днів.

3. Товар не ремонтують по гарантії.

Варто пам'ятати, що у випадку обману в електронних товарах Ви маєте право звернутися із заявою про шахрайство до поліції. Також можете звернутися до Державної служби України з питань безпечності харчових продуктів та захисту споживачів (http://www.consumer.gov.ua). Але, як показує практика, ці дії не завжди дають бажаний результат. Тому, якщо у вас є інформація про продавця або виробника, є підтвердження оплати товару, то найкращий спосіб захистити свої права – це звернутися з письмовою претензією до продавця, де вказати нарахування штрафу. У разі отримання відмови на претензію – вирішити спір через суд. Слід зазначити, що судовий збір за подання позовної заяви про захист прав споживачів не сплачується.

Однак, аби не потрапити у таку ситуацію, при покупці товарів через інтернет необхідно завжди звертати увагу на наступні важливі моменти [8]:

1. Репутація та добросовісність продавця. Основною метою продавця є прагнення реалізувати свій товар. Аби привернути увагу споживачів та зацікавити своїм товаром в інтернеті, продавець створює сайт або сторінку в соцмережі. При цьому покупець не знає, хто є дійсним власником (продавцем) товару. Цю інформацію він може отримати лише за наявності реальних контактних даних (адреса, телефон, вид господарської діяльності). Якщо вся інформація про продавця доступна, це дає можливість перевірити його наявність у Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань на сайті https://usr.minjust.gov.ua/

Також за необхідності це дає змогу зв'язатися з ним, запросити додаткові документи, а у разі отримання неякісного товару або неповернення коштів – надіслати на його адресу претензію, а за необхідності звернутися до суду. Адже якщо на сайті є лише номер телефону і назва сайту, то ви не зможете ні повернути товар, ні кошти, оскільки невідомо, з кого вимагати усунення порушень ваших прав.

2. Відомості про товар та виробника. Перед тим, як замовити товар, обов'язково дізнайтеся всю інформацію про продукцію. Якщо даних недостатньо на сайті, запитайте у продавця.

Ви маєте право вимагати у продавця наступну інформацію про товар:

- основні характеристики продукції: назва товару, номінальна кількість (масу, об'єм, розмір), умови використання; відомості про вміст шкідливих для здоров'я речовин, генетично модифікованих організмів, найменування та місцезнаходження виробника;
- дані про ціну (тариф), включаючи плату за доставку, та умови оплати;
- дату виготовлення;
- відомості про умови зберігання;
- гарантійні зобов'язання виробника (виконавця);
- строк придатності;
- строк доставки товару або надання послуги;
- сертифікат, якщо продукція підлягає обов'язковій сертифікації.

Також не забувайте вимагати гарантійний талон на товар. Адже протягом гарантійного строку виробник або продавець бере на себе зобов'язання з безоплатного ремонту або заміни відповідної продукції.

3. Оплата товару та його доставка. Здійснюйте оплату по факту отримання товару, після його огляду та перевірки. Якщо ви замовили доставку товару кур'єром, прослідкуйте, щоб він надав вам товарний чек з печаткою продавця, і за необхідності товарний талон та сертифікати на товар. Огляньте (протестуйте) доставлений товар. Переконайтеся, що до нього додаються всі чеки. Тільки після цього сплачуйте покупку. Якщо продавець, все ж таки, вимагає сплату частини або всієї суми коштів, скористайтеся окремою кредитною карткою з обмеженою сумою коштів. У призначенні платежу обов'язково вкажіть за що і кому сплачуєте. Надішліть на електронну пошту продавця скан-копію платіжного документу і вимагайте від нього письмового, електронною поштою підтвердження отримання такої оплати. Обов'язково зберігайте всі документи, що підтверджують зв'язок із продавцем та факт оплати товару. Це може бути електронне листування, скріншот сторінки сайту з обраним вами товаром, доказ оплати (електронна квитанція).

4. Право на повернення товару. Покупець має право розірвати укладений через інтернет-договір і повернути товар протягом 14-ти днів з моменту одержання товару. Після закінчення цього терміну повернення можливе тільки за гарантією. Це правило поширюється на непродовольчі товари належної якості за умови, що вони не використовувалися і зберегли товарний вигляд, споживчі властивості та ярлики. Також у покупця має бути наявний розрахунковий документ (чек).

В інтересах споживачів Кабінет Міністрів України затвердив «Перелік товарів належної якості, що не підлягають обміну (поверненню)». Тому повернути продукцію і отримати назад свої гроші можна далеко не за всі групи товарів. До списку «неповернення» потрапили всі продовольчі товари (їжа, напої, алкоголь, тютюнові вироби), ліки, медичні інструменти, прилади та апарати, предмети санітарної гігієни. Також обміну та поверненню не підлягають деякі непродовольчі товари: постільна та натільна білизна, косметика, парфумерія, товари для новонароджених, ювелірні вироби, друкована продукція та інше.

Врахуйте й те, що товар, придбаний через інтернет, ви будете доставляти в магазин вже самі. Якщо ж купували річ за подарунковим сертифікатом, то повернути товар в такому випадку може виявитися дуже непросто, оскільки законодавчо це питання не врегульоване. Тому вирішувати, повертати вам гроші чи обмінювати цей товар на інший будуть у торговій точці, яка випустила ваучер.

Будь-які витрати, пов'язані з поверненням продукції, покладаються саме на продавця. Якщо продавець не повертає сплачені кошти за товар або послугу у разі розірвання договору, покупець має право нараховувати неустойку у розмірі 1% від вартості продукції (послуги) за кожний день затримки повернення коштів.

5. Можливість замінити товар. Законодавство передбачає можливість заміни продавцем товару за його відсутності іншим. Про це покупця повинні повідомити перед укладенням договору.

Продавець може замінити товар тільки тоді, коли одночасно виконуються три умови:

• інший товар відповідає меті використання замовленого;

• має таку ж або кращу якість;

• його ціна не перевищує ціни замовленого товару.

Покупець, реалізуючи своє право на обмін (повернення) товару, придбаного через інтернет, повинен надіслати на адресу продавця Претензію-повідомлення з описом вкладеного у посилку (в межах 14 днів). Складність у повернені товару може виникати через цілісність його коробки (упаковки). Доволі часто можна зустріти таку умову, що товар повинен бути повністю укомплектований, а цілісність упаковки має відповідати тій, яка була на момент продажу. Зверніть увагу на те, що ви маєте право на ознайомлення зі змістом посилки. Проте слід враховувати, що товар при поверненні (обміні) має бути у повній його комплектації, інакше це зробити набагато складніше.

Варто взяти до уваги іще таких два моменти, які пов'язані із купівлею товарів в електронних магазинах, які можуть виявитися несправжніми.

1. На серйозному сайті, крім товарів, також присутня безкоштовна інформація – статті, огляди, відгуки тощо.

2. Переконайтеся, що сайт розміщений на платному хостингу. Якщо інтернет магазин знаходиться на безкоштовному хостингу, то тримайтеся від нього подалі. Власник серйозного проєкту ніколи не розмістить свій сайт на безкоштовному хостингу, тільки із-за того, що це не надійно для нього самого.

Перед здійсненням покупки спробуйте зв'язатися з автором товару або ж сайту. Переконайтеся, що там дійсно є люди, і служба підтримки реагує на ваші повідомлення. Якщо на сайті немає даних для зв'язку, то це повинно вас насторожити. Здійснюйте покупки на перевірених сайтах.

Виходячи з усього вищевикладеного, на державному рівні мають бути розроблені заходи забезпечення конфіденційності та кібербезпеки приватних користувачів та комерційних організацій. Варто зауважити, що кібербезпека – це дійсно складний процес, але вона є обов'язковою складовою успішного бізнесу. Кожна складова бізнес-процесів, представляє лише окрему ланку у нескінченному ланцюзі взаємопов'язаних елементів. Сьогодні компаніям складніше, ніж коли-небудь, чітко визначити критичні точки у власній багатогранній інфраструктурі через яку вони взаємодіють з оточуючим світом. Такі умови створюють підґрунтя для хакерських атак.

Об'єктом уваги зловмисників стають абсолютно різні за масштабами та сферою діяльності компанії. Найбільш часто, заходи безпеки обумовлюються рівнем загроз і ризиків. На жаль, кіберпростір повен загроз, проте заходи по запобігання атак повинні обумовлюватися рівнем ризику, оскільки тактика і методи кіберзлочинців постійно змінюються.

Зовнішніми загрозами для бізнесу є [6]: шкідливе ПО; DDoS-атаки; фішингові атаки; проникнення у мережу; втрата пристроїв зі збереженими паролями. Внутрішніми найпопулярнішими загрозами є вразливе програмне забезпечення та витоки через співробітників або їх з вини.

Збільшення обсягів, оброблюваних клієнтських даних, і зростаюча роль інтелектуальної власності в успіху продукту призводять до виникнення нових форм розкрадання інформації. Конкурентів цікавить інформація про внутрішні процеси у компанії, дані про співробітників, фінансова інформація, інтелектуальна власність, дані корпоративного банківського аккаунту.

Проблема кібербезпеки полягає у тому, що бізнес рідко використовує надійне антивірусне ПЗ чи спеціалізовані рішення щодо захисту від DDoS-атак, вживає дій для захисту інформації та фінансових транзакцій. Система захисту складається з багатьох взаємопов'язаних частин: організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем. Юридична складова є обов'язковою і такою, що передує усім стадіям. Своєчасного оновлення антивіруса і блокування сумнівних сайтів на офісних комп'ютерах недостатньо.

Насправді зламати інформаційні системи набагато легше, ніж забезпечити їх захист та ефективне функціонування. Універсального підходу не має. Необхідно розібратися у походженні атаки, провести розслідування, ідентифікувати вразливі місця, які дали змогу шкідливому ПО розповсюдитися. Далі потрібно вжити заходів щодо вдосконалення процесів, швидкого виявлення індикаторів кіберзагроз та мінімізувати виникнення подібних інцидентів у майбутньому. Бізнес повинен сформувати більш глибоке розуміння існуючих на сьогоднішній день кібер-ризиків, забезпечити належний моніторинг та розробити плани швидкого реагування, не обмежуючись заходами запобігання ризикам.

Впровадженню ефективної технічної складової захисту від кібератак, передує клопітка робота юристів у симбіозі з фахівцями з кібербезпеки, яка полягає у проведенні ефективного IT-комплаєнсу і ризик-менеджменту. Якщо ж уже відбувся інцидент інформаційної безпеки, юристи разом із фахівцями допоможуть провести ефективне розслідування та вплинути на порушника правовими засобами захисту за протиправне посягання.

Питання кібербезпеки наразі є досить гострим для усіх країн світу. До прийняття Закону України «Про основні засади здійснення кібербезпеки України», національне регулювання обмежувалося нормами загального характеру, прийнятими на галузевому рівні міністерств та відомств та деякою кількістю Указів

Президента України. Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу зафіксовані Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України ще у документі НД ТЗІ 2.5-004-99. Вже давно існують національні криптографічні алгоритми, відображені у відповідних ДСТУ 4145-2002 та ДСТУ ГОСТ 28147-89. Нажаль, дія вищезазначеного Закону не поширюється на відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) у комунікаційних та/або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах у мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси).

Застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом. Тому Кабінет Міністрів України повинен сформувати вимоги та забезпечити функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України (CERT-UA) періодично публікує рекомендації, які стосуються безпеки поштового сервісу, з протидії загрозі інсайдера, усунення вразливостей, пов'язаних з некоректним налаштуванням DNS-серверів, з самостійного пошуку та ліквідації веб-шеллів, тощо.

У Європі розуміють важливість захисту даних. Так, усім відомий нормативний акт Європейського Союзу, який встановлює правила роботи з персональними даними (GDPR) ставить досить жорсткі вимоги до технічної складової захисту персональних даних у тому числі. 9 травня 2018 року набрала чинності Директива Європейського парламенту і Ради (ЄС) №2016/1148, під назвою «Безпека мереж та інформації». За цією Директивою, кожна держава-член ухвалює національну стратегію щодо безпеки мережевих та інформаційних систем, що визначає стратегічні цілі та доречну політику та регуляторні інструменти з метою досягнення та підтримання високого рівня безпеки мережевих та інформаційних систем. Надавачі цифрових послуг повинні забезпечити рівень безпеки, співмірний з рівнем ризику, що виникає для безпеки цифрових послуг, які вони надають, враховуючи важливість інших послуг для операцій інших суб'єктів господарської діяльності у межах Союзу. На практиці, ступінь ризику для операторів основних послуг, які часто є істотними для підтримки важливої соціальної та економічної діяльності, є вищим ніж для надавачів цифрових послуг.

Таким чином, вимоги до безпеки для надавачів цифрових послуг повинні бути менш суворими. Надавачі цифрових послуг повинні мати свободу вживати заходи, які вони вважають належними для управління ризиками, що виникають для безпеки їхніх мережевих та інформаційних систем. Через свій транскордонний характер, надавачі цифрових послуг повинні підлягати більш гармонізованому підходу на рівні Союзу. Імплементаційні акти повинні сприяти конкретизації та реалізації таких заходів.

Отже, кібербезпека потребує постійної підтримки та аналізу її ефективності. Слід узгоджувати бізнес-ініціативи з питаннями безпеки. Важливою складовою захисту є постійне оновлення засобів забезпечення безпеки та підняття рівня захисту.

Як і в усіх інших країнах, орієнтованих на демократичну модель розвитку, під безпосереднім (за формою власності і можливостями адміністративно-правового впливу) контролем держави в Україні перебуває лише частина національної критичної інформаційної інфраструктури (НКІІ). Значний її сегмент – у галузях енергетики, хімічної промисловості, транспорту, ІКТ, банківському секторі, комунальному господарстві тощо – перебуває у приватній та інших формах власності. Поряд із цим як український так і міжнародний досвід свідчить про те, що:

1) саме недержавні об'єкти кібербезпеки, зазвичай, є найбільш вразливими для кібератак;

2) повноцінний захист таких об'єктів вимагає об'єднання зусиль приватного та державного секторів і системної взаємодії між ними;

3) широке, тобто не обмежене лише об'єктами НКІІ, КДПП є взаємовигідним і сприяє оптимізації галузевої державної політики та зміцненню національної безпеки (звісно, за умови адекватного інституційно-правового регулювання).

Сьогодні існує критична потреба у розвитку кібербезпекового державно-приватного партнерства (КДПП), яка обумовлена низкою причин, серед яких насамперед такі:

• активна приватизація деяких секторів критичної інфраструктури, унаслідок якої державні органи не можуть самостійно гарантувати повноту захисту критичної інформаційної інфраструктури;

• накопичення великої кількості електронних інформаційних ресурсів, які мають важливе значення для діяльності як приватних власників так і органів державного управління;

• залежність інфраструктури від інформаційно-телекомунікаційних систем та їхньої уразливості;

• зростаюча конвергенція комп'ютерних мереж, унаслідок чого ураження однієї з інформаційно-комунікаційних систем може суттєво позначитися на функціонуванні інших;

• у підприємств малого та середнього бізнесу, зазвичай, бракує повноважень і ресурсів для повноцінного захисту власної інформаційної інфраструктури, тому вони зацікавлені в отриманні відповідних послуг від державних органів та/або від крупних корпорацій.

Саме тому різні форми КДПП розглядаються нині як один з основних інструментів побудови ефективних систем кіберзахисту і широко застосовуються у міжнародній практиці.

Поряд із викладеним вище і недержавний сектор в Україні, і державні відомства демонструють значний потенціал для формування повноцінної платформи КДПП у загальнонаціональних масштабах. Наприклад, саме на засадах ДПП триває робота над створенням в Україні потужного центру з кібербезпеки на базі ДК «Укроборонпром». Крім представників РНБОУ, Міністерства оборони, СБУ, ДССЗЗІ, Департаменту кіберполіції, фахівців НАТО, консультантів турецької державної компанії HAVELSAN та спеціалістів НТУУ «КПІ», у проекті беруть участь громадська неприбуткова організація «Українська академія кібербезпеки» і українська команда «білих» хакерів DCUA (одна з найсильніших у світі).

З кінця 2015 р. в Україні, крім державного CERT-UA, діє офіційно акредитований міжнародною мережею FIRST приватний центр реагування та боротьби з кіберінцидентами. Ідеться про вітчизняну компанію CyS-Centrum, яка спеціалізується на моніторингу й нейтралізації ІБ-загроз з використанням апаратно-програмних рішень власної розробки, а також на консалтингу у сфері інформаційної безпеки. Ще у квітні 2015 р. МВС України та корпорація «Майкрософт» підписали Меморандум про взаєморозуміння, який засвідчив взаємну зацікавленість у співпраці у сфері захисту даних, інформаційної та кібербезпеки. У листопаді 2017 р. подібний же меморандум, спрямований на організацію взаємодії у побудові комплексних рішень технічного забезпечення відомчої діяльності у масштабах держави, застосування інновацій у сфері держуправління, а також оптимізації наявного ресурсу, був підписаний представниками Національної поліції України та компанії «Майкрософт Україна». Особливо високу динаміку розвитку КДПП демонструє Департамент кіберполіції Національної поліції України. Зокрема, з 2016 р. налагоджена системна співпраця між відомством і українськими профільними компаніями ProtectMaster (protectmaster.org) і Berezha Security (berezhasecurity.com), а також з громадською організацією «Експертів кібербезпеки» (залучення фахівців, обмін даними, проведення спільних конференцій, тренінгів для держслужбовців). Департаментом також організовано регулярний обмін інформацією та досвідом з фахівцями з Харківського національного університету радіоелектроніки і Національного аерокосмічного університету ім. М. Є. Жуковського.

Крім того, у вересні 2017 р. за сприяння Української асоціації операторів зв'язку «Телас» було підписано меморандум про співпрацю між Департаментом кіберполіції й дата-оператором lifecell, за умовами якого останній на безоплатній основі передав Департаменту систему власної розробки для екстреного інформування в умовах надзвичайних ситуацій EmergencyNotificationSystem (ENS). Серед іншого, система дає змогу локалізувати кіберзагрозу й уникнути її розповсюдження за допомогою оперативного інформування про небезпеки завчасно визначених груп отримувачів через голосові виклики, SMS та електронні листи.

При цьому Міністерство оборони України зацікавлене у розширенні спроможностей Збройних Сил України щодо підготовки та здійснення кібероборони та планує організацію державно-приватного партнерства за основними напрямами щодо [4]:

- створення кіберрезерву;
- використання інфраструктури та обчислювальних спроможностей;
- отримання консультаційної та матеріальної допомоги.

Зазначену діяльність на цей час розпочато у взаємодії з Громадською радою при Міністерстві оборони України та провідними ІТ-компаніями України. Служба безпеки України також напрацювала значний досвід у цій сфері. З ініціативи СБУ започатковано спільний з Радою Європи проєкт Cybercrime@EAPIII, спрямований на зміцнення співробітництва державних, у т. ч. правоохоронних і спеціальних органів країн – членів Східного партнерства, з приватним ІТ-сектором у сфері протидії кіберзагрозам, а також використання електронних доказів у досудових розслідуваннях. У межах цього проєкту незалежними експертами вже розроблено проект Меморандуму про порозуміння з питань співпраці в боротьбі з кіберзлочинністю та злочинами, під час доведення яких використовуються електронні докази.

Одним з найбільш важливих та перспективних напрямів КДПП є освітній напрям – підготовка кваліфікованих кадрів і поширення серед працівників компаній та пересічних користувачів культури інформаційної та кібернетичної безпеки (запуск загальнонаціональної програми «комп'ютерного лікнепу»).

Відомо, що Україна має значний потенціал у цій сфері. Разом із цим як експерти-освітяни, так і професійна ІТ-спільнота констатують наявність системних проблем у цій сфері: відсутність належного рівня кваліфікації у підготовці сучасних фахівців з питань кібербезпеки та інформаційної безпеки в закладах освіти; низькій рівень зарплати професорсько-викладацького складу в інститутах та фінансування фахівців у державних компаніях; застарілу навчальну програму з підготовки фахівців з питань кібербезпеки та інформаційної безпеки; відсутність координації у системі освіти між замовниками кадрів та закладами освіти; відірваність фахівців з інформаційної та кібербезпеки від міжнародної системи стандартизації; брак наукових досліджень з проблем кібербезпеки [4].

Критично важливим є також забезпечення належного рівня обізнаності персоналу компаній та установ в питаннях кібернетичної та інформаційної безпеки. Форми КДПП тут можуть бути різноманітними: спільні семінари, тренінги, онлайн-курси, залучення науково-аналітичних та консалтингових компаній всіх форм власності і багато іншого.

Важливим є постійний та системний обмін даними щодо актуальних кіберзагроз і можливостей (інструментів) боротьби з ними. Для цього оптимальним було би створення та підтримка на основі широкої КДПП національної системи обміну даними про кіберінциденти та їх реєстр. Це дозволило б підрозділам з ІТ-безпеки компаній та установ перевіряти маркери компрометації, відслідковувати, кому ще розсилалися

аналогічні зразки шкідливого програмного забезпечення, обмінюватися індикаторами атак, убезпечуючи таким чином свої об'єкти від кіберзлочинців.

Кібербезпекове державно-приватне партнерство найдоцільніше організовувати на таких принципах і засадах [4]:

• формування відносин довіри між державними суб'єктами (регуляторами) кібербезпеки і керівництвом приватних підприємств;

• створення умов, за яких приватні об'єкти кіберзахисту добровільно приводитимуть свої програми управління ризиками у відповідність до вимог регулятора (галузевих регуляторів) та надаватимуть всю необхідну інформацію в інтересах захисту критичної інфраструктури;

• постійне врахування галузевої специфіки процесів інформатизації та дотримання кібербезпеки у різних секторах економіки, запровадження інституту галузевих регуляторів;

• основними контактними (координуючими) суб'єктами захисту критичної інфраструктури повинні бути тільки державні установи;

• діяльність державних структур унормована (суворо регламентована) у стосунках з приватним сектором – у розвитку ДПВ належить використовувати інструментарій пільг і привілеїв;

• створення співтовариств для обміну інформацією;

• організація CERT у різних галузях і на різних рівнях;

• розробка та розвиток у рамках ДПВ спільних автоматизованих систем моніторингу кібератак.

Висновки. У нових умовах неминуче повинно змінитися співвідношення прав ІТ-компаній та користувачів. Якщо перші, як і раніше, повинні мати можливість обробляти та аналізувати персональні дані в інтересах розвитку бізнесу, то другі – повинні мати право знати, як, кому і чому передається їх персональна інформація, а також мати можливість виправляти особисту інформацію у разі потреби і навіть запросити її видалення, за винятком випадків, коли існує законна потреба або юридичне зобов'язання у збереженні цих даних. Крім того, з метою забезпечення конфіденційності та кібербезпеки приватних користувачів і комерційних організацій потрібно: створити ефективний наглядовий орган у сфері захисту персональних даних, однак при цьому заходи безпеки та онлайн-обмеження повинні відповідати міжнародним стандартам; не потрібно забороняти використовувати шифрування, оскільки такі обмеження знижують можливості громадян із захисту себе від незаконних втручань у приватність; політика держави у інтернет-сфері має бути спрямована на сприяння розвитку та функціонуванню безпечних інтернет-технологій і формування механізмів захисту від сервісів та протоколів, які ставлять під загрозу технічне функціонування інтернету від вірусів, фішингу тощо.

Важливим є також постійний та системний обмін даними щодо актуальних кіберзагроз і можливостей (інструментів) боротьби з ними. Для цього оптимальним було би створення та підтримка на основі широкої КДПП національної системи обміну даними про кіберінциденти та їх реєстр.

Список використаних джерел

1. Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). Київ: Київ. нац. торг.-екон. ун-т, 2019. URL: https://knute.edu.ua/file/NjY4NQ==/250dafc576ffd3c6a92546eebacc834d.pdf (дата звернення: 02.12.2020).

2. Види шахрайства. URL: https://financer.com/ua/vydy-shahraystva/ (дата звернення: 02.12.2020); Офіційний сайт Мінфіну України. URL: https://minfin.com.ua/ua/2018/07/09/34266317/ (дата звернення: 02.12.2020).

3. Гончаров Д. О. Організація протидії кібершахрайству, що використовує фітингові веб-ресурси. URL: http://ir.nmu.org.ua/bitstream/handle/123456789/154337/%D0%93%D0%BE%D0%BD%D1%87%D0%B0%D1%80%D0%BE%D0%B2.pdf?sequence=1 (дата звернення: 02.12.2020).

4. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. Київ : НІСД, 2018. С.59-64.

5. Заборони та свободи в інтернеті: як виглядатиме Декларація цифрових прав людини. URL: zmina.info/articles/zaboroni_ta_svobodi_v_interneti_jiak_vigljiadatime_deklaracijia_cifrovih_prav_ljiudini/ (дата звернення: 02.12.2020).

6. Кібербезпека бізнесу – це не лише технічні заходи. URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/ (дата звернення: 03.12.2020).

7. Мошенничество с банковскими картамы. URL: https://kltcredit.ua/ua/moshennichestvo-s-bankovskimi-kartami (дата звернення: 02.12.2020).

8. Покупки через інтернет: поради юриста. URL: https://ldn.org.ua/consultations/pokupky-cherez-internet-porady-yurysta/ (дата звернення: 03.12.2020)

9. Фішинг і таргет-фішинг. URL: https://www.imena.ua/blog/phishing-and-target-phishing/ (дата звернення: 02.12.2020).

References

1. Bezpeka sotsialno-ekonomichnykh protsesiv v kiberprostori [Security of socio-economic processes in cyberspace]: materialy Vseukr. nauk.-prakt. konf. (Kyyiv, 27 berez. 2019 r.). Kyyiv: Kyyiv. nats. torh.-ekon. un-t, 2019. URL: https://knute.edu.ua/file/NjY4NQ==/250dafc576ffd3c6a92546eebacc834d.pdf

2. Vydy shakhraystva [Types of fraud]. URL: https://financer.com/ua/vydy-shahraystva/ (data zvernennya: 02.12.2020); Ofitsiynyy sayt Minfinu Ukrayiny. URL: https://minfin.com.ua/ua/2018/07/09/34266317/

3. Honcharov, D. O. Orhanizatsiya protydiyi kibershakhraystvu, shcho vykorystovuye fitynhovi veb-resursy [Anti-cyber fraud organization that uses fitting web resources]. URL: http://ir.nmu.org.ua/bitstream/handle/123456789/154337/%D0%93%D0%BE%D0%BD%D1%87%D0%B0%D1%80%D0%BE%D0%B2.pdf?sequence=1

4. Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyy dosvid ta mozhlyvosti dlya Ukrayiny [Public-private partnership in the field of cybersecurity: international experience and opportunities for Ukraine]: analit. dop. / za zah. red. D. Dubova. Kyyiv: NISD, 2018. S. 59-64.

5. Zaborony ta svobody v interneti: yak vyhlyadatyme Deklaratsiya tsyfrovykh prav lyudyny [Prohibitions and freedoms on the Internet: what the Declaration of Digital Human Rights will look like]. URL: zmina.info/articles/zaboroni_ta_svobodi_v_interneti_jiak_vigljiadatime_deklaracijia_cifrovih_prav_ljiudini/

6. Kiberbezpeka biznesu – tse ne lyshe tekhnichni zakhody [Cybersecurity of business is not just a technical measure]. URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/

7. Moshennichestvo s bankovskimi kartami [Fraud with bank cards]. URL: https://kltcredit.ua/ua/moshennichestvo-s-bankovskimi-kartami

8. Pokupky cherez internet: porady yurysta [Online shopping: legal advice]. URL: https://ldn.org.ua/consultations/pokupky-cherez-internet-porady-yurysta/

9. Fishynh i tarhet-fishynh [Phishing and target phishing]. URL: https://www.imena.ua/blog/phishing-and-target-phishing/

ДАНІ ПРО АВТОРА
Шульга Ольга Антонівна, доктор економічних наук, доцент, доцент кафедри менеджменту і маркетингу, Державний університет інтелектуальних технологій і зв'язку
e-mail: shulga_olga_a@ukr.net
ORCID iD 0000-0002-3230-3124

ДАННЫЕ ОБ АВТОРЕ
Шульга Ольга Антоновна, доктор экономических наук, доцент, доцент кафедры менеджмента и маркетинга, Государственный университет интеллектуальных технологий и связи
e-mail: shulga_olga_a@ukr.net

DATA ABOUT THE AUTHOR
Shulga Olga, Doctor of Economics, Associate Professor, Associate Professor of Management and Marketing, State University of Intelligent Technologies and Communications
e-mail: shulga_olga_a@ukr.net