ДЕМЧЕНКО
Пилип Станіславович
Phildem1945@meta.ua

УДК 342.389

ІНФОРМАЦІЙНО-ЕЛЕКТРОННА БЕЗПЕКА ВИБОРЧОГО ПРОЦЕСУ: УКРАЇНСЬКІ РЕАЛІЇ ТА ЗАРУБІЖНИЙ ДОСВІД (НА ПРИКЛАДІ ОСТАННІХ ПРЕЗИДЕНТСЬКИХ ВИБОРІВ У США 2016 Р. ТА ФРАНЦІЇ 2017 Р.)

INFORMATION AND ELECTRONIC SECURITY OF THE ELECTORAL PROCESS: UKRAINIAN REALITIES AND FOREIGN EXPERIENCE (BASED ON EXAMPLE OF THE LAST US AND FRENCH ELECTIONS OF PRESIDENTS 2016 AND 2017)

студент, КНУ ім. Т. Шевченко

У статті розглядаються основні положення щодо сутності інформаційно-електронної безпеки виборчого процесу, виявлення її особливостей необхідних для забезпечення безпеки проведення виборів в державі. Наводиться приклади Сполучених Штатів Америки та Франції як держав, які мають сталу концепцію інформаційно-електронної безпеки та досвід останніх президентських виборів. На основі цих теоретико-практичних особливостей пропонується основи щодо встановлення інформаційно-електронної безпеки виборчого процесу в правовій та технічній сферах в Україні.

В статье рассматриваются основные положения о сущности информационно-электронной безопасности избирательного процесса, выявление ее особенностей необходимых для обеспечения безопасности проведения выборов в государстве. Приводятся примеры Соединенных Штатов Америки и Франции как государств, имеющих развитую концепцию информационно-электронной безопасности и опыт последних президентских выборов. На основе этих теоретико-практических особенностей предлагаются основы развития информационно-электронной безопасности избирательного процесса в правовой и технической сферах в Украине.

The main case of this article - the nature of the information and electronic security of the electoral process, identification of the features, thatrequired to ensure safe election. The examples of the United States of America and France as countries, that have developed conception of information and e-security and experience of last elections of Presidents. Based on these theoretical and practical features, article gives ideas for the development of information and electronic security of the electoral process in legal and technical spheres in Ukraine.

Ключові слова: *інформаційно-електронна безпека, кібернетична безпека, виборчий процес, вибори, інформаційна інфраструктура.*

Ключевые слова: *информационно-электронная безопасность, кибернетическая безопасность, избирательный процесс, выборы, информационная инфраструктура*

Keywords: *information and electronic security, cybernetic security, electoral process, elections, information infrastructure*

ВСТУП

Дана робота присвячена визначенню поняттю та сутності інформаційно-електронної безпеки виборчого процесу як засобу забезпечення основних принципів виборчого права та надання можливості реалізації прозорості та справедливості проведення голосування та об'єктивного підрахунку результатів виборів. Представлена коротка характеристика сучасних виборчих інформаційних інфраструктур в Україні, а також досвід США та Франції під час проведення останніх президентських виборів на основі аналізу їхнього законодавства та стратегічних розробок у відповідній сфері.

ПОСТАНОВКА ПИТАННЯ – дослідити важливість інформаційно-електронної безпеки у виборчому процесі, надати оцінку з точки зору необхідності правового забезпечення реалізації відповідних засад, які націлені на досягнення позитивних результатів у розвитку загальної кібернетичної безпеки України та використання сучасних технологій у виборчому процесі. Під час дослідження використовувалася правова база Сполучених Штатів Америки та Французької Республіки щодо досягнень даних держав у

сфері інформаційно-електронної безпеки під час виборчого процесу, а також аналіз практичних викликів в забезпеченні виборчого процесу.

РЕЗУЛЬТАТИ

Науково-технічний прогрес людства останні 80 років забезпечив утворення різноманітних електронно-обчислювальних систем, пристроїв та приладів, які знайшли своє місце у багатьох сферах людської діяльності та повсякденного життя. Потрібно зазначити, що у сучасному столітті особливу важливість дані вироби отримують через повсякденне використання у державно-владному житті в тому числі у процесі волевиявлення населення через головний інститут прямої демократії – вибори.

Разом з тим необхідно зазначити, що існування відповідних електронно-обчислювальних систем, які використовуються при проведені виборчого процесу (будь-то електронний реєстр виборців, електронна система голосування чи підрахунку голосів тощо) потребує забезпечення належної захисної бази, існування якої обумовлене можливістю неправомірного втручання у виборчий процес та спростування результатів з конкретною метою. Можна зазначити, що втручання у виборчий процес через електронні системи його забезпечення можуть застосовуватися як й політичними опонентами, так і іншими державами у формі кібернетичної зброї для забезпечення реалізації своїх інтересів, шляхом втручання у виборчій процес.

Сама категорія інформаційна безпека буде мати різні підходи до визначення її поняття та функціонального призначення. В нашому випадку, розглядаючи дане явище з точки зору царини права, можна дати наступне твердження, що кібернетична безпека – є сукупністю засобів та підходів, які націлені на безпечне використання правових та інформаційних даних виборчого процесу, а також наявності способів невтручання у виборчий процес через електронно-обрахункові системи чи пристрої та оперативного – усунення наявних перешкод та порушень.

Таким чином, визначившись з розумінням інформаційної безпеки постає інше питання – як саме забезпечити інформаційну безпеку виборчого процесу, та які основні складові має дане явище.

Але перед усім необхідно зазначити, що вибори – одна з форм безпосередньої демократії, яка дає можливість шляхом загального, рівного та прямого, таємного голосування обради серед кандидатів осіб на виборні посади в органи державної влади та місцевого самоврядування.[1 с. 198-199]. В Україні на сьогодні правовою основою виборів всіх видів та типів є: Конституція України (в першу чергу положення статей 5, 69, 71), Закон України «Про вибори Президента України», Закон України «Про вибори народних депутатів до Верховної Ради України», Закон України «Про місцеві вибори», а також ряд підзаконних нормативно – правових актів. Таким чином, як ми бачимо, вибори являють собою багатогранну та складу структуру, яка характеризується складністю виборчого процесу – врегульованого правовими нормами виборчих правовідносин, щодо порядку підготовки та організації виборів, проведення голосування, підрахунку голосів та оприлюднення результатів виборів. Зазначена вище загальна характеристика виборів та виборчого процесу дає розуміння того, що для забезпечення їх ефективного проведення та гарантії дотримання основоположних принципів виборчого права вказує на необхідність наявності розвинутої та врегульованої системи інформаційної безпеки. Розуміння виборчої безпеки у цьому плані буде розумітися як наявність розвинутої державної програми створення та розвинення інформаційної безпеки виборчого процесу з однієї сторони, так і можливість забезпечити інформаційну безпеку з кожного з учасників з іншої сторони.

Так на приклад щодо забезпечення інформаційної безпеки учасників виборчого процесу, на думку Н.Н. Малишевського в структурі виборчого штабу можна визначити два основних елемента які націлені на забезпечення даного роду безпеки – служба безпеки та відповідальні за контрпропаганду [2 с. 25]. Але разом з тим, можна визначити, що дана оцінка не є повною, оскільки являє собою недостатню увагу цілого розуміння інформаційної безпеки. Відповідно до цього, І.А. Вітренко дає наступну критику даної позиції: по-перше в рамках даного розуміння інформаційної безпеки їй виділяється другорядна роль, по-друге розуміння інформаційної безпеки у цьому випадку буде мати реактивний характер, що є малоефективним в умовах динамічності виборчого процесу, по-третє є неефективним розділенням функції забезпечення інформаційної безпеки між такими елементами служби безпеки та служби забезпечення безпеки в інформаційному просторі.[3 с.155]

Власний підхід до розуміння проблематики забезпечення інформаційної безпеки має Г.В. Пушкарьової, через який описується конкурентна середа політичного менеджменту та формуються основні способи зниження негативного впливу конкурентної середи. Серед основних чинників, які визначають суттєву роль інформаційної безпеки у виборчому процесі у такому випадку визначаються забезпечення руху інформації про основні плани кандидатів, захист від зовнішних нападок противників, проведення контрпропагандиських акції [4, с .321-326].

Потрібно зазначити, що покладення завдання забезпечення інформаційно-електронної безпеки виборчого процесу є важливим завданням для будь-якої держави сучасного світу в незалежності від рівня розвитку її електронної інфраструктури чи забезпечення законодавчою базою. Прикладом даного твердження можна привести перші за останні 20 років вибори у М'янмі, які широко освітлювалися ЗМІ, але лише один факт виборчого процесу у даній країні залишився неоголошеним в масовому порядку – за тиждень до виборів М'янма пережила хакерську атаку типу «відмова в обслуговуванні», що призвело до відключення від Інтернету. Як факт, дане втручання до виборчого процесу, дана кібернетична атака ззовні посприяло визнанню більшістю країн світової спільноти фіктивними, а дана атака була однією з найсильніших на той момент [5].

Врешті решт, актуальність для України забезпеченні сталої політики в сфері інформаційної безпеки виборчого процесу грає велику роль, оскільки рок за

роком все більше державних установ використовує електронно-обчислювальні системи та пристрої, які націлені на спрощення та ефективність реалізації владних програм. Серед основних досягнень у сфері виборів потрібно зазначити функціонування Державного реєстру виборців, якій відповідно до Закону України «Про Державний реєстр виборців» від 22.02.2007 р. № 698 – є автоматизованою інформаційно-телекомунікаційною системою, що призначена для зберігання, обробки даних, які містять передбачені цим Законом відомості, та користування ними, створена для забезпечення державного обліку громадян України, які мають право голосу відповідно до статті 70 Конституції України. Відповідно до статті 2 цього Закону, завданнями ДРВ є ведення персоніфікованого обліку виборців та складання списків виборців для проведення виборів Президента України, народних депутатів України, депутатів Верховної Ради Автономної Республіки Крим, місцевих рад, сільських, селищних, міських голів, всеукраїнських та місцевих референдумів [6]. Потрібно зазначити, що даний нормативно-правовий акт набув чинності 1 жовтня 2007 р., у той час як експлуатація самого ДРВ почалася 29 березня 2009 р..

Потрібно зазначити, що з початку свого функціонування дана інформаційно-аналітична система отримала широке визнання, одними з котрих є нагородження у номінації «Найкращій телекомунікаційний проект» в категорії «Проект загальнодержавного рівня. Телекомунікаційна інфраструктура» на міжнародній конференції Cisco Expo-2009, а також відзнака Центральної виборчої комісії компанією «DELL» за створення і розвиток IT-інфраструктури Реєстру [7].

Разом з тим, необхідно вказати, що для постійного та ефективного функціонування, дана система повинна постійно розвивати системи кібернетичного захисту бази даних та вироблення заходів щодо усунення втручання при зовнішньому втручанню.

Інша сторона забезпечення кібернетичної безпеки пов'язана з питанням впровадження механізму електронних виборів в Україні. Потрібно зазначити, що на сьогодні дана практика існує у таких державах як Велика Британія, США, Канада, Австрія, Естонія. Під проведенням даного типу виборів розуміється використовування різного роду технології електронного голосування та підрахунку голосів.

В перспективі використання електронних виборів в Україні в рамках окремих їх компонентів можливе вже на наступних виборах народних депутатів до Верховної Ради у 2019 р. [8]. Досягненнями даної системи є забезпечення справедливості та чесності проведення виборів із застосуванням електронно-обчислювальних технологій. Разом з тим, перспектива введення даного типу виборів може заощадити державі понад 740 млн. грн., які зараз ідуть лише на зарплату за підрахунок виборів протягом 10 днів [9]. Але, як і ситуація з Державним реєстром виборців, проведення електронних виборів в Україні потребує наявності ефективних систем кібернетичної безпеки, яка забезпечить усунення можливості втручання до бази даних результатів голосування та забезпечить усунення махінацій щодо розподілу голосів між кандидатами.

Але враховуючи вітчизняні реалії, потрібно зазначити, що Україні необхідно орієнтуватися на досвід розвинутих держав. Цікаві практичні надбання можна прослідити у проведенні виборчого процесу у Сполучених Штатах Америки та Франції на основі проведення президентських кампаній 2016 та 2017 рр. відповідно. Слід зазначити, що данні держави мають високий технічний потенціал щодо контролю інформаційно-електронної безпеки виборів, а також широку нормативно-правову базу в сфері виборчого законодавства, яка встановлює положення щодо забезпечення безпеки виборів та основи відповідних процесів.

Розглядаючи досвід Сполучених Штатів у забезпеченні інформаційно-електронної безпеки виборчого процесу необхідно первинно зазначити, що американська конституція встановлює відповідальність за проведення виборів на уряди штатів. Такий підхід означає утворення всередині федеративної держави великої кількості виборчих процесів на рівні штату чи конкретної місцевості, що на думку Д. Фідлера не може не створити проблеми для кібернетичної атаки під час виборів [10]. Важливою віхою виборчого права у США було прийняття рішення Конгресом про фінансування з коштів федерального бюджету введення електронних машин для голосування відповідного технічного стандарту, що в свою чергу зробило необхідність вироблення політики забезпечення комп'ютерної, інформаційної та мережної безпеки для виборчої діяльності. Підставою такого рішення стало необхідність забезпечення уніфікованих технікних пристроїв для голосування на всій території держави після гучного скандалу та наступному розгляду у Верховному Суді США щодо підрахунку голосів виборців у штаті Флорида під час президентських виборів 2000 р., як результат складності формулювання перфокарти бюлетеню – «метелика» таким чином, що прихильники кандидата від демократичної партії Альберта Гора могли проголосувати за його опонента – кандидата від республіканської партії Джорджа Буша мл. [11].

Слід зазначити, що федеральною комісією по сприянню виборів (EAC) були вироблені добровільні керівні положення щодо голосування від 2005 р., які містили вказівки щодо забезпечення виборчого процесу відповідним програмним «софтом», телекомунікаціями та засобами безпровідного зв'язку [10]. Але в 2014 р. президентська комісія з виборів зазначила про непогодженість у вироблені даної концепції. В першу чергу зазначалася криза взаємодії між IT-спеціалістами та посадових осіб, відповідальних за захист технологій голосування виборчого процесу [10].

Потрібно зазначити, що до недавнього часу політика інформаційно-електронної безпеки виборчого процесу мало була досліджена у США. І хоча ще до початку виборчих перегонів 2016 р. було відомо про імовірність впливу на виборчу інфраструктуру виборчого процесу шляхом кібернетичних атак, врешті решт американським урядом на розгляд відповідне питання почало активно виноситися лише

з січня 2017 р.. Крім того, необхідно зазначити, що не було виявлено серйозних успіхів у досліджені електоральної кібербезпеки в рамках загальної інформаційної безпеки.

Якщо ж ми будемо аналізувати виконавчі органи державної влади США, яки покликані забезпечити безпеку виборчого процесу, то умовно їх можна розподілити на три рівні:

1) Федеральний рівень який складається з Агенства Національної Безпеки при Міністерстві Оборони США, основною метою котрого є забезпечення кібернетичної безпеки в інформаційній сфері; Національне управління кібербезпеки США при Міністерстві Внутрішніх Справ на який і покладена левова частка функцій із захисту виборчого процесу; Національна сумісна група з розслідувані кібернетичної безпеки, яка входить до складу ФБР, яке в свою чергу підзвітне Міністерству Юстиції) та забезпечує розслідування втручання у кібернетичний простір всередині держави.

2) Другий рівень представляє собою наявність шести центрів, які є підзвітними одному з трьох вище зазначених міністерств, а саме :комп'ютерна команда швидкої готовності, Національна об'єднана група з розслідувань кіберзлочинів, Центр захисту від кіберзлочинів, Національний оперативний центр з інформаційних загроз, Кіберкомандування Збройних Сил США, Розвідувальне управління – центр реагування на інциденти.

3) Невеликі локальні та регіональні структури, що здійснюють забезпечення кібернетичної безпеки виборчого процесу на рівні штату [12].

Слід зазначити, що для виконання покладених завдань відповідні установи отримають великі кошти з федерального бюджету США кожний рік. Наприклад, АНБ, у складі котрого працює близько 120 тис. осіб, має бюджет 3,5–13 млрд. доларів. Міністерство внутрішньої безпеки має штат приблизно 225 тис. осіб та бюджет в 52 млрд. доларів. У свою чергу, Національне управління кібернетичної безпеки США, має бюджет у 400 млн. доларів на рік [12].

Дані показники правового розвитку та технічно – матеріального забезпечення вказують на високий рівень інформаційно-електронної безпеки з урахуванням новаторства науково-технічного прогресу у цій державі та можливість швидко вирішувати нові проблеми щодо регулювання інформаційної безпеки як на загальному рівні, так і в контексті виборчого процесу.

Але навіть і даний підхід не зміг забезпечити стабільність виборчого процесу 2016 р., в результаті котрих ми знаємо про велику кількість скандалів пов'язаних з розкриттям електронної бази даних основних учасників виборчих перегонів минулого року – Дональда Трампа (кандидат від республіканської партії) та Гілларі Клінтон (кандидат від демократичної партії), а також фіксування неймовірно великої кількості хакерських атак на Північноамериканський континент у день проведення голосування, що могло вплинути на результати виборів.

Одним з прикладів можна назвати хакерську атаку на штаб демократичної партії США у липні 2016 р., якій протягом місяця зазнав втручання до серверів від кіберзлочинців, результатом котрого стали три взломи бази даних партії, а також розголошення електронної переписки між демократами, даних щодо виборів до Конгресу, а також отримання доступу до програм обробки даних після атаки на сервер Національного комітету демократичної партії [13]. Через місяць подібних атак зазнав штаб республіканця – Трампа, але в силу захищеності як державними службами, так і приватними компаніями, основної мети дана атака не досягла, хоча певним чином вказується, що основне завдання було створити збій у електронній системі республіканців [14]. Крім того , останніми даними розслідувань, вказується про атаки на 39 штатів російськими хакерами у день голосування. Основною метою даної атаки було взламування програмного забезпечення виборчого процесу, а також отримати доступ до бази даних списків виборців [15]. Дані події вказують на той факт, що в Сполучених Штатах одразу після завершення після завершення виборчих перегонів 2016 р. почалася розробка нових методів та стратегічних підходів щодо захисту національної кібернетичної безпеки в сфері електронних технологій. Разом з тим, стає очевидним, що можливість впливу на виборчий процес шляхом інформаційних технологій у веденні нового типу кібернетичного протистояння.

Розглядаючи французький досвід інформаційно-електронної безпеки виборчого процесу потрібно зазначити, що за часів початку президентства Н. Саркозі у 2008 р. була видана третя Біла книга (документ, який визначає основні пріоритетні напрямки національної політики та безпеки Франції). Серед основних положень оборони та безпеки непалу увагу відводилося на інформаційну безпеку та розвитку нового виду кібернетичних війн. Саме за даними положеннями подалі у Франції почали вироблятися основні напрямки кібернетичної безпеки держави та створення відповідних стратегій захисту [16].

Відповідна програма мала чотири стратегічні мети: зробити Францію передовою державою світу в сфері кібернетичної безпеки, захистити суверенітет Франції в інформаційному полі, закріплення кібербезпеки основною національною інфраструктурою, забезпечення безпеки у інформаційному полі. Відповідні цілі повинні бути досягнуті через наступні області дії французького уряду: аналізу інформаційних процесів та прогнозування результатів; виявлення, запобігання та протидія негативних чинників; посилення та збереження наукових, технологічних, індустріальних та людських можливостей; прийняття французьким парламентом відповідних законів та інших нормативно-правових актів; захист інформаційної інфраструктури та вміння їй ефективно управляти, розвивати міжнародні зв'язки; розповсюджувати знання та політику щодо об'єктів кібербезпеки.

Для рішення відповідних амбіційних проектів, було перетворено Центральний відділ безпеки інформаційних систем на Національне агентство безпеки інформаційних систем у 2009 р., як основного органу

державної влади в сфері забезпечення інформаційної безпеки.

Національне агентство безпеки інформаційних систем керується Генеральним секретарем Національної Оборони який є підзвітний Прем'єру-Міністру Франції. Утворення даного агентства пов'язане з необхідність діяльності щодо захисту основних інформаційних інфраструктур у Франції. Основними завданнями даного органу є:

1) Оперативне реагування на кібератаки на основні інфраструктури органів державної влади та місцевого самоврядування.

2) Запобігти можливість використання новітніх електронних технологій та технічних пристроїв у створенні інформаційних загроз.

3) Вести політику, щодо усунення недоліків основних інфраструктур

4) Тримати суспільство інформованих щодо можливих кібернетичних загроз та проведення необхідних заходів інформаційної безпеки [17].

Однак не дивлячись на досягнення в сфері політики інформаційно-електронної системи, врешті решт у Франції під час президентських виборів 2017 р. мали місце певні широкі заходи щодо обмеження використання сучасних інформаційних технологій, а саме в сфері застосування електронного голосування, яке використовується для проведення виборів у французьких заморських територіях. Дане рішення, як каже державний секретар по зовнішній торгівлі, розвитку туризму та справам французів у зарубіжжі Маттіас Фекл, пов'язане з рекомендацією експертів Національного агенства з безпеки інформаційних систем щодо можливого надвисокого рівня кібератак, котрі можуть вплинути на результати волевиявлення громадян [18].

Але в тім порушення кіберпростору виборчого процесу Франції під час виборчих перегонів за пост президента не вдалося. Єдиною жертвою хакерських атак став штаб кандидата в президенти від руху «Вперед!» Е. Макрона. Протягом з січня 2017 р. сервери його сили зазнали п'яти потужних хакерських атак, що вказує на виборність кіберзлочинців у організації плану дії щодо конкретного об'єкту та завдань [19]. Одним з результатів даного зовнішнього впливу можна назвати отримання доступу до 9 гігабайтів переписки членів партії та учасників передвиборчої кампанії Макрона. Дану інформацію зловмисники розмістили на сайті pastebin.com в п'ятницю ввечері, коли завершився термін дії кампанії та передвиборчої агітації. Протидію яку можно було визначити у той момент, було звернення представників виборчої комісії Франції до національних ЗМІ не публікувати відповідні дані до завершення виборів. Врешті решт дані події не завадили Е.Макрону стати наступним президентом 5-ї Французької Республіки.

ВИСНОВКИ

Таким чином на основі американського та французького досвіду інформаційно-електронної безпеки можна визначити основні пріоритети для українських реалій захисту інформаційної сфери виборчого процесу. Необхідними кроками, котрі повинні забезпечити безпеку та правомірність виборчого процесу, а також можливість застосовувати новітні провідні технічні засоби та електронні системи повинні бути:

1) Розробка та прийняття нормативно-правових актів, перш за все Закону про інформаційно-електронну безпеку в Україні для забезпечення правового регулювання безпеки в інформаційній сфері. Також необхідне прийняття відповідних законодавчих змін до існуючого виборчого законодавства щодо інформаційно-електронної безпеки та застосування новітніх електронно-технічних засобів та систем.

2) Визначити основні органи державної влади, які будуть відповідальні за реалізацію відповідну концепцію та стратегію інформаційно-електронної безпеки виборчого процесу. Визначення місця та ролі ЦВК України, окружних та дільничних виборчих комісій щодо прав та обов'язків у сфері реалізації інформаційно-електронної системи.

3) Забезпечити інформування з громадянами про їх статус виборця та правил користування електронно-технічними засобами та системами під час виборчого процесу.

4) Створити освітні та професійні умови для забезпечення кадрів державних органів, які будуть займатися підтриманням інформаційно-електронної безпеки кібернетичного простору в цілому так і виборчого процесу в Україні.

Список використаних джерел

1. Конституційне право України. Повний курс: навч. посіб/ О.В. Совгиря, Н.Г. Шукліна. – 2-е видання, перероб. і доп. – Київ.: Юринком Інтер, 2012 р. – 544 с.

2. Малышевский Н.Н. «Технология и организация выборов». – Минск. Издательство «Харвест», 2003 г., – 256 с.

3. Ветренко И.А. Место и роль информационной безопасности в избирательных кампаниях. Ученые записки СКАГС, 2015 год. – № 3, – с.154 -157

4. Пушкарева Г.В. Политический менеджмент. Москва. Издательство «Дело» 2002 г., 400 с.

5. Кибервойны XXI века: самые громкие случаи применения кибернетического оружия [Електронний ресурс]. – Режим доступу: https://www.kommersant.ru/doc/2729773

6. Закон України «Про Державний реєстр виборців» Верховна Рада України; Закон від 22.02.2007 № 698-V [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/698-16

7. Шаміна Л.В. Сучасний стан і перспективи розвитку адміністративно – правового забезпечення реалізації конституційних виборчих прав громадян України [Електронний ресурс]. – Режим доступу:http://applaw.knu.ua/index.php/arkhiv-nomeriv/1-7-2014/item/248-suchasnyy-stan-i-perspektyvy-rozvytku-administratyvno-pravovoho-zabezpechennya-realizatsiyi-konstytutsiynykh-vyborchykh-prav-hromadyan-ukrayiny-shamina-l-v

8. Віктор Жора «Чи бути електронним виборам» [Електронний ресурс] - Режим доступу: http://infosafe.ua/article-4

9. «Чи будуть в Україні електронні вибори» СОЦПОРТАЛ від 05.11.2015 [Електронний ресурс] – Режим доступу: http://socportal.info/2015/11/05/chi-budut-v-ukrayini-elektronni-vibori.html

10. David P. Fidle. Cyber Brief «Transforming Election Cybersecurity» may 2017 [Електронний ресурс] - Режим доступу: https://www.cfr.org/sites/default/files/report_pdf/CyberBrief_Fidler_Elections_OR_2.pdf

11. Американские гонки:машина для голосования [Електронний ресурс] – Режим доступу: http://usa.lenta.ru/ref/machine/

12. Мировые кибервойска: США, КНР, РФ, Украина / Antivirus.UA [Електронний ресурс]. – Режим доступу: http://antivirus.ua/content/mirovye-kibervojska-ssha-knr-rf-ukraina

13. Штаб Клинтон подтвердил хакерскую атаку на свою сеть EurAsiaDaily [Електронний ресурс]. – Режим доступу: http://eadaily.com:8080/ru/news/2016/07/30/shtab-klinton-podtverdil-hakerskuyu-ataku-na-svoyu-set

14. Хакеры взломали компьютерные сети предвыборного штаба Трампа и других республиканцев Newsru.com [Електронний ресурс]. - Режим доступу http://www.newsru.com/world/19aug2016/hack.html

15. Атаки российских хакеров во время выборов в США затронули 39 штатов LB.Ua [Електронний ресурс]. – Режим доступу: https://lb.ua/world/2017/06/13/368948_ataki_rossiyskih_hakerov_vremya.html

16. Во Франции будет разработана новая концепция обороны и безопасности страны [Електронний ресурс]. – Режим доступу: http://www.rodon.org/polit-070824122439

17. The French Network and Information Security Agency. Press Release 2009 [Електронний ресурс] - Режим доступу: https://www.ssi.gouv.fr/uploads/IMG/pdf/ANSSI_PRESS_RELEASE.pdf

18. Из-за кибератак Франция отказалась от электронного голосования на выборах Голос.UA [Електронний ресурс]. – Режим доступу: http://ru.golos.ua/politika/izza_kiberatak_frantsiya_otkazalas_ot_elektronnogo_golosovaniya_na_vyiborah_9247

19. Хакеры выложили в сеть 9 Гб переписки штаба Макрона Gordon.com [Електронний ресурс]. – Режим доступу: http://gordonua.com/news/worldnews/hakery-vylozhili-v-set-9-gb-perepiski-shtaba-makrona-186831.html