МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ
ІІ Всеукраїнської науково-практичної конференції

20 листопада 2020 року

Видавничий дім
«Гельветика»
2020

УДК 004.056(063)
К38

Відповідальний редактор – Дикий Олег Вікторович, декан факультету кібербезпеки та інформаційних технологій, к. ю. н., доцент.

Укладачі:
Логінова Наталія Іванівна – завідувач кафедри інформаційних технологій, к. пед. н, доцент;
Бойко Віктор Дмитрович – доцент кафедри кібербезпеки, к. т. н.;
Флюнт Мар'яна Орестівна – аспірантка кафедри кримінології та кримінально-виконавчого права

К38 **Кібербезпека** в сучасному світі : матеріали ІІ Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. – Одеса : Видавничий дім «Гельветика», 2020. – 244 с.

ISBN 978-966-992-297-7

У збірнику містяться матеріали доповідей, присвячених актуальним проблемам кібербезпеки в сучасному світі, що змінюється.

Подані матеріали відповідають сучасним тенденціям розвитку кібербезпеки в Україні та можуть бути корисними як у навчальному процесі, так і при проведенні наукових досліджень студентами та молодими вченими, а також для практичних працівників у зазначеній сфері.

УДК 004.056(063)

ISBN 978-966-992-297-7

ПЕРЕДМОВА

Шановні учасники ІІ Всеукраїнської науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики»!

Щиро вітаю Вас на відкритті чергового заходу науково-технічної спрямованості, що проводиться Національним університетом «Одеська юридична академія». Головною метою проведення конференцій в університеті завжди було об'єднання талановитих науковців, ідей і досвіду задля вирішення актуальних теоретичних та практичних проблем, а також консолідація зусиль для подальших наукових досліджень.

Одними з найпріоритетніших напрямів діяльності університету завжди був та залишається розвиток творчого потенціалу і всебічна підтримка молодих вчених. Саме проведення наукових конференцій надає можливість студентам, аспірантам та науковцям вільно висловлювати свої думки та ідеї щодо питань забезпечення кібербезпеки, запропонувати практичні напрацювання та поділитися результатами своїх досліджень. Учасники конференції проявили значну зацікавленість у дослідженні технічних питань функціонування інформаційних систем, економічної безпеки в системі національної безпеки, інституційно-правових механізмів забезпечення інформаційної безпеки та соціально-політичних умов формування кіберпростору. Особливу увагу було приділено тематиці формування культури інформаційної безпеки у сучасному суспільстві, яка зараз є пріоритетною у формуванні та реалізації державної політики України. Глибокий інтерес у майбутніх фахівців із кібербезпеки виник також до питань протидії кібербулінгу, фішингу та іншим негативним явищам в кіберпросторі, адже це є одним з пріоритетних напрямів роботи державних інституцій та однією з найбільших проблем використання кіберсередовища.

Загалом сфера інформаційної безпеки та інформаційних технологій сьогодні є найбільш перспективною. У зв'язку з цим з перших днів існування факультету кібербезпеки та інформаційних технологій керівництво прагнуло, насамперед, створити сучасний та студентоцентрований центр підготовки фахівців в сфері ІТ технологій, який був би конкурентоспроможним в Україні та за її межами. Для цього застосовуються сучасні технології в організації навчального процесу, використовується позитивний інноваційний досвід провідних зарубіжних закладів вищої освіти, модернізується матеріально-технічна база. Зараз вчені факультету кібербезпеки та інформаційних технологій продовжують традиції одеської школи, успішно розвивають і примножують наукові досягнення своїх попередників. На факультеті кібербезпеки та інформаційних технологій створені найкращі умови для підготовки кваліфікованих фахівців з кібербезпеки та інформаційних технологій. Саме тому проведення таких наукових заходів вже стало традиційним. Багато робіт учасників конференції підготовлено іноземними мовами, що дозволяє інтегрувати надбання української науки до світового середовища.

Хочу щиро подякувати кожному учаснику всеукраїнської науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» за Ваш внесок до сучасної науки та побажати успіхів у подальших дослідженнях на науковій діяльності!

СЕРГІЙ КІВАЛОВ,
президент Національного університету
«Одеська юридична академія»,
доктор юридичних наук, професор,
академік НАПрН України,
заслужений юрист України

РОЗДІЛ 1.
ІНСТИТУЦІЙНІ ТА ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Dykyi Oleh Viktorovich
National University «Odessa Law Academy»,
Dean of the Faculty of Cybersecurity and Information Technologies,
PhD in Law, docent

MECHANISM OF COUNTERACTION TO CYBERCRIME: CRIMINOLOGICAL ASPECTS

The twentieth century has become an era of new challenges, associated with the rapid development of science and technology, the emergence of new technologies. However, at the same time, socially-negative phenomena began to appear as positive practices, and cyber-security became one of them. Without going into the history of the emergence of cybercrime, it is worth noting that countering this phenomenon is extremely difficult through the constant emergence and development of existing technologies. In fact, law enforcement agencies are limited by law and technology, and criminals are deprived of such restrictions. In this regard, countering cybercrime is reduced to the investigation and suppression of criminal activity, in exceptional cases it is aimed at its prevention.

Given the current trends of cybercrime in the world, the UN General Assembly, in a resolution of 12/17/2018, expressed concern about the increase in cybercrime and the introduction of information and telecommunication technologies in the commission of many types of crimes. In this regard, recommended the Member States to intensify their efforts in the fight against cybercrime and the criminal use of information and communication technologies in all its forms and to develop international cooperation in this area, including the exchange of electronic evidence [1].

Usually, for effective counteraction to crime, including cybercrime, the means and methods that are developed on the basis of modern scientific achievements are key. We believe that it is precisely criminological science that has such potential, since the subject of research includes crime itself and its determination, the personality of the criminal. On the basis of these components, it can develop effective means and methods of combating crime. It is criminological science that has the methodological apparatus that allows us to consider the problem of combating cybercrime in a comprehensive manner and propose ways to improve such activity. Now cybercriminology is at the stage of its formation – as a separate area of criminological science.

It is worth noting that the scientific support of countering cybercrime, both in domestic and world science, is underdeveloped, despite numerous studies by scientists. There may be many reasons for this, for example, the lack of clear boundaries of the research subject, outdated methods of collecting and analyzing empirical material, ignoring the results of research in related industries, including technical, and the like. In this regard, the nature of cybercrime is distorted, simplified to computer crimes or in the field of information technology. Moreover, the lack of deep criminological research on cyber-media creates real problems in the practice of countering this type of crime in the context of international cooperation. Thus, in the report on the work of the twenty-fifth session of the Commission on Crime Prevention and Criminal Justice of the UN Economic and Social Council for 2016, the importance of having adequate national legislation and enhancing international cooperation in the fight against cybercrime was emphasized. Also, there were different opinions on the best approach to fighting cybercrime at the international level [2]. For example, participants drew attention to the need to develop a new comprehensive international legal instrument on cybercrime, which would focus on, inter alia, procedural issues. Despite the fact that this issue is still unresolved, the main international document is the Convention on Cybercrime of

the Council of Europe, which was adopted in 2001. This indicates the absence of a unified approach to combating cybercrime, despite the formal definition of the mechanism for combating this type of crime and its components. Therefore, it is fundamental to determine the effectiveness of this mechanism in dynamics, in order to find the best practices in countering cybercrime.

List of sources used

1. Укрепление программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, в особенности ее потенциала в сфере технического сотрудничества. Принята резолюцией 73/186 Генеральной Ассамблеи ООН от 17 декабря 2018 года. *Организация Объединенных Наций : офіційний веб-сайт.* URL: https://undocs.org/pdf?symbol=ru/A/RES/73/186

2. Доклад о работе двадцать пятой сессии (11 декабря 2015 года и 23-27 мая 2016 года) Комиссии по предупреждению преступности и уголовному правосудию Экономического и Социального Совета ООН. *Организация Объединенных Наций : офіційний веб-сайт.* URL: https://undocs.org/pdf?symbol=ru/E/2016/30

Key words: cybercrime, mechanism, counteraction
Ключевые слова: киберпреступность, механизм, противодействие
Ключові слова: кіберзлочинність, механізм, протидія

Бердиченко Ірина Олегівна
Чорноморський національний університет імені Петра Могили,
кандидат юридичних наук, викладач
Міністерство внутрішніх справ України, заступник начальника
управління Департаменту інформатизації

ЗАКОНОДАВЧІ НОВАЦІЇ В СФЕРІ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ, ШЛЯХИ ПОДАЛЬШОГО УДОСКОНАЛЕННЯ

Закон України «Про основні засади забезпечення кібербезпеки України» [1] передбачає розроблення та застосування якісно нового законодавства у сфері кібербезпеки, що засноване на усвідомленні тенденцій до значного зростання кількості та розширення діапазону кібератак з метою порушення конфіденційності, цілісності і доступності інформаційних ресурсів, штатного режиму функціонування інформаційно-телекомунікаційних систем, перш за все тих, що циркулюють на критично важливих об'єктах інфраструктури нашої країни. Зокрема, цим Законом ще у 2017 році було визначено необхідність розроблення порядку формування переліку об'єктів критичної інформаційної інфраструктури, переліку таких об'єктів та порядок їх внесення до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядку формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури, які повинні бути затверджені Кабінетом Міністрів України. Наслідком цих дій повинен стати комплексний аналіз сектору безпеки і оборони, і його важливою складовою має стати огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, що обробляється в них.

9 жовтня 2020 року Урядом прийнято постанову № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» [2], якою упорядковано ряд з вищеозначених питань. Так, відповідно до абзацу першого частини третьої статті 4

Закону України «Про основні засади забезпечення кібербезпеки України» Кабінет Міністрів України затвердив: Порядок формування переліку об'єктів критичної інформаційної інфраструктури та Порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування.

Вказані рішення Уряду є важливим кроком в реалізації Закону України «Про основні засади забезпечення кібербезпеки України» зважаючи на актуальність нормативно-правового врегулювання питань кіберзахисту критичної інформаційної інфраструктури, разом з тим необхідно зазначити і про низку проблемних питань, які наразі залишаються невирішеними. Мова йде про необхідність прийняття на державному рівні, профільного закону, яким би були комплексно врегульованні питання захисту критичної інформаційної інфраструктури. Відповідні спроби нормативного врегулювання цих питань вже були, але наразі залишаються без вирішення. Необхідно зазначити, що завдання щодо розробки проекту Закону України «Про критичну інфраструктуру та її захист» визначено в Рішенні Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», введеному в дію Указом Президента України від 16 січня 2017 року № 8 [3].

Розпорядженням Кабінету Міністрів України від 06 грудня 2017 року № 1009-р «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» [4] на Міністерство економічного розвитку і торгівлі України разом із заінтересованими центральними органами виконавчої влади, іншими державними органами і установами покладено завдання щодо розробки Закону України «Про критичну інфраструктуру та її захист» (далі – проект Закону).

У травні 2019 року проект Закону, яким, зокрема, пропонувалося визначення основних засад державної політики у сфері захисту критичної інфраструктури, урегулювання правових і

господарських відносин, що виникають під час такої діяльності, повноважень державних органів та інше, подано Кабінетом Міністрів України на розгляд Верховної Ради України (реєстраційний номер 10328) [5], але у зв'язку з припиненням її повноважень проект Закону було знято з розгляду.

Отже, з прийняттям постанови Кабінету Міністрів України від 09 жовтня 2020 року № 943 забезпечено нормативно-правове врегулювання ряду важливих питань у сфері захисту об'єктів критичної інформаційної інфраструктури і це дійсно важливий крок у напрямку подальшого розвитку правового забезпечення кіберзахисту. Адміністрації Державної служби спеціального зв'язку та захисту інформації доручено:

- сформувати перелік об'єктів критичної інформаційної інфраструктури та внести в установленому порядку Кабінетові Міністрів України;
- створити державний реєстр об'єктів критичної інформаційної інфраструктури та забезпечити його функціонування;
- встановити форму подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури.

Міністерствам та іншим органам виконавчої влади доручено сформувати секторальні переліки об'єктів критичної інформаційної інфраструктури, що належать до сфери їх управління, забезпечити їх ведення та надання Адміністрації Державної служби спеціального зв'язку та захисту інформації відомостей про об'єкти критичної інформаційної інфраструктури.

Необхідно нагадати, що це не перше рішення у напрямку правового врегулювання питань захисту об'єктів критичної інформаційної інфраструктури. Для прикладу можна згадати Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, затвердженого постановою Кабінету Міністрів України від 3 серпня 2005 року № 688 [6]. Зазначений реєстр створений і функціонує в Держспецзв'язку. Адміністрацією Держспецзв'язку видано наказ від 24.04.2007

№ 72 [7], який зареєстровано в Міністерстві юстиції України 14 травня 2007 року за № 500/13767, «Про затвердження Порядку формування й користування інформаційним фондом Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління».

Розділом 5 згаданого порядку встановлюються Правила користування Інформаційним фондом Реєстру. Пунктом 5.1. визначено, що дані Інформаційного фонду використовуються Державною службою спеціального зв'язку та захисту інформації України для:

- проведення аналізу стану захисту державних електронних інформаційних ресурсів в ІТС;
- підготовки аналітичних матеріалів Кабінетові Міністрів України щодо стану захисту державних електронних інформаційних ресурсів ІТС органів виконавчої влади;
- надання методичної допомоги і координації діяльності міністерств та інших центральних органів виконавчої влади, пов'язаної із захистом державних електронних інформаційних ресурсів в ІТС (пункт 5.1).

У той же час відповідно до пункту 5.2 допуск до відомостей Інформаційного фонду, надання відомостей Інформаційного фонду в повному обсязі або передача його копій (як у повному обсязі, так і частково) іншому суб'єкту заборонені, крім випадків, передбачених законодавством. А згідно із пунктом 5.3 відомості з Інформаційного фонду можуть бути надані органу, що їх надав, на підставі мотивованого запиту. Отже ми бачимо, що правові норм встановлено, але їх практична реалізація викликає питання.

Пам’ятаємо, що 23 грудня 2019 року відбулися слухання у Комітеті Верховної Ради України з питань цифрової трансформації з порядком денним: «Національна кібербезпека та кіберзахист України, у тому числі у сфері критичної інфраструктури» [8]. Необхідність проведення комітетських слухань була

викликана тим, що тема кібербезпеки в Україні за останні роки набула значної актуальності. Не тільки Україна, а й увесь світ змінив своє ставлення до зазначеної проблеми, – зросло усвідомлення, що найнебезпечніші кібернетичні та інформаційні загрози виходять не від поодиноких хакерів, а від агресивно-налаштованих країн.

Отже приходимо до висновку, що вимоги сьогодення до кіберзахсту, зокрема критичної інформаційної інфраструктури, свідчать про необхідність запровадження системного підходу до розв'язання проблеми на загальнодержавному рівні у вигляді створення відповідної системи захисту. Тому пріоритетом має стати розробка та подання до Верховної Ради проекту Закону України щодо критичної інформаційної інфраструктури та її захисту, оскільки створення системи захисту критичної інформаційної інфраструктури в Україні має вирішуватись з урахуванням усього існуючого спектра загроз та забезпечення взаємопов'язаності різних систем та органів, необхідності запровадження системного підходу до розв'язання цієї проблеми. Існує необхідність у формуванні нормативно встановленого порядку проведення комплексної оцінки загроз критичній інфраструктурі та загальної методології оцінки ризиків, пов'язаних із функціонуванням критичної інфраструктури, запровадженні єдиних підходів до організації управління об'єктами системи на державному та місцевому рівнях, визначення засад взаємодії залучених до захисту критичної інформаційної інфраструктури державних органів та суб'єктів господарювання, суспільства та громадян.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403). [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2163–19.

2. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури». Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/943–2020-%D0%BF#Text.

3. Указ Президента «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/8/2017#Text.

4. Розпорядження Кабінету Міністрів України від 06 грудня 2017 року № 1009-р «Про схвалення Концепції створення державної системи захисту критичної інфраструктури». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1009–2017-%D1%80#Text.

5. Проєкт Закону України «Про критичну інфраструктуру та її захист». Номер, дата реєстрації: 10328 від 27.05.2019. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/.

6. Постанова Кабінету Міністрів України від 3 серпня 2005 року № 688 «Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління». [Електронний ресурс]. – Режим доступу: https://www.kmu.gov.ua/npas/19617517.

7. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації країн від 24.04.2007 № 72 «Про затвердження Порядку формування й користування інформаційним фондом Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління». [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/z0500–07#Text.

8. Звіт про роботу Комітету з питань цифрової трансформації за другу сесію Верховної Ради України дев'ятого скликання (вересень 2019 – січень 2020 рр.). [Електронний ресурс]. – Режим доступу: https://komit.rada.gov.ua/news/dijaln_komit9skl/zvit_rc9skl/73521.html.

Ключові слова: об'єкти критичної інформаційної інфраструктури, кіберзахист, правове врегулювання.

Ключевые слова: объекты критической информационной инфраструктуры, киберзащита, правовое регулирование.

Keyword: objects of critical information infrastructure, cyber protection, legal regulation.

Чанышев Рашид Ибрагимович
Национальный университет «Одесская юридическая академия»,
доцент кафедры информационных технологий, кандидат
юридических наук, доцент

ЭЛЕКТРОННОЕ РЕЗИДЕНТСТВО В УКРАИНЕ

20 октября 2020 года инициативная группа народных депутатов Украины внесла на рассмотрение Верховной Рады Украины проект Закона Украины «О внесении изменений в Налоговый кодекс Украины и в некоторые другие законодательные акты Украины относительно ведения предпринимательской деятельности э-резидентами в Украине» [1].

Толчком для этого послужило изданное 25 июля 2020 года Кабинетом Министров Украины постановление № 648 «О реализации экспериментального проекта по внедрению и реализации в Украине электронного резидентства». Тем самым в Украине был сделан первый шаг к введению в стране института электронного резидентства.

Согласно указанного законопроекта электронным резидентом Украины может стать любой совершеннолетний гражданин другого государства или лицо без гражданства. Электронный резидент, зарегистрировавшийся как физическое лицо -предприниматель, получает статус электронного резидента – предпринимателя и получает возможность осуществлять предпринимательскую деятельность в Украине, не покидая при этом страны пребывания.

Информационная система «Э- резидент» предназначена для сбора, обработки и предоставления информации о лицах, пожелавших стать электронными резидентами в Украине, и о лицах, уже получивших такой статус.

Информационную систему «Э- резидент» планируется тесно интегрировать с Единым государственным веб-порталом электронных услуг «Портал Дія».

Согласно законопроекту, на первом этапе электронное резидентство будет доступно только для физических лиц –

предпринимателей (ФЛП). В законопроекте указано, что физические лица – предприниматели, получившие регистрацию в качестве электронного резидента, обязаны проводить все расчеты исключительно в безналичной форме. Электронные резиденты должны будут получить преимущество в виде более низких налогов.

Целью и задачей принятия данного законопроекта является привлечение в Украину дополнительных инвестиций и создание благоприятных условий для ведения бизнеса э-резидентами в Украине, что должно привести к увеличению доходов государственного бюджета, путем наполнения его за счет налогов, уплачиваемых э-резидентами [2].

Сама по себе данная идея не нова: с 1 декабря 2014 года в Эстонии была запущена программа электронного резидентства, ориентированная, в первую очередь, на привлечение предпринимателей, не связанных с физическим производством, таких, например, как разработчиков программного обеспечения.

С учетом того, что Эстония является членом Европейского Союза, у предпринимателей, зарегистрированных за его пределами, появляется официальная возможность, через созданные в Эстонии предприятия, вести предпринимательскую деятельность в Европейском Союзе.

Для получения статуса электронного резидентства в Эстонии достаточно получения электронно-цифрового удостоверения личности в виде специальной идентификационной карты (ID-карты). Выданная карта будет действительна на протяжении 5 лет [3].

Оформить карту можно дистанционно на сайте программы эстонского электронного резидентства [4] или непосредственно в бюро обслуживания Департамента полиции и погранохраны Эстонии, а также в любом посольстве или консульстве Эстонской Республики.

Для оформления карты требуется предоставление копии документа, удостоверяющего личность получателя, каковым

могут быть паспорт, удостоверение личности Европейского Союза или копия проездного документа государства гражданской принадлежности (для лиц без гражданства). При оформлении карты взымается пошлина в размере 100 евро. При оформлении карты в посольстве или консульстве пошлина составит 120 евро.

Дополнительным требованием является предоставление файла с актуальной (не более полугода с момента ее создания) цветной фотографией будущего э-резидента (минимальное разрешение которой должно быть не менее чем 1300х1600 пикселей, при этом размер файла не должен превышать 1…5 МБ). Несмотря на это требование, фото получателя карты на самой карте не размещается, а карта не может являться удостоверением личности.

Заявка на получение удостоверения (ID-карты) рассматривается на протяжении 30 дней. Заявка может быть отклонена в случаях, когда указанное лицо может оказаться причастным к зарегистрированным финансовым махинациям или мошенничествам.

Получить удостоверение можно на территории Эстонии или в том посольстве (консульстве) этой страны, в котором была подана заявка. Для получения карты необходимо явиться лично. При выдаче карты у получателя берутся отпечатки пальцев.

При этом выданная карта не дает права иностранцам налогового резидентства, разрешения на въезд в Европейский союз или в Эстонию, как и права на проживание в Эстонии.

Получивший э-резидентство предприниматель может совершать сделки, используя интернет-банки, подавать налоговые декларации в электронной форме и подписывать полученной цифровой подписью документы и договоры.

К 2020 году более 65 000 человек стали электронными резидентами Эстонии, в том числе – 862 гражданина Украины. При этом было создано 10100 компаний [5]. Программа e-Residency принесла Эстонии более 35 миллионов евро прямого дохода.

Однако на разработку, внедрение и поддержку этой программы было потрачено около 10 млн евро (т.е. примерно 30% от полученных средств).

В целом программу e-Residency можно считать вполне успешной. По пути Эстонии пошли и другие страны, в частности, в 2018 году подобная программа была реализована в Азербайджане.

Реализация программы e-Residency в Эстонии стала возможной благодаря разработанной эстонскими компаниями и введенной в эксплуатацию еще в 2001 г. централизованной системы обмена данными «X-Road», позволяющей осуществить обмен информацией через Интернет с обеспечением конфиденциальности и целостности передаваемых данных, используя единый набор пользовательских интерфейсов и систему аутентификации (принцип интероперабельности) [6].

Поскольку данная система за прошедшие годы ни разу не была скомпрометирована (3 октября 2016 года ее исходные коды были лицензированы MIT (Массачусетским технологическим институтом), ее начали использовать и в других странах, таких, как Финляндия, Азербайджан, Кыргызстан, на Фарерских островах, в Исландии, Японии и Намибии.

Система X-Road легла в основу созданной в Украине Министерством цифровой трансформации Украины в сотрудничестве с «Академией электронного управления» и рядом компаний системы электронного взаимодействия государственных электронных информационных ресурсов «Трембита» [7]. В отличие от X-Road – «Трембита» является распределенной системой. Ее использование не предусматривает централизации данных и изменения их владельца.

Система «Трембита» используется Министерством цифровой трансформации Украины для обеспечения работы вышеупомянутого сервиса «Дія», на базе которого и предлагается осуществить систему электронного резидентства в Украине.

Следует отметить, что сама идея введения электронного резидентства в Украине основана на том факте, что в

аналогичной эстонской системе наибольшее число зарегистрировавшихся е-резидентами юридических лиц являются предприятиями из Украины.

Казалось бы, что этот факт свидетельствует о большом стремлении к получению е-резидентства среди наших предпринимателей. Однако надо учитывать тот факт, что Эстония, в отличие от Украины, является членом Европейского Союза. Весьма вероятно, что именно это и делает е-резиденство в Эстонии таким привлекательным.

Кроме того, как было отмечено выше, внедрение данной системы обошлось Эстонии в 10 млн евро, так что внедрение аналогичной системы в Украине, с учетом вышеизложенного, может и не дать ожидаемого экономического эффекта.

Побочным эффектом может стать и практика «отмывания денег» гражданами других стран посредством получения е-резидентства в Украине. При этом децентрализованность системы «Трембита» может сыграть отрицательную роль.

Список использованной литературы:

1. Проект Закону України «Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо ведення підприємницької діяльності е-резидентами в Україні» – URL: https://cutt.ly/OgZaxGc. – Дата звернення: 19.10.2020 р.

2. Пояснювальна записка від 20.10.2020. – URL: https://cutt.ly/0gZsUEh. – Дата звернення: 19.10.2020 р.

3. Э-резидентство (Eesti.ee – единый источник государственной информации и э-услуг) – URL: https://cutt.ly/dgZdgMc. – Дата обращения: 19.10.2020 г.

4. Become an e-resident. – URL: https://cutt.ly/UgZfxf4. – Last accessed: 19.10.2020 y.

5. Электронное резидентство: Как это будет работать в Украине. – URL: https://bitly.su/iweBd8G. – Дата обращения: 19.10.2020 р.

6. X-Road. – URL: https://cutt.ly/RgZgaRf. – Last accessed: 19.10.2020 y.

7. Міністерство та Комітет цифрової трансформації України. Система «Трембіта» – URL: https://bitly.su/pdvX. – Дата звернення: 4.11.2020 р.

Ключові слова: електронне резидентство, ID-карти, процедура оформлення електронного посвідчення, система X-Road, системи «Трембіта» і «Дія».

Ключевые слова: электронное резидентство, ID-карты, процедура оформления электронного удостоверения, система X-Road, системы «Трембита» и «Дія».

Keywords: e-Residency, ID-cards, electronic certificate, the X-Road system, the «Trembita» and «Diya» systems.

Левківська Ярослава Вікторівна
Національний університет «Одеська юридична академія»
аспірантка кафедри кримінології та кримінально-виконавчого права

НАПРЯМИ СУЧАСНИХ ДОСЛІДЖЕНЬ КРИМІНОЛОГІЧНОЇ ХАРАКТЕРИСТИКИ ТА ПОПЕРЕДЖЕННЯ ШАХРАЙСТВА, ЩО ВЧИНЯЄТЬСЯ В МЕРЕЖІ ІНТЕРНЕТ

Практично безмежні можливості глобальної мережі Інтернет у сфері передачі та обробки інформації, що забезпечують комунікацію в різних формах, вчинення фінансових операцій, торгівлі та інше, з одного боку, роблять мережу Інтернет найсприятливішим середовищем для розвитку суспільних відносин, з іншого боку, це тягне за собою виникнення такого негативного явища, як інтернет-злочинність. Міжнародна організація Group-IB, що досліджує стан комп'ютерної злочинності на пострадянському просторі, зазначає, що фінансові збитки світового ринку через комп'ютерні злочини за минулий рік перевищили 7 млрд доларів США, а доходи злочинців із СНД складають 2,5 млрд доларів, тобто «комп'ютерні» злочинці країн СНД контролюють більш ніж третину світового ринку кіберзлочинності [1]. Зареєстрований масив кримінальних правопорушень у аналізованій сфері свідчить про їх суттєве зростання за останні роки і має такі показники: у 2013 році було обліковано 595 кримінальних правопорушення, у 2014 році – 443, у 2015 році – 598, у 2016 році – 865, у 2017 році – 2573, у 2018 році – 2301 [2].

Водночас з усієї сукупності кримінальних правопорушень, що вчиняються з використанням мережі Інтернет, частка шахрайств становить 58% [3, с. 3]. Такий високий відсоток зумовлений розвитком технологій у сфері комп'ютеризації та постійним розширенням сфери застосування комп'ютерної техніки. Поряд з цим, проблема поширення шахрайства в мережі Інтернет особливо актуалізується сьогодні, адже багато сфер в умовах карантину перейшли в онлайн. Тому успішність запобігання таким кримінальним правопорушенням, їх викриття та притягнення винних осіб до відповідальності наразі є дуже важливим, як для кожної людини так і для держави в цілому.

Проведенням наукових досліджень окремих аспектів кримінологічної характеристики та попередження шахрайства, що вчиняється в мережі Інтернет займаються такі вчені, як Д. С. Азаров, Ю. М. Батурин, П. Д. Біленчук, А. С. Білоусов, І. Г. Богатирьов, В. М. Бутузов, А. Г. Волевоз, В. Д. Гавловський, О. В. Демешко, Д. О. Зиков, М. В. Карчевський, А. А. Комаров, С. А. Кузьміна, В. Д. Ларичев, А. К. Лебедєв, О. В. Лисодєд,О. В. Мазоліна,К. В. Манжула,В. М. Машкова,С. С. Мірошниченко,А. В. Микитчик,Ю. М. Онищенко,П. І. Орлова,С. О. Орлов, Н. А. Савінова, О. В. Смаглюк, Л. В. Сорока, К. В. Тітуніна, С. С. Чернявський,В. І. Шакун,С. В. Шапочка,В. П. Шеломенцев, О. М. Юрченко та інші.

Слід зауважити, що починаючи з 2000-х років суттєво збільшується кількість досліджень кримінальних правопорушень в сфері ІТ-технологій.

На рівні дисертаційних робіт окремі аспекти зазначеної проблематики вивчалися М. В. Карчевським «Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)» (2003 р.), «Кримінально-правова охорона інформаційної безпеки України» (2013 р.), О. Е. Радутним «Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю» (2002 р.), Н. А. Розенфельд

«Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» (2003 р.), М. В. Плугатир «Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації» (2010 р.), Н. А. Савінова «Кримінально-правова політика забезпечення розвитку інформаційного суспільства в України» (2013 р.), С. В. Шапочки «Запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж» (2018 р.), Ричка Д. О. «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (2019 р.).

В. О. Голубєв у 2003 році опублікував монографію «Інформаційна безпека: проблеми боротьби з кіберзлочинами». У 2005 році вийшов науково-практичний коментар за редакцією А. А. Музики та Д. С. Азарова «Законодавство України про кримінальну відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення», а згодом монографія Д. С. Азаров «Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)» (2007 р.). У 2016 році М. О. Кравцова та О. М. Литвинов випустили монографію «Запобігання кіберзлочинності в Україні». З останніх наукових праць можна виокремити навчально-практичний посібник «Протидія злочинам у сфері використання інформаційних технологій» за редакцією М. В. Карчевського 2019 року.

Водночас при всій значущості цих та інших наукових напрацювань, враховуючи постійних розвиток інформаційних технологій, створення численних інформаційних систем, розробка більш досконалих технічних пристроїв, а також динаміку поширення Інтернет-шахрайства, на сьогодні, назріла необхідність проведення комплексного дослідження кримінологічної характеристики та попередження шахрайства, що вчиняється

в мережі Інтернет. Тому напрямами наших наступних наукових розвідок стануть різні аспекти зазначеної теми.

Список використаних джерел:

1. Основные услуги и тарифы на рынке киберпреступности в странах СНГ. URL: http://www.interface.ru.
2. Єдиний звіт про кримінальні правопорушення по державі: офіційний сайт Генеральної прокуратури України URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402
3. Комаров А. А. Криминологические аспекты мошенничества в глобальной сети Интернет: дис. на соискание ученой степени канд. юрид. наук: спец. 12. 00. 08. Саратов, 2011. 262 с.

Ключові слова: шахрайство, шахрайство в мережі Інтернет, попередження шахрайства.

Ключевые слова: мошенничество, мошенничество в сети Интернет, предупреждение мошенничества.

Keywords: fraud, Internet fraud, fraud prevention.

***Науковий керівник**: к.ю.н., доцент Дикий О. В.*

Флюнт Мар'яна Орестівна

Національний університет «Одеська юридична академія»,
аспірантка кафедри кримінології та кримінально-виконавчого права

КІБЕРЗЛОЧИН ТА КІБЕРЗЛОЧИННІСТЬ У КРИМІНОЛОГІЧНИХ ДОСЛІДЖЕННЯХ: СУЧАСНІ ПІДХОДИ ТА ПРОБЛЕМАТИКА

Формування актуальної кібербезпекової політики та забезпечення ефективності її реалізації, функціонування безпечного кіберпростору, а також попередження та протидія кіберзлочинності є одними з найбільш актуальних завдань та викликів для держав і міжнародної спільноти на сучасному етапі розвитку суспільства. Саме тому дослідження окремих питань забезпечення кібербезпеки є об'єктом дослідження науковців різних сфер.

У кримінології кібербезпека розглядається як взаємодія окремих складових, – державної політики щодо забезпечення

кібербезпеки; суб'єктів забезпечення кібербезпеки; засобів, способів і методів забезпечення кібербезпеки. Однією з ключових загроз кібербезпеці є, зокрема, кіберзлочинність.

Не зважаючи на те, що кіберзлочини та кіберзлочинність є предметом вивчення все більшої кількості сучасних науковців, існують деякі труднощі дослідження даного соціального явища, що, своєю чергою, уповільнює функціонування системи забезпечення кібербезпеки як на національному, так і на міжнародному рівнях, оскільки остання формується на основі теоретичних досліджень. Розгляньмо деякі проблемні моменти.

По-перше, *відсутній єдиний підхід до термінології у правовій доктрині та роботах вітчизняних та закордонних науковців.* Так, у сучасних дослідженнях активно застосовують поняття «комп'ютерні злочини», «кіберзлочини», «віртуальні злочини», «інформаційні злочини», «цифрові злочини», «високотехнологічні злочини», «злочини, пов'язані з використанням мережі Інтернет», «злочини, пов'язані з використанням телекомунікаційних систем», «електронні злочини» тощо. Зазначені терміни по-різному описуються, тлумачаться один через одного, крім того, то розмежовуються, то ототожнюються різними дослідниками.

Неоднаковим є застосування термінології й у чинному законодавстві. Так, Кримінальний кодекс України (далі – КК України) оперує поняттям «кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», жодного разу не згадуючи поняття «кіберзлочин», а Закон України «Про основні засади забезпечення кібербезпеки» застосовує іншу термінологію, – «кіберзлочин» і «комп'ютерний злочин», фактично ототожнюючи зазначені поняття та визначаючи їх як «…суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [1].

Варто зазначити, що термін «кіберзлочин» є найбільш вживаним у побутовому спілкуванні, політиці та публіцистиці, в порівнянні з іншими (суміжними) категоріями. У буденному розумінні, – кіберзлочин це загальне поняття, яке охоплює усі злочини, що вчиняються у мережі інтернет та/або з використанням комп'ютерів та/або сучасних інформаційних комунікаційних технологій. Така неоднозначність у термінології спричиняє плутанину та помилкову взаємопідміну понять, що своїм результатом має отримання помилкових даних, а отже й неревалентність дослідження.

По-друге, *невідповідність чинного законодавства міжнародним стандартам.*

У вересні 2005 року Україною було ратифіковано (із застереженням) Конвенцію Ради Європи про кіберзлочинність (так звану Будапештську конвенцію). Конвенцією сформовано новий міжнародний стандарт – злочин міжнародного характеру – кіберзлочин, що за своєю правовою конструкцією є збірним поняттям, яке включає декілька різнопланових протиправних посягань [2].

Так, у Конвенції перелічено основні види кіберзлочинів, схарактеризовано окремі процесуальні заходи та описано загальні принципи міжнародного співробітництва у сфері протидії кіберзлочинам. Зокрема, Конвенцією передбачено чотири основні групи кіберзлочинів [3]: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, – незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями; правопорушення, пов'язані з комп'ютерами, – підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами; правопорушення, пов'язані зі змістом, – правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських і суміжних прав.

Зазначені у Конвенції кіберзлочини частково передбачені КК України. Так, розділом XVI КК України встановлено відповідальність за кримінальні правопорушення у сфері викорис-

тання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Крім того, для кваліфікації правопорушень, що фактично є кіберзлочинами, з точки зору норм Конвенції, застосовують також статті з інших розділів Особливої частини КК України: ст. 163 – порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, ст. 176 – порушення авторського права і суміжних прав, ст. 190 ч. 3 – шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, ст. 301 – ввезення, виготовлення, збут і розповсюдження порнографічних предметів, ст. 359 – незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації.

Відсутність чіткого визначення у кримінальному законі яке діяння є кіберзлочином; «розпорошеність» у КК України статей, якими встановлено відповідальність за правопорушення, що відповідно до норм Конвенції є кіберзлочинами; невключення ряду правопорушень, що є конвенційними кіберзлочинами до кримінального законодавства України зумовлюють неправильну кваліфікацію та необлікування значної кількості вчинених злочинів. Наслідком зазначеного є латентність, помилковість у статистичних даних, а отже й відсутність оцінки реального стану кіберзлочинності у нашій державі.

Необхідність чіткого нормативного визначення та доповнення кримінального закону нормами, що встановлюють відповідальність за конвенційні злочини зумовлена й тим, що кримінальне право є фундаментальною наукою щодо кримінології (як науки кримінального циклу), а остання, будучи теоретико-прикладною наукою одним зі своїх основних предметів дослідження має злочини. Таким чином, некоректним є йменування у кримінологічних дослідженнях «злочином» діянь, що не є криміналізованими, тобто таких, що не є злочином з точки зору закону про кримінальну відповідальність, адже аналогія у цій галузі не застосовується.

По-третє, *обмеженість кримінологічних досліджень способів вчинення кіберзлочинів.*

Формування державної політики та розробка ефективної системи заходів протидії злочинам передбачає попереднє вивчення способів їх вчинення. У кримінології способам вчинення злочинів приділено недостатньо уваги, – зазвичай спосіб розглядається поверхнево та фрагментарно, а їх опис базується на основі статистичних даних (у розрізі звітності Офісу генерального прокурора України, – Форма № 1). Такими ж поверхневими є переважна більшість наявних робіт щодо способів вчинення кіберзлочинів, – дослідження, здійснені на основі вивчення матеріалів слідчої та судової практики є швидше винятком, а не закономірністю. Таким чином, неналежне вивчення злочинів, вчинених у кіберпросторі, зумовлює існування певних кліше щодо сучасної кіберзлочинності, не дозволяє виявити основні тенденції даного виду злочинності та спрогнозувати її подальший розвиток.

Окрім зазначених, проблематичним у дослідженні кіберзлочинності вважаємо: обмеженість методів вивчення кіберзлочинності; незначне врахування результатів досліджень закордонних фахівців та міжнародних наукових спільнот; застарілість та поверхневість наявних досліджень; мала кількість судової практики щодо кримінальних справ даної категорії (у співвідношенні до кількості зареєстрованих та облікованих злочинів, визначених, зокрема, Розділом XVI КК України).

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05 жовтня 2017. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

2. Гринчак І. В. Кіберзлочинність як злочин міжнародного характеру. URL: http://nbuv.gov.ua/j-pdf/Nivif_2015_12_15.pdf

3. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

Ключові слова: кіберзлочинність, міжнародний стандарт, криміналізація, спосіб вчинення кіберзлочинів, політика кібербезпеки.
Ключевые слова: киберпреступность, международный стандарт, криминализация, способ совершения киберпреступлений, политика кибербезопастности.
Keywords: cybercrime, international standard, criminalization, method of committing cybercrimes, cybersecurity policy.

***Науковий керівник**: к.ю.н., доцент Дикий О. В.*

Керусов Максим Вікторович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТ ПРОВАЙДЕРІВ

Термін інформаційна безпека в сучасному світі надзвичайно широкий. Вон включає в себе як контроль за непоширенням інформації, яка вважається секретною, так і облік своєчасного, повного і якісного інформування громадян про події в країні і світі, вільний доступ до різних джерел інформації – і в той же час просування цілісності суспільства, підтримання його морального благополуччя, захист від різноманітних несприятливих інформаційних впливів.

Актуальність порушення проблеми захисту інформаційної безпеки обумовлюється зростанням доступу до мереж загального користування окремих категорій негативно настроєних осіб, певною уразливістю окремих мереж, збільшенням спроб злочинних елементів на здобування або руйнування інформації, а також збільшення кількості шахраїв які намагаються вкрасти персональні данні.

Політика інформаційної безпеки являє собою набір обмежень, вимог, рекомендацій, правил, які регламентують порядок інформаційної діяльності в організації і направлені на досягнення і підтримку стану інформаційної безпеки в організації.

Також можна сказати що під політикою інформаційної безпеки розуміється набір законів, обмежень, правил і рекомендацій, які регламентують порядок опрацювання інформації і направлені на захист інформації від певних загроз

Причиною появи політики інформаційної безпеки є вимога до такого документа від регулятора – організації, яка визначає правила функціонування підприємств цієї галузі. У цьому випадку відсутність політики інформаційної безпеки може призвести до репресивних дій проти підприємства або навіть до повного припинення його діяльності. Крім того, галузеві або загальні, місцеві чи міжнародні стандарти мають конкретні вимоги або керівні принципи.

Відсутність політики інформаційної безпеки викликає негативну оцінку, що в свою чергу впливає на публічні показники підприємства – позицію в рейтингу, рівень надійності тощо.

На мою думку політику інформаційної безпеки умовно можна розділити на 2 напрямки:

– Законодавче закріплені акти які мають бути застосовані усіма провайдерами. До них можна віднести: указ президента України № 47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Рішення НКРЗІ № 22 від 15.01.2019 Про надання операторам, провайдерам телекомунікацій рекомендації щодо поширення серед користувачів правил безпеки в кіберпросторі, Закон, ВР України, від 18.11.2003, № 1280-IV «Про телекомунікації»

– Розробка провайдером власної політики інформаційної безпеки.

У деяких користувачів може виникнути питання: що може розробляти провайдер якщо основні положення заложенні законодавчими актами (закон про телекомунікації глави VI споживачі телекомунікаційних послуг і VII оператори, провайдери телекомунікацій (саме в них вказані права і обов'язки споживачів і операторів)).

На свій розгляд інтернет провайдери залишають:

– постачання додаткових послуг та їх оплату;

– з метою захисту інтересів абонентів і мережі оператори міжміського (міжнародного) телефонної мережі можуть здійснювати, при наявності необхідного програмного забезпечення і технічних засобів, оперативний контроль використання послуг з кожного телефону (моніторинг);

– в разі різких відхилень (обсяги, види послуг і т.д.) Оператор може вжити заходів для виявлення їх причин (можливе стороннє підключення, неузгоджене використання телефону і т.д.)

У наш час інформаційні технології постійно розвиваються, що призводить до появи нових ризиків та загроз. Однак основними проблемами, що виникають сьогодні в процесі захисту порушених прав, є складність встановлення порушника, складність реалізації заходів реагування, враховуючи екстериторіальний характер Інтернету, а також підтримка балансу між реакціями на порушення та збереження свободи в інформаційному просторі.

Складнощі з встановленням особи злочинця пов'язані з особливостями Інтернету, в якому від більшості користувачів не потрібно повідомляти особисті дані. Регулярно з'являються ініціативи щодо впровадження більш повної ідентифікації, в тому числі у вигляді змін у законодавстві. До них відносяться неодноразові пропозиції зареєструвати веб-сайти, аналогічні традиційним ЗМІ. Однак в більшості випадків такі ініціативи відкидаються через значне громадського спротиву. Їх введення загрожує перетворенням в механізм цензури.

Однак в деяких випадках держава залишає за собою вирішальний голос стосовно користування веб ресурсами як приклад можна навести Указом Президента України від 15,05,2017 року Ш 133/2017 введено у дію рішення РНБО щодо обмеження діяльності в Україні російських соціальних мереж та сервісів. У даному переліку 52 російських сайти, щодо яких вжито санкційні заходи.

Отже можна зробити висновок що хоча політика інформаційної безпеки у інтернет провайдерів може відрізнятися

проте основні пункти в них будуть однакові – ті що вказані в закріплених законодавчих актах.

Список використаних джерел:

1. закон України Про телекомунікації: офіц. веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/1280–15#Text
2. Укртелеком офіц. веб-сайт. URL: https://ukrtelecom.ua/reference/zakhist-personalnikh-danikh/

Ключові слова: політика інформаційної безпеки, інформаційна безпека, інформаційна безпека в інтернеті.

Ключевые слова: политика информационной безопасности, информационная безопасность, информационная безопасность в интернете.

Keywords: information security policy, information security, information security on the Internet.

***Науковий керівник**: д. фіз.-мат. н., професор Василенко М. Д.*

Малюта Владислав Васильович
Національний університет «Одеська юридична академія»,
студент 3-го курсу факультету кібербезпеки
та інформаційних технологій

СМАРТ-КОНТРАКТ ЯК ГАРАНТІЯ БЕЗПЕКИ ДОГОВІРНИХ ПРАВОВІДНОСИН

Актуальність обраної теми дослідження слід розглядати в нерозривній сукупності ознак, що дозволяють визначити тему як актуальну. Такими ознаками є: відповідність сучасному стану наукового дослідження, відповідність тенденціям розвитку наукової думки, практична обґрунтованість теми.

Дану тему прямо або опосередковано розглядали в своїх роботах такі науковці як Савельєв А. І., Баранов О. А., Лещенко Д., Коваленко С. та інші. На даний момент реалізація технології смарт-контрактів є можливою як технічно, так і юридично, проте безпосереднього правового оформлення смарт-контракти ще не отримали, що дає можливість ствер-

джувати, в контексті суцільної діджиталізації та цифрової трансформації, про відповідність сучасним тенденціям розвитку. Практична значущість цієї теми полягає у можливості за допомогою розглянутої технології автоматизувати велику частину бізнес-процесів, створити незалежну децентралізовану систему забезпечення договорів, підвищити довіру контрагентів та знизити витрати на посередництво під час укладання, забезпечення і виконання угод.

З огляду на вищезазначені підстави, слід вважати тему дослідження актуальною, а подолання проблем смарт-контрактів – запорукою гармонійної цифровізації держави та суспільства, а також забезпечення конституційних прав людини на розпорядження власним майном та вільну підприємницьку діяльність [1].

Смарт-контракт або ж розумний договір – це договір, який існує в формі програмного коду, що імплементовано на платформі Blockchain, який забезпечує автономність і самовиконання умов такого договору у разі настання заздалегідь визначених в ньому обставин [2].

Розумні контракти дозволяють здійснювати надійні операції без сторонніх осіб. Ці операції відстежуються та незворотні. Смарт-контракти містять всю інформацію про умови контракту і виконують усі передбачені дії автоматично.

Законодавчого закріплення, як зазначалось вище, смарт-контракт ще не отримав, проте це не означає вихід його з правового поля. Договір може бути укладений у будь-якій формі, якщо вимоги щодо форми договору не встановлені законом. Це означає, що договір у вигляді програмного коду прирівнюється за юридичною значущістю до звичайного договору [3].

За винятком тих правочинів, які потребують нотаріального посвідчення, договір укладений у формі смарт-контракту може використовуватись у переважній більшості правочинів, зокрема: купівлі-продажу, позики, доручення, міни, позички, доручення, тощо.

Для створення смарт-контракту необхідно виконати ряд умов, а саме необхідно створювати його на децентралізованій платформі з технологією Blockchain, вказати умови договору, надати програмі доступ до блокування та розблокування активів та завірити договір цифровими ключами сторін [4].

Смарт-контракт має ряд переваг над звичайною письмовою формою договору:

1. Технологія Blockchain дозволяє виключити можливість фальсифікації будь якої інформації, що є предметом договору або відомостями про виконання умов договору. Така технологія є одночасно механізмом забезпечення збереження інформації, її достовірності та захисту від випадкового знищення.

2. Автоматизація частини або всього договору дозволяє вкладати його між контрагентами, навіть за умови їх низької довіри один до одного, що виключає людський фактор із правовідносин.

3. Можливість інтеграції смарт-законів у алгоритм перевірки блоків інформації, що дозволяє уникнути витрат на юридичні послуги при перевірці законності правочину.

4. Рахунок умовного зберігання (ескроу) здійснює ті самі функції, що і смарт-контракт, однак відсутність посередника в особі банку при переказі коштів дозволяє уникнути витрат на банківські послуги.

5. Технологія Blockchain дозволяє здійснювати розрахункові операції, передбачені умовами договору швидко та на будь-які відстані.

Найбільш реалістичне тлумачення розумних контрактів позиціонує їх у межах вищої законодавчої системи. Як і у випадку з паперовими контрактами, можуть бути встановлені додаткові вимоги, а статті бути анульованими або перетлумаченими на основі намірів сторін та вищого законодавства. Державний закон завжди визнаватиметься вищим за код. Таким чином, хоча більшість обговорень смарт-контрактів визнають, що вони забезпечать підвищення ефективності в деяких областях, вони не замінять традиційне договірне право або контрактних юристів [5].

В контексті розвитку сучасного законодавства в напрямку діджиталізації, формальне визначення та закріплення смарт-контракту є об'єктивно обумовленою необхідністю. Для більшого залучення розумних договорів в цивільний обіг та уникнення технічних та правових проблем реалізації таких договорів на практиці слід розробити Закон України «Про розумні договори», узгодити його з чинним законодавством та Конституцією України. В законі слід визначити поняття смарт-контракту, сферу його застосування, необхідні умови його чинності, вимоги до оформлення та змісту, порядок вирішення спорів та притягнення до відповідальності за порушення законодавства у сфері розумних договорів. Відповідно до створеного закону необхідно внести зміни до Податкового Кодексу, Закону України «Про захист прав споживачів», Закону України «Про електронну комерцію», інших законів та підзаконних актів. Впровадження вищезазначених змін до національного законодавства сприятиме становленню і розвитку правового інституту смарт-контракту, підвищенню швидкості та зручності договірних відносин, розвитку підприємництва та насиченню державної економіки.

Список використаних джерел:

1. Конституція України: Конституція України; Верховна Рада України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 03.11.2020)

2. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. – 2016. – № 3. – С. 32–60. URL: https://elibrary.ru/item.asp?id=26468044 (дата звернення: 03.11.2020).

3. Цивільний кодекс України: Кодекс України; Закон, Кодекс від 16.01.2003 № 435-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/435–15 (дата звернення: 04.11.2020).

4. Andrew Tar. Smart Contracts, explained. October 31, 2017. URL: https://cointelegraph/com/explained/smart-contracts-explained (дата звернення: 04.11.2020).

5. Philip Boucher, Susana Nascimento, Mihalis Kritikos. How blockchain technology could change our live (In-depth Analysis). February, 2017. URL: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA(2017)581948 (дата звернення: 04.11.2020).

Ключові слова: смарт-контракт, блокчейн, правочин, автоматизація договорів.

Ключевые слова: смарт-контракт, блокчейн, сделка, автоматизация договоров.

Keywords: smart contract, blockchain, transactions, automation of contracts.

Науковий керівник: *ас. Байталюк Д. Р.*

РОЗДІЛ 2.
ЕКОНОМІЧНА БЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Горбаченко Станіслав Анатолійович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат економічних наук, доцент

УПРАВЛІНСЬКІ ПЕРЕДУМОВИ ЕКОНОМІЧНОЇ БЕЗПЕКИ В КІБЕРПРОСТОРІ

В сучасному світі питання управління економічною безпекою набувають особливої важливості, адже саме від них залежить геополітичне майбутнє країни, стан національної економіки, соціально-економічний добробут громадян, становлення їхньої національної самосвідомості. Економічна складова є провідною й для національної безпеки України, особливо з урахуванням глобальної економічної кризи та трансформації чинників розвитку національної економіки. Адже, виявляючись у сферах впливу інших видів національної безпеки, проникаючи до них і взаємодоповнюючи, економічна безпека акумулює у собі їхній вплив, залишаючись при цьому фундаментом національної безпеки.

Сучасні дослідники визначають економічну безпеку як стан держави, що забезпечує можливість створення і розвитку умов для плідного життя її населення, перспективного розвитку її економіки в майбутньому та зростання добробуту її мешканців [1, с. 23]. З точки зору існуючої управлінської ієрархії забезпечення економічної безпеки може здійснюватися на рівні держави, регіонів та суб'єктів господарювання.

В масштабі країни економічна безпека виступає не тільки необхідним фундаментом для забезпечення військової, технічної, продовольчої, екологічної безпеки, але й матеріальною

основою для забезпечення національного суверенітету. Серед реальних та потенційних загроз економічній безпеці на рівні держави вагоме місце займають: критичні обсяги та несприятлива динаміка державного боргу, істотне скорочення валового внутрішнього продукту, погіршення інвестиційної привабливості, кадрова криза, зменшення інноваційної активності та науково-технічного потенціалу; нестабільність законодавчого базису, зростання кредитних ризиків, неефективність антимонопольної політики тощо.

На регіональному рівні дотримання економічної безпеки передбачає спрямування пріоритетів на одержання конкурентних переваг на внутрішньому та зовнішніх ринках, економічну незалежність регіону та можливість подолання загроз в економічній сфері. Економічну безпеку регіону визначають як такий його фінансово-економічний стан, при якому забезпечується повноцінне використання всіх видів наявних ресурсів та досягнення бажаних економічних інтересів регіону, та створюються умови для повноцінного стратегічного розвитку в майбутньому [2, с. 208]. Важливість саме регіонального рівня обумовлюється, насамперед, існуючими тенденціями децентралізації та поширенням повноважень об'єднаних територіальних громад. При цьому пріоритетні напрями регіональної політики економічної безпеки відповідають за змістом пріоритетним економічним інтересам та визначають напрями їхньої реалізації. Найбільший вплив на рівень економічної безпеки регіону здійснюють такі чинники як: географічне положення, природно-ресурсний потенціал, економічна спеціалізація, транзитний потенціал, соціально-економічні зв'язки, інвестиційна привабливість, технологічний потенціал, рекреаційний потенціал, стан навколишнього середовища, демографічний фактор, рівень підтримки з боку держави.

На локальному рівні, тобто для окремих підприємств та організацій економічна безпека передбачає запобігання внутрішнім і зовнішнім загрозам з метою гарантування ефективного і стабільного функціонування та динамічного розвитку. Можна

стверджувати, що економічна безпека характеризує поточний стан захищеності найбільш важливих інтересів підприємства від нечесної конкуренції, надмірного тиску з боку контролюючих органів, некомпетентних рішень, недосконалої нормативної бази, а також здатність підприємства до протистояння цим загрозам та, навіть, перетворення їх у можливості. Окремим напрямом економічної безпеки для підприємств є захист від недоброчесної конкуренції.

На будь-якому рівні економічної безпеки вплив на неї здійснюють високий ступінь автоматизації управління і глобалізації інформаційних систем через інформаційно-телекомунікаційні системи загального користування. Це, в свою чергу, надає поштовх до формування глобального інформаційного суспільства і нового середовища його функціонування, тобто кіберпростору.

Під кіберпростором розуміють віртуальне середовище, що надає можливості для здійснення комунікацій та реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та інших глобальних мереж передачі даних.

Запорукою забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, є створення національної системи кібербезпеки. Закон України «Про основні засади забезпечення кібербезпеки України» у ст. 1 визначає кібербезпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [3].

Серед характеристик, що становлять сутнісну основу сучасних тенденцій трансформації кіберсередовища, основну цінність для економічної безпеки становлять наступні: зміна

характеру діяльності осіб, які ухвалюють рішення щодо заходів з кібербезпеки системних об'єктів; цифровізація економічної, наукової, освітньої та соціально - культурної діяльності держави і соціуму; перехід від паперового документообігу до електронно - цифрового; підтримка безпечної, стійкої і надійної роботи операційного/інформаційного середовища, яке мінімізує наслідки злочинних кібервтручань [4, с. 80].

На державному рівні економічна безпека пов'язана з інформаційною інфраструктурою, яка в сучасній геополітичній ситуації набуває статусу критичної з відповідними похідними: вона стає об'єктом першого удару і потребує для свого захисту збалансованої державної політики в інформаційному просторі. До критичної інформаційної інфраструктури належать економіка, транспорт, енергетика, фінансова система, системи управління структур, що забезпечують безпеку та оборону держави.

Таким чином забезпечення належного рівня економічної безпеки України є неможливим без відповідного захисту у кіберпросторі. Проблеми кіберзахисту вже носять не характер локальних загроз функціонуванню підприємств, а розглядаються на національному рівні із залученням усіх зацікавлених структур, а отже, потребують відповідних управлінських рішень на національному рівні.

Список використаних джерел:

1. Пастернак-Таранушенко Г. А. Економічна безпека держави. Методологія забезпечення: монографія. К.: Київський ек-ний інститут менеджменту, 2003. 320 с.

2. Маргасова В. Г. Економічна безпека регіону. *Глобальне управління та економіка: науковий журнал.* 2015. № 1 (1). С. 206–210.

3. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII, редакція від 03.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

4. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері.* 2018. № 1. С. 75–86.

Ключові слова: економічна безпека, кіберпростір, цифровізація економіки, кібербезпека
Ключевые слова: экономическая безопасность, киберпространство, цифровизация экономики, кибербезопасность.
Keywords: economic security, cyberspace, digitalization of the economy, cybersecurity.

Котлубай Вячеслав Олексійович
Національний університет «Одеська юридична академія»,
доцент кафедри національної економіки,
кандидат економічних наук, доцент

Рединa Євгенія Валентинівна
Національний університет «Одеська юридична академія»,
доцент кафедри національної економіки,
кандидат економічних наук, доцент

ПЕРЕДУМОВИ СТВОРЕННЯ ЦИФРОВОЇ ВАЛЮТИ В УКРАЇНІ

За останні кілька років ставлення центральних банків у світі щодо цифрової валюти кардинально змінилося. Так, на підставі опитування проведеного Bank for International Settlements, за останні три роки кількість центральних банків світу залучених до пілотного проекту створення цифрових валют склало близько 80%, на сукупну долю яких припадає майже три чверті світового населення та 90% глобальної економіки.

У 2020 р. Китай, Південна Корея та Швеція проводили експерименти з впровадженням цифрової національної валюти. Також, про можливий випуск національної цифрової валюти і початок експериментів з цифровим євро оголосив Європейський ЦБ, емітент другої за значимістю валюти в світі [1].

Однією з головних причин зміни думки центральних банків щодо впровадження власної цифрової валюти є створення приватних проектів, таких як Libra (криптовалюта Facebook),

які в змозі створити конкуренцію центральним банкам і підірвати грошовий суверенітет цих країн. Це призвело до того, що криптовалюта Facebook зіткнулася з хвилею критики від влади Великобританії, Німеччини, Італії, Канади, США, Франції та Японії. У зв'язку з чим, керуюча нею асоціація Libra Association, в яку входять більше 20 компаній і організацій, збирається змінити свою стратегію, перетворивши Libra в платіжну систему, в якій буде впроваджена підтримка доларів і євро [2].

На сьогоднішній день, пандемія коронавірусу здійснила широкомасштабний вплив на поведінку домогосподарств і компаній щодо платежів. Значно посиливши популярність онлайн-платежів і безконтактних платежів, тим самим збільшивши попит споживачів на швидкі, низьковитратні та надійні грошові транзакції. У зв'язку з чим, глобальна економіка сьогодення потребує впровадження відповідних платіжних інструментів, за допомогою яких можна здійснювати розрахунки швидко, недорого і без зайвих посередників, таких як Visa або Mastercard.

Сьогодні цифрові валюти вже глибоко проникли в світ гейминга. За рахунок ігрових токенов можна купувати квитки на змагання, оплачувати нові версії ігор, купувати товари і певні можливості для комп'ютерних ігор. Це говорить про те, що популярність криптовалюти в геймінговій індустрії буде тільки зміцнюватися. Одна з причин, завдяки якій геймери тяжіють до блокчейну, полягає в тому, що, на відміну від традиційних ігор, середа блокчейн дозволяє гравцям отримати справжнє право володіння своїми ігровими предметами. Це означає, що ігри, створені на блокчейн з використанням NFT-токенів, створюють інноваційну економічну систему, яка дозволяє гравцям заробляти реальні гроші під час гри. Оборот такої системи, за попередніми оцінками, становить близько 370 мільярдів доларів [3].

Необхідно зазначити, що при описі цифрових грошей часто вживаються терміни «цифрова валюта» та «криптовалюта». Слід розуміти, що це не зовсім тотожні поняття.

Так, цифрова валюта – це гроші, які використовуються в інтернеті та існують тільки у віртуальному форматі, вони не мають фізичного еквівалента в реальному світі. У той час як криптовалюта – це різновид цифрової валюти. Це актив, який використовується в якості засобу обміну і вважається надійним, тому що в його основі лежить криптографія.

Незважаючи на те, що криптовалюта це тільки різновид цифрової валюти, існує ряд критичних відмінностей однієї від іншої. Так цифрова валюта, на відміну від криптовалюти, централізована. Тобто існує певна група людей і мережа комп'ютерів, які контролюють мережеві транзакції, також цифрова валюта потрібує повної ідентифікації користувача. В той час як криптовалюта забезпечує більшу анонімність та транзакції з криптовалютою більш прозорі ніж у цифрової валюти [4].

Головними причинами чому центральні банки в світі розглядають можливість впровадження цифрових валют є:

– зменшення залежності від долара або іншої валюти;

– зниження вартості транзакцій і розширення можливостей для здійснення транскордонних платежів;

– цифрова валюта не витісняє інші форми грошей, наприклад, банківські депозити. Банкам потрібні депозити, щоб надавати кредити позичальникам;

– впровадження державної цифрової валюти може підвищити і спростити збирання податків – практично до 100%;

– держава отримає великий масив даних про своїх громадян і їх фінанси;

– впровадження цифрового валюти дозволить контролювати роботу держави, дозволяючи простежити, куди було витрачено кожну бюджетну гривню / цент / юань [5].

В Україні питання про створення цифрової валюти було підняте на при кінці 2016 р. Українським центробанком розглядалася можливість випуску власної ЦВЦБ – е-гривні. Е-гривня повинна була стати цифровим еквівалентом готівки та обмінюватися без обмежень на готівкові або безготівкові гривні в співвідношенні одна до одної.

Вже у 2018 р. Національний банк України реалізував пілотний проект з випуску Е-гривні. В рамках цього проекту регулятор здійснював дослідження міжнародного досвіду, правових аспектів, макроекономічного ефекту та розглядав різні варіанти бізнес-моделі поводження Е-гривні в Україні [6].

За результатами пілотного проекту можна зробити висновки, що Е-гривня здатна в перспективі вирішити ряд питань:

– створити на території України новий, швидкий, економічний та зручний платіжний інструмент;

– оптимізувати тарифи та зменшити операційні витрати на проведення розрахунків;

– зменшити рівень використання готівки в країні;

– підвищити фінансову інклюзію (доступ населення до інноваційних фінансових продуктів і послуг) та рівень фінансової освіти громадян [7].

Проте перед Національним банком стоїть складне завдання: яку структуру CBDC (digital currencies of central banks) платіжної системи необхідно обрати.

На нашу думку, найбільш доцільною вважаємо «гібридну» або «опосередковану» платіжну систему, при якій роздрібні платежі обслуговують банки-посередники, але реєстр транзакцій веде центробанк, який також здійснює управління резервною технічною інфраструктурою, що дозволить запустити платіжну систему у разі виникнення збою у посередників. У цьому варіанті поширенням CBDC може займатися як центральний банк (безпосередньо на гаманці користувачів, відкритих в центробанку), так і безпосередньо банки-посередники (в такому випадку гаманці в центробанку відкривають тільки банки). До впровадження такої платіжної системи також схиляються центробанки Китаю, Канади, Швеції, Бразилії, Великобританії та ЄЦБ. Також, для спрощення інтеграції цифрової валюти, доцільно використати досвід Китаю: впровадження через соціальну та бюджетну сфери.

Важливою потенційною проблемою є ситуація, коли емітентом державної цифрової валюти виступатиме приватна

компанія. Це ризик, уразливості цифровий валюти і її контролю. Тому це питання потребує ще ретельного опрацювання та дослідження відповідного іноземного досвіду.

Список використаних джерел:

1. Цифровая валюта центральных банков: мировой опыт [Електронний ресурс]. – Режим доступу: https://econs.online/articles/regulirovanie/tsifrovaya-valyuta-tsentralnykh-bankov-mirovoy-opyt/.

2. Из криптовалюты в платежную систему. Facebook может сменить профиль Libra [Електронний ресурс]. – Режим доступу: https://tech.liga.net/technology/novosti/iz-kriptovalyuty-v-platejnuyu-sistemu-facebook-mojet-smenit-profil-libra.

3. Цифровая валюта станет неотъемлемой частью индустрии гейминга [Електронний ресурс]. – Режим доступу: https://beincrypto.ru/czifrovaya-valyuta-stanet-neotemlemoj-chastyu-industrii-gejminga/.

4. Цифровые валюты vs. Криптовалюты: В чем разница [Електронний ресурс]. – Режим доступу: https://ru.ihodl.com/tutorials/2017–12–21/cifrovye-valyuty-vs-kriptovalyuty-v-chem-raznica/.

5. Как государственные цифровые валюты изменят нашу жизнь [Електронний ресурс]. – Режим доступу: https://vc.ru/finance/128259-kak-gosudarstvennye-cifrovye-valyuty-izmenyat-nashu-zhizn.

6. Цифровая гривня: какой следующий шаг? [Електронний ресурс]. – Режим доступу: https://nv.ua/biz/experts/elektronnaya-grivnya-poyavitsya-li-svoya-cifrovaya-valyuta-v-ukraine-nbu-50071239.html.

7. Будущее национальной валюты: появится ли в Украине е-гривна [Електронний ресурс]. – Режим доступу: https://psm7.com/emoney/budushhee-nacionalnoj-valyuty-poyavitsya-li-v-ukraine-e-grivna.html.

Ключові слова: криптовалюта, цифрова валюта, блокчейн, центральний банк.

Ключевые слова: криптовалюта, цифровая валюта, блокчейн, центральный банк.

Keywords: cryptocurrency, digital currency, blockchain, central bank.

Лобода Юлія Геннадіївна
Національний університет «Одеська юридична академія»,
кандидат педагогічних наук, доцент

ВИКОРИСТАННЯ КРИТИЧНИХ ТЕХНОЛОГІЙ ЯК НАЙВАЖЛИВІША ДЕТЕРМІНАНТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА РОЗВІТКУ ЕКОНОМІКИ

Опанування передовими технологіями та їх використання є найважливішою детермінантою національної безпеки та розквіту економіки будь-якої країни. Перевага країни у технологічній галузі зумовлює її пріоритетні позиції на світовому ринку й збільшує її оборотний потенціал. Рівень технічного розвитку держави здебільшого визначають за рівнем розвитку критичних технологій, що мають, як правило, характер технологій подвійного використання.

До критичних базових технологій подвійного використання уналежнюють технології, розробка та використання яких відіграє значну роль при досягненні національних ідей як у галузі безпеки, так і у галузі економічного та соціального розвитку країни [1].

Процес розвитку базових технологій у країнах різний та нерівномірний. Сьогодні США, Європа та Японія – це країни з високим рівнем розвитку технологій. Ці країни «тримають у руках» ключові технології та забезпечують собі стійке положення на міжнародних ринках готової продукції.

Карл Уейк, характеризуючи поняття «нова технологія», описав такі її властивості [2]:

– стохастичність (непередбачуваність) – нові технології настільки складні й варіативні, що реалізуються не завжди передбачено. Їх важко контролювати, використовуючи раціоналістичні підходи. Результатами окремих стадій таких технологій можуть бути абсолютно несподівані речі.

– безперервність – це властивість нових технологій, пов'язана з широкою автоматизацією технологічних процесів. В автоматизованих системах увага оператора концентрується не на ефективності, а на надійності роботи і найважливішим

його завданням стає підтримка системи в робочому стані. Відповідно в організаціях, що ґрунтуються на нових технологіях, увага керівника також зміщена – з безпосереднього керівництва і контролю на забезпечення надійності. В організаціях, що широко використовують сучасні інформаційні технології, інформаційні потоки розподілені таким чином, що значна кількість інформації проходить повз керівника.

– абстрагованість – якщо раніше людина могла безпосередньо спостерігати за технологічним процесом (на конвеєрі, у майстерні), то нові технології позбавляють її такої можливості. Ми не знаємо точно, і тим більше не можемо проконтролювати, як надсилається електронний лист, як скачується файл з Інтернету тощо.

Розглянемо оновлений перелік критичних технологій, в який на даний момент, включені деякі інформаційні технології:

– Інформаційні технології, до складу яких входять "Технології створення завадозахищених та шифрованих каналів управління та передачі даних", "Технології спеціального призначення, в тому числі для створення ефективних систем захисту від інформаційної зброї та шпигунства"; "Технології створення і нарощення системи захисту інформації та кіберзахисту в інформаційно-телекомунікаційних системах"; "Технології штучного інтелекту і робототехніки" [3];

– CAE-технології засновані на критичній технології "Інформаційні технології та системи штучного інтелекту (машинний збір і оброблення зображень, обробка й розуміння мови, експертні системи та системи підтримання прийняття рішень)" і є інструментарієм для проведення математичного моделювання та обчислювального експерименту на основі принципово нових математичних моделей, містять ефективні кількісні методи реалізації таких моделей, алгоритми яких адаптовані до архітектури сучасних ЕОМ.

– CAE-технології тісно пов’язані з критичною технологією "Інтелектуально високі технології керування рухомими об'єктами", оскільки орієнтовані на ефективне використання обчислювальних систем підвищеної обчислювальної потужності, містять підсистеми автоматизації розпаралелювання

обчислень і є прикладними програмними комплексами для розв'язання актуальних прикладних задач високої складності.

– CAE-технології здійснюють вплив і на інші критичні технології "Нові лазерні технології, лазерна техніка для технологічних цілей", "Технології виробництва оптичних матеріалів для електроніки", "Технології очищення вихлопних газів двигунів внутрішнього згорання", "Технології безлюдного високопродуктивного видобутку вугілля з тонких і похилих пластів з використанням сімейства автоматизованих модульно-поєднаних комплексів нового покоління", "Технології принципово нових конкурентоспроможних рідинно-кристалічних засобів відображення інформації".

Якщо проаналізувати позиції України у глобальних рейтингах конкурентоспроможності (Global Competitiveness Index, GCI), то можна констатувати такі результати: індекс конкурентоспроможності 16,02 пункту з 2007 року по 2019 рік, досягнувши рекордного максимуму в 57,03 пункту в 2018 році і рекордного мінімуму в 3,90 пункту в 2011 році [4].

Серед проблем, які залишаються перешкодою для поліпшення існуючого стану, не лише погіршення макроекономічної ситуації, технологічна відсталість і відсутність інновацій, фізичне і моральне старіння технологічного обладнання, науково-дослідної бази, занизький рівень наукоємності української продукції, а й загострення проблем ринку праці, неадекватність рівня якості і змісту вищої технічної освіти стратегічній спрямованості розвитку світової та вітчизняної економік [5].

У ситуації, що склалася, необхідно ефективно використовувати технологічні досягнення інших розвинених країн, розвивати технологічну співдружність та прагнути максимально широкої кооперації та міжнародному розподілу праці, ураховуючи динаміку цих процесів у всьому світі. Необхідно розуміти, що передові в технологічній сфері країни вже створили єдиний технологічний простір. Тому, спираючись на міжнародну співпрацю та розподіл праці, потрібно оволодівати низкою технологій – критичних технологій, що забезпечують обороноспроможність та безпеку країни, а також забез-

печують конкурентоспроможність вітчизняної наукомісткої продукції на міжнародному ринку.

Список використаних джерел:

1. Лобода Ю. Г. Педагогічні умови використання комп'ютерно-інтегрованиї технологій у процесі підготовки майбутніх інженерів: дис… канд. пед. наук: 13.00.04 / Лобода Юлія Геннадіївна. – Одеса, 2010. – 280 с.
2. Weick, Karl E. Technology as equivoque. Sensemaking in New Technologies / In Paul S. Goodman, Lee S. Sproull and Associates (eds.) Technologies and Organization. San. Francisco: Jossey-Bass, 1990, P. 5–44.
3. Кабінет Міністрів України. Розпорядження від 30 серпня 2017 р. № 600-р Київ. Деякі питання розвитку критичних технологій у сфері виробництва озброєння та військової техніки. – Режим доступу: https://zakon.rada.gov.ua/laws/show/600–2017-%D1%80#n11 (дата звернення: 10.11.2020).
4. Ukraine Competitiveness Index2007–2019 Data |2020–2022 Forecast | Historical. https://tradingeconomics.com/ukraine/competitiveness-index. (дата звернення: 10.11.2020).
5. Інноваційний розвиток в Україні: наявний потенціал і ключові проблеми його реалізації (Аналітична доповідь Центру Разумкова) // Національна безпека і оборона. – № 7 (55). – К.: Український центр економічних і політичних досліджень імені Олександра Разумкова, 2004. – С. 2–25.

Ключові слова: технології, критичні технології, інформаційні технології.

Ключевые слова: технологии, критические технологии, информационные технологии.

Keywords: technology, critical technology, information technology.

Кравцов Олександр Олександрович
Національний університет «Одеська юридична академія»,
студент 4 курсу факультету кібербезпеки
та інформаційних технологій

ДОСЛІДЖЕННЯ ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ СУЧАСНОГО ПІДПРИЄМСТВА

В нову еру використання технологій, людство частіше почало використовувати та інтегрувати інформаційні

технології не тільки для полегшення повсякденного життя, але також для оптимізації праці, пришвидшення вироблення різних послуг та безлічі інших завдань.

Почалося використання інформаційних технологій в бізнесі та на підприємствах, які в собі представляють необхідність для підтримки та розвитку економіки країни.

В їх розпорядженні з'явилися інформаційні системи – системи, що обробляють та зберігають необхідну для їх потреб інформацію. Але з часом такі складні системи було все складніше контролювати та контролювати, тому, зі згодом для цього з'явилися, як логічний крок вперед, інформаційні інфраструктури, які були використані не тільки для підприємств, але і наукових цілей. Разом з ними покращився не лише локальна передача та обробка інформації, але і глобальна.

Згідно з законодавством: «Інформаційна інфраструктура – сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування» [1].

Використання таких інфраструктур зменшує роль місця, часу та ієрархії у структурі та управлінні організаціями. Залишається величезний спектр організаційних можливостей які можливо застосувати та треба дослідити.

Складаючись в першу чергу з інформаційних систем, треба брати до уваги також проблеми їх захисту. Захист інформаційних систем відповідає за цілісність та безпеку системних ресурсів та діяльності. Більшість організацій розвинених країн залежать від безпечної роботи своїх інформаційних систем.

Насправді, сама структура суспільства часто залежить від цієї безпеки. Багато інфраструктурних мереж – включаючи електроенергію, водопостачання та охорону здоров'я – покладаються на це. Інформаційні системи лежать в основі відділень інтенсивної терапії та систем управління повітряним рухом. Фінансові установи не могли пережити повний збій своїх інформаційних систем довше, ніж день-два.

Тому завжди треба брати до уваги не тільки захист інформаційної інфраструктури в цілому, але особливо її частини, так як вони можуть скомпрометувати всю інфраструктуру.

Незважаючи на бажаність загальних стандартів, підприємства в основному не змогли узгодити протоколи або стандарти зв'язку для різних видів запитів. Однією з причин цього збою були неадекватні технології (наприклад, використання примітивних форматів подання даних у фіксованому форматі) та надмірна складність.

З іншої сторони, загальні стандарти локальних підприємств більше підтримуються законодавством, яке, в свою чергу потребує вдосконалень, та яке допоможе реалізувати необхідний захист для інформаційної структури не лише окремих підприємств, але і країни в цілому.

Цікавим для дослідження буде питання забезпечення успішного функціонування інформаційної інфраструктури спеціальним відділом, який складається зі спеціалістів в інформаційних технологіях, та питання проектування конкретних систем в інформаційній інфраструктурі підприємства з подальшим його захистом та захистом інформації яка обробляється в такій інфраструктурі.

Список використаних джерел:

1. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України; Стратегія від 15.05.2013 № 386-р // Офіційний вісник України офіційне видання від 21.06.2013–2013 р., № 44, стор. 79, стаття 1581, код акта 67438/2013

Ключові слова: кібербезпека, інформаційна інфраструктура, підприємство.

Ключевые слова: кибербезопасность, информационная инфраструктура, придприемство.

Key words: cybersecurity, information infrastructure, enterprise.

***Науковий керівник**: д. ф-м. н., д.ю.н., професор Василенко М. Д.*

РОЗДІЛ 3.
СОЦІАЛЬНО-ПОЛІТИЧНІ УМОВИ ФОРМУВАННЯ КІБЕРПРОСТОРУ

Логінова Наталія Іванівна
Національний університет «Одеська юридична академія»,
завідувач кафедри інформаційних технологій,
кандидат педагогічних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА В ЕЛЕКТРОННОМУ УРЯДУВАННІ

Електронне урядування є одним з провідних напрямів розвитку інформаційного суспільства сьогодення, що передбачає ефективне використання сучасних інформаційно-комунікаційних технологій та інформаційних ресурсів для забезпечення відкритої взаємодії органів публічної влади та суспільства, надання повного комплексу державних послуг.

Електронне урядування передбачає організацію державної влади за допомогою локальних інформаційних мереж та сегментів глобальної інформаційної мережі інтернет, що дозволяє забезпечити роботу в режимі реального часу, спростити та зробити доступним спілкування громадян з органами державної влади та отримання різних адміністративних послуг [1].

Проблеми інформаційної безпеки електронного урядування в силу специфіки адміністративного процесу управління безпосередньо пов'язані з процесом інформатизації органів державної влади, що здійснюється на основі Концепції розвитку електронного урядування в Україні. Згідно даної Концепції елементами ІТ-інфраструктури електронного урядування є система електронної взаємодії державних реєстрів, система електронної ідентифікації, електронний кабінет громадянина, вебпортал електронного урядування, спеціальні захищені

мережі передачі даних, захищені центри обробки даних, базові державні реєстри [2].

У зв'язку з цим можна виділити основні загрози та вразливості, які притаманні електронному урядуванню:

– несанкціонований доступ до інформації користувачів та адміністративних інформаційних ресурсів;

– несанкціоноване втручання в програмне забезпечення;

– зараження комп'ютерними вірусами та міжсайтова вразливість адміністративних інформаційних порталів;

– неефективні механізми розмежування доступу до даних користувачів;

– недоступність сервісу або перевищення встановлених законом термінів з надання адміністративних послуг та інше.

Несанкціонований доступ до інформаційних ресурсів сьогодні є найбільш поширеним видом інформаційних загроз. Він полягає в тому, що користувач отримує доступ до об'єкту, на який у нього немає дозволу відповідно до політики безпеки. Для запобігання цій небезпеці в системах електронного урядування необхідно використовувати ідентифікацію та аутентифікацію. Система цифрової ідентифікації громадян є одним з ключових елементів національної програми «Держава в телефоні». Відсутність єдиної системи цифрової ідентифікації в Україні знижує ефективність розвитку електронного урядування.

Втручання в програмне забезпечення пов'язане з несанкціонованим впливом з метою порушення цілісності, конфіденційності та доступності адміністративних інформаційних ресурсів. До них відносяться завантаження підробленої інформації або видалення деяких інформаційних контентів.

Зараження комп'ютерними вірусами відбувається через адміністративні інформаційні портали з метою отримання персональної інформації користувачів, блокування доступу до інформаційних ресурсів, виведення з ладу інформаційних адміністративних порталів.

Адміністративні інформаційні портали часто схильні до атак хакерів та злому. Зламані портали є метою

несанкціонованого отримання персональної інформації користувачів, встановлення шкідливих вірусних програм, шахрайством, проникненням у внутрішню мережу адміністративних установ тощо.

Розмежування доступу сприяє використанню ресурсів інформаційної системи в суворій відповідності до встановлених правил доступу до інформації, в залежності від відповідних ресурсів. Порядок доступу до інформації визначається вимогами, правилами використання, збереження та поширення інформації. ІТ-інфраструктура інформаційних порталів з надання адміністративних послуг повинна бути доступна не тільки внутрішнім співробітникам (державним службовцям), але й громадянам, які звертаються за певними адміністративними послугами. Відповідно, кількість користувачів, що мають доступ до адміністративної інформації, постійно зростає. Тому одним з основних способів зменшення ризиків витоку інформації є ефективний розподіл повноважень користувачів за допомогою систем управління і контролю доступу.

Недоступність сервісу або перевищення встановлених законом термінів з надання адміністративних послуг пов'язане з перевантаженістю, відсутністю необхідних документів та компетентних співробітників. Для вирішення даної проблеми в листопаді 2020 р. розроблені поправки до Закону України «Про внесення змін до деяких законодавчих актів України щодо оптимізації мережі та функціонування центрів надання адміністративних послуг та удосконалення доступу до адміністративних послуг, які надаються в електронній формі». Зокрема, Закон передбачає моніторинг якості адміністративних послуг, що надаються в електронній формі, спрощення подачі заяв, організація для громадян зворотного зв'язку з пропозиціями та зауваженнями про якість послуг, що надаються на вебпорталах адміністративних органів та інше.

Різноманіття вразливостей і загроз говорить про складність забезпечення інформаційної безпеки електронного урядування. Тому доцільно сформувати умовну концептуальну модель інформаційної безпеки електронного уряду, в

якій треба чітко спланувати розвиток інформаційної безпеки, удосконалити політику безпеки в цій галузі, визначити ризики і загрози інформаційній безпеці, джерела цих загроз, способи та методи їх реалізації. А також удосконалити засоби захисту, що вже існують, і розробити нові, з метою впровадження, експлуатації та розподілу адміністративних інформаційних ресурсів.

Список використаних джерел:

1. Соломко Ю. . Електронне урядування: поняття, сутність, принципи та напрями розвитку. Ефективність державного управління, 2018, ВИП. 2 (55), Ч. 1.

2. Концепція розвитку електронного урядування в Україні: Розпорядження КМУ від 20.09.2017 № 649-р.

Ключові слова: інформаційна безпека, електронне урядування, адміністративні інформаційні ресурси, загрози інформації

Ключевые слова: информационная безопасность, электронное управление, административные информационные ресурсы, угрозы информации

Keywords: information security, e-governance, administrative information resources, information threats

Василенко Микола Дмитрович
Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, доктор юридичних наук,
професор

Матковська Інга Олексіївна
студентка 4 курсу факультету кібербезпеки
та інформаційних технологій

ДЕЯКІ ПИТАННЯ РИЗИКІВ (ІНФОРМАЦІЙНИХ РИЗИКІВ) В КОНТЕКСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Відомо, що соціальна інженерія сформувалася в науку і представляє собою вивчення людської поведінки та факторів,

які на неї впливають. Вона досліджує причини поведінки тої чи іншої людини та обставин та середовища, що впливають на формування системи її цінностей та саму поведінку [1]. Оскільки на чолі приведеного визначення стоїть людина та її поведінка, то важливою стає створена нею безпечна ситуація, яка проявляється, в першу чергу, в ризиках, пов'язаних з діяльністю самою людини. Відбувається проникнення ризику в усі сфери людської діяльності, а тому поділяти ризики на види досить важко: це процес нескінченний і недоцільний. Однак доречним сталося дослідити ризики за механізмом виникнення. Так, виділяють ризики, пов'язані з несприятливими умовами життєдіяльності (функціонування організацій); ризики, зумовлені небезпечними явищами (форс-мажором) в природному, техногенному, соціальному та діловому середовищі; зумовлені негативними тенденціями розвитку, що приводять до криз (для організації до погіршення її фінансового стану і в результаті до банкрутства). Тенденції можуть бути пов'язані із зовнішніми факторами, що формують несприятливу кон'юнктуру для організації, або з внутрішніми, пов'язаними, наприклад, з протиріччями всередині самої організації [2].

В зазначених вище умовах виникає ситуація невизначеності, яка представляє собою сукупність обставин і умов, за яких можливі зміни стану об'єкта ризику стають абсолютно непередбачуваними. Ця ситуація виключає можливість об'єктивного оцінювання ризику. Однак певне зменшення невизначеності до рівня так званої статистичної невизначеності породжує ризикову ситуацію, яка характеризується, існуванням кількох можливих станів (як варіант – множини станів, що сягає нескінченості), ймовірність реалізації кожного з яких відома. Якщо реалізацію на об'єкт ризику будь-якого з можливих станів вважати подією, РС визначається існуванням множини варіантів можливого розвитку подій, ймовірність кожного з яких характеризується відповідною кількісною або якісною оцінкою. За умов виникнення ризикової ситуації стає

актуальним проведення аналізу й оцінювання ризиків, зокрема дослідження обставин появи, умов та форм розвинення ризиків.

Отже, загалом під невизначеністю розуміють неповне або неточне уявлення про значення різних параметрів в майбутньому, що породжується неповнотою і (або) неточністю інформації щодо виникнення в ході реалізації рішення несприятливих ситуацій і наслідків, що призводить до ризику. У той же час ситуація ризику вважається фактично різновидом невизначеності, коли при настанні подій ймовірно і об'єктивно існує можливість оцінити їх вірогідність. Різниця між ризиком і невизначеністю відноситься до способу завдання інформації та визначається наявністю (у разі ризику) або відсутністю (при невизначеності) імовірнісних характеристик неконтрольованих змінних. Ці відмінності враховуються в математичної теорії дослідження операцій, де розрізняють задачі прийняття рішень при ризику і відповідно в умовах невизначеності.

Інформаційна невизначеність є або єдиною основою випадковості події для людини, або вона супроводжує і доповнює об'єктивну випадковість. З такого висновку виходить інформаційна парадигма ризиків будь-якої природи: інформаційна невизначеність є суть усіх ризиків. При таких умовах важливим чинником в ризиках стає психологічна складова явища. При цьому будь-яке прийняття рішення ґрунтується на мисленні, що відбувається в умовах невизначеності (в більшій чи меншій мірі), на особистісної зумовленості виборів і особистих або соціальних моделях прийняття рішення. Незалежно від інтелектуальної бази мислення конкретної людини, специфіки техногенної або соціальної ситуації, в якій він змушений діяти, особливості морально-етичних, моральних установок, ступеня інтенсивності їх відстоювання індивідом всі варіанти прийняття ризикованого рішення об'єднує загальна властивість – вони є реалізацією суб'єктом інтелектуально-особистісних зусиль, спрямованих

на зниження рівня невизначеності ситуації. При цьому людина сприймає своє рішення як довільний вибір, здійснений ним відносно вільно (аспект вимушеність присутній завжди, але не завжди пригнічує волю) в рамках певної альтернативи можливих варіантів поведінки. Інформаційна складова ризику найбільш вагома у випадках використання прогнозної інформації, дефіциту часу на обробку інформації і ухвалення рішення, в умовах активної інформаційної протидії конкурентів або супротивника. На відміну від інших складових ризику інформаційна складова обов'язково є присутньою в кожній ризиковій події. Змінюється лише її відносна величина.

Настанню ризикової події можуть сприяти свідомі або неумисні дії людини. Навіть маючи якісну інформацію, фахівець може прийняти неправильне рішення або виконати неприпустиму дію, яка спричинить реалізацію ризикової події. Значна частина ризикових подій пов'язана з технічними системами, технологічними процесами, отриманими людиною речовинами і іншими об'єктами, що є продуктами людської діяльності. Техногенні аварії, збої і відмови устаткування, екологічні катастрофи, пандемії далеко не вичерпують повного переліку компонентів цього типу. Людина майже безсила перед цілим рядом стихійних лих. Значна частина з них доки ще не піддається точному і своєчасному прогнозуванню.

Сьогодні практично відсутні дієві підходи до трактування поняття «Інформаційний ризик», в яких в якості можливих небажаних подій розглядалися б події, що призводять до зниження достовірності, повноти та актуальності інформації на стадії її отримання та введення в інформаційну систему. У поняття інформаційний ризик не включають також риски, пов'язані з можливою наявністю помилок в моделях, алгоритмах обробки інформації, програмах, які використовуються для вироблення рішень, що управляють, і виготовленні безпосередньо з участю людини. Разом з технічною складовою і в інформаційних ризиках основною все ж-таки залишається людина. Виникають складності у розпізнаванні достовірної (недосто-

вірної) інформації: треба враховувати морально-етичний стан людини, а також стан правового регулювання, захисту персональної інформації особи та постійне технічне удосконалення конкретних інформаційно-комунікаційних систем [1].

Достатньо швидко технічні системи захисту все більше й більше удосконалюються за рахунок постійного розвитку сучасних технологій, обліку безлічі потреб, які створюють додаткові ризики. До грамотно відбудованим технічним системам захисту можна тривалий час не підходити і останні будуть справно виконувати свої основні функції та завдання, а люди як і раніше будуть

залишатися найбільш вразливою ланкою, коли вони мають доступ до інформації та на них можна впливати методами соціальної інженерії.

Соціальні інженери користуються тим, що психологічні маніпуляції не вимагають великих витрат і специфічних знань (крім кількох психологічних прийомів), їх можна застосовувати протягом тривалого часу, а ще їх складно виявити. Люди, які володіють цінною інформацією або мають до неї доступ, можна порівняти з доступним плодом: вони на увазі і до них дуже легко дотягнутися.

Захищатися від технік соціальної інженерії складно, так як жертви часто не здогадуються про те, що їх обдурили і використали їх слабкості, щоб роздобути конфіденційну інформацію. Вирішити проблему можна одним способом: підвищувати нашу усвідомленість. А для цього нам доведеться навчитися правилам роботи з інформацією і донести небезпеку її розкриття, щоб вміти визначити інформацію, вразливу до атаки [3].

Тему ризиків в контексті соціальної інженерії можна можна продовжувати і далі, але це все одно не захистить інформаційні технології і апаратуру від зловмисників і шахраїв усіх мастей. Випливає один вахливий висновок: типових протидій діям соціальних інженерів і соціальній інженерії не існує і, і навряд чи може існувати. Кожна ситуація вимагає індивідуального підходу і всебічного розгляду.

Список використаних джерел:

1. Резник Ю. М. Соціальна інженерія: предметна область і межі застосування. Социс. 1994. № 2. С. 28–34.
2. Василенко М. Д., Козін О. Б. Право в теорії ризиків: ґенеза ризиків від правової до інфомаційної складових (інституційний підхід). Юридичний вісник. – О.: ВД «Гельветика». 2019. № 4. С. 43–51.
3. Касперски Кріс. Секретна зброя соціальної інженерії: Компанія АйТи. 2005. С. 15.

Ключові слова: соціальна інженерія, людина, ризики, інформаційні ризики, невизначеність, метод, інформаційні атаки.

Ключевые слова: социальная инженерия, человек, риски, информационные риски, неопределенность, метод, информационные атаки.

Keywords: social engineering, human, risks, information risks, uncertainty, method, information attacks.

Трофименко Олена Григорівна
Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

АНАЛІЗ СТАНУ Е-УРЯДУВАННЯ В УКРАЇНІ

За умов повсюдного дистанціонування та карантину, спричинених глобальним спалахом пандемії COVID-19, цифрові рішення стали життєво важливими для подолання ізоляції, інформування та спілкування людей. Уряди усього світу докладають наполегливих цифрових зусиль щодо залучення нових способів надання якісних е-послуг.

Світовий досвід доводить, що е-урядування надає значні можливості для трансформації системи державного управління в інструмент сталого розвитку разом зі зменшенням часових і матеріальних витрат громадян і бізнесу при взаємодії з державою, забезпеченням прозорості діяльності органів влади, суттєвим зменшенням бюрократії і корупції, залученням громадян до участі у державних справах [1].

При цьому світова спільнота приділяє значну увагу міжнародному співробітництву у цій сфері з метою створення ефективних моделей управління з урахуванням специфіки та менталітету тої чи іншої країни. Так, починаючи з 2003 року відділ державного управління та управління розвитком ООН раз на два роки проводить дослідження з оцінки готовності і можливості національних державних структур у використанні інформаційних та комунікаційних технологій для надання громадянам державних послуг, на підставі чого складається рейтинг країн світу за рівнем розвитку е-уряду. Рейтинг E-Government Development Index (EGDI) формується виходячи з індексу розвитку е-уряду на основі оцінки ступеня охоплення та якості е-послуг, рівня розвитку ІТ-інфраструктури та людського капіталу.

Так, за даними рейтингу EGDI-2020 Україна посіла 69 місце з-посеред 193 країн, погіршивши свої показники, порівняно з даними попереднього дослідження 2018 року, на 13 пунктів [2]. Це суттєве для країни просідання здебільшого зумовлено недостатньо розвиненою телекомунікаційною інфраструктурою. Так, індекс Telecommunications Infrastructure Index (TII) для нашої країни склав лише 0.5242, хоча він і зріс, порівняно зі значенням в EGDI-2018–0.4364. Проте він набагато гірший, порівняно, приміром, з показниками нашої країни-сусідки Білорусі, де TII має значення 0.8281, не кажучи про світового лідера за цим показником Монако, де цей індекс становить 1.0. Подібна, хоча і трохи краща ситуація з індексом онлайн-послуг. У рейтингу EGDI-2018 він мав значення 0.5694, нині в EGDI-2020 він дещо зріс до 0.6824. Надалі варто залучати успішний досвід лідера регіону за цим показником Естонії (0.9941) та світового лідера Кореї задля швидкого й успішного розвитку е-урядування як ефективного інструмента забезпечення прозорості влади, боротьби з корупцією, підвищення якості обслуговування і залучення громадян. Адже акцент на вдосконаленні надання державних е-послуг може значно прискорити прогрес у загальному розвитку е-уряду.

Якщо більш детально проаналізувати причини низького значення індексу розвитку телекомунікаційної інфраструктури (ТІІ) нашої країни, то стають зрозумілими можливі напрями діяльності держави щодо якнайскорішого покращення ситуації. Сам індекс ТІІ складається з чотирьох показників. Найкращі досягнення України відзначено у показнику використання мобільних стільникових телефонів – значення становить 120 на 100 жителів. Показник відсотку осіб, які користуються Інтернетом, становить лише 62.55%. Показник користування послугами фіксованого (дротового) широкосмугового зв'язку дотягнув лише до 12.8%, в той час як показник активних користувачів послуг мобільного широкосмугового зв'язку є 47.16% жителів.

Крім того, в Україні індекс відкритих урядових даних має значення 89.69%, в той час коли цей показник, приміром, в Молдові, Узбекистані, Казахстані, Естонії та в усіх розвинених країнах цей показник становить 100% [2]. Саме рейтинг прозорості державних органів спрямований на підвищення ефективності управління державними підприємствами, поліпшення якості демократії в країні, зменшення ризиків корупції та розкрадання державних коштів. Нині в Україні найменш прозорими визнано переважно ті органи місцевого самоврядування та державні підприємства, які не мають власних вебресурсів, або вони в них малоінформативні і не мають зворотного зв'язку від громадян до урядовців. Тому варто вибудувати систему автоматизованого надання державних е-послуг і максимально вилучити чиновників з процесу надання цих послуг. А для покращення стану прозорості та підзвітності державних установ, окрім використання новітніх технологій, доречно залучати громадян до участі в процесах ухвалення рішень, боротьби з корупцією.

Вагомим з численного переліку заходів щодо спрощення розбудови цифрової держави є реалізація та запровадження національного проекту «Дія», який у подальшому має стати простим і зрозумілим єдиним сервісом для отримання широкого спектру е-послуг держави.

Позаяк цифрова трансформація країни є колосальним інвестиційним ресурсом, варто суттєво покращити рівень покриття території України цифровими інфраструктурами:

– покрити 100% території широкосмуговим доступом до Інтернету і тим самим прибрати цифровий розрив у доступі громадян до цифрових технологій;

– оцифрувати всі державні послуги і спростити їх надання громадянам і бізнесу у рамках єдиного електронного вікна з максимально простою і зрозумілою, проте надійною і захищеною ідентифікацією громадян;

– побудувати сучасні інфраструктури Інтернету речей, зручної і простої електронної ідентифікації тощо.

– посилити контроль щодо нових викликів та ризиків з кібербезпеки та конфіденційності даних.

Впровадження на державному рівні цифрових інновацій та вдосконалення е-урядування у ці важкі часи дозволить пом'якшити наслідки глобальної кризи і навіть сприятиме розбудові цифрової інфраструктури країни, а як наслідок – національного сталого розвитку.

Список використаних джерел:

1. Трофименко О. Г. Аналіз передового світового досвіду е-урядування. *Порівняльно-аналітичне право: електронне наукове фахове видання*. Ужгород, 2018. № 1. С. 220–224. URL: http://pap.in.ua/1_2018/65.pdf.

2. E-Government Survey 2020. URL: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.

Ключові слова: е-урядування, е-уряд, е-послуги, державні послуги, цифрова інфраструктура.

Ключевые слова: электронное управление, электронное правительство, электронные услуги, государственные услуги, цифровая инфраструктура.

Keywords: e-governance, e-government, e-services, public services, digital infrastructure.

Антіпіна Надія Сергіївна
Національний університет «Одеська юридична академія»,
студентка 1 курсу факультету кібербезпеки
та інформаційних технологій

ОСОБЛИВОСТІ ПРОТИДІЇ КІБЕРБУЛІНГУ

Термін «Кібербулінг» (англ. Cyber bullying) почав активно використовуватися в кінці 90-х, під час поширення інтернету та розвитку соціальних мереж. Під ним розуміється вид булінгу (цькування), де агресивна, токсична поведінка однієї особи чи групи осіб, що спрямовала на жертву поширюється за допомогою засобів Інтернету: соціальних мереж, месенджерів, ігрових платформ. Зазвичай це поняття використовують по відношенню до дітей, а для дорослих існує формулювання «кіберхаррасмент» (cyber harassment).

Центром дослідження кібербулінгу в США (Cyberbullying Research Center) було проведено 10 опитувань, в яких взяли участь 20000 учнів середньої та старшої школи 2007–2016 рр, в результаті яких отримали, що близько 28% учнів протягом життя були жертвами інтернет булінгу. За даними опитування, що влаштувала благодійна організація протидіїї булінгу (Ditchthe Label) у Великобританії в 2017 році, 17% осіб у віці 12–20 років стикалися з кібербулінгом. 29% українських підлітків і молодих людей говорять про те, що стали жертвами булінгу в інтернеті. Для жертв наслідки можуть варіюватися від відчуття образи та гніву до ненависті та самогубства. Булінг є причиною появи низької самооцінки, тривожності, депресії та інших проблем, які потенційно можуть загрожувати їхньому психічному та емоційному здоров'ю. Спираючись на ці дані, можна побачити, що проблема кібербулінгу є масштабною, особливо в період навчання у школі, актуальною в усьому світі. Це підтверджує необхідність розробки програм, спрямованих як на попередження, так і на усунення випадків булінгу, підтримку та захист жертв цькування.

Булінг в інтернеті поділяють на такі різновиди: флеймінг – розпалювання конфлікту між учасниками, що супроводжується образливими висловлюваннями, погрозами без певної мети; тролінг – розміщення в інтернеті провокаційних повідомлень з метою викликати негативну емоційну реакцію або конфлікти між учасниками; хейтінг – негативні коментарі та повідомлення, критика на адресу конкретної людини або явища, часто без обґрунтування своєї позиції; кіберсталкінг – переслідування, залякування, домагання до жертви, збирання її особистої інформації, використовуючи засоби інтернету; аутінг – оприлюднення особистої інформації жертви без її згоди та інш. Складність владнання проблеми цькування в інтернеті полягає в тому, що кібербулінг та його види мають неконтрольований характер; злочинці можуть бути анонімними; інформація чи фотографії, розміщені в Інтернеті або переслані масовими електронними листами, можуть охопити більшу аудиторію швидше, ніж традиційні методи, завдаючи жертвам більшої шкоди; немає обмежень щодо того, хто може переглядати чи стати учасником процесу; набагато легше отримати доступ до персональної інформації жертви.

В Україні офіціальна протидія булінгу стала можливою 18 грудня 2018 року після прийняття Закону № 8584 «Про внесення змін до деяких законодавчих актів щодо протидії булінгу», який вперше визнає юридично поняття булінгу в українському законодавстві та передбачає відповідальність не тільки за вчинення, але й за приховування випадків булінгу. Законом визначено, що булінг (цькування) – це діяння учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, у тому числі із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи або такою особою стосовно інших учасників освітнього процесу, внаслідок чого могла бути чи була заподіяна шкода психічному або фізичному здоров'ю потерпілого Також вчинення булінгу тягне за собою накладення певний штрафів,

які збільшуються при повторному звинуваченні. Також, за неповідомлення керівником закладу освіти уповноваженим підрозділам органів Національної поліції України про випадки булінгу тягне за собою накладення штрафу від 850 до 1700 грн або виправні роботи на строк до одного місяця з відрахуванням до 20% заробітку.

Соціальні мережі несуть відповідальність за захист своїх користувачів також вживають заходів для усунення можливості їх кібербулінгу. У кожної соціальної платформи є інструменти, з їх допомогою можна повідомляти про випадки цькування або залякування. Розглянемо на прикладі декількох популярних мереж.

1) Facebook та Instagram

Facebook має інформаційний ресурс «Центр запобігання цькування», що призначений допомогти користувачам уникнути булінгу в інтернеті відносно себе та інших людей. Користувач завжди може відправити анонімну скаргу на пост, коментар, історію в Facebook чи Instagram. Скарги розглядаються цілодобово більш ніж 50 різними мовами; після підтвердження, що певна інформація дійсно є образливою або залякуючою – вона видаляється, а конфіденційність цієї скарги зберігається. Facebook має спеціальний посібник, який допоможе вам прийняти необхідні дії, якщо ви стали жертвою булінгу. У Instagram є Керівництво для батьків, яке містить поради для батьків, опікунів і дорослих довірених осіб про те, як вирішити проблему інтернет-цькування, а також центральний портал, де можете дізнатися про їхні інструменти безпеки. Використовуючи інструменти, доступні прямо на сайті, можна повідомити про те, що особа є жертвою цькування, або свідком булінгу іншого користувача. Детальну інформацію про те, як відправити скаргу можна знайти в Центрі підтримки Instagram і Центрі підтримки Facebook. Інструмент в Instagram під назвою Restrict (обмеження доступу до свого облікового запису), надає можливість непомітно захистити свій обліковий запис так, щоб агресор не буде цього знати. Це було зроблено,

щоб допомогти жертвам, які бояться відкрито протистояти агресивно налаштованим особам. Інша опція цих соцмереж дозволяє користувачам включити настройку, яка використовує штучний інтелект, що автоматично фільтрує і приховує негативні коментарі, націлені на те, щоб образити людей. Facebook та Інстаграм видаляють всю інформацію, яка не збігається з їх політикою, такі як: сторінки, які ідентифікують та цькують приватних осіб, мають зображення чи відеозаписи актів фізичного насильства, обмінюються особистою інформацією певної особи для шантажу чи переслідування тощо. Якщо контент був видалений помилково, користувач має право відправити апеляцію щодо видалення контенту або аккаунта через Центр підтримки.

2) Twitter

Twitter закликає людей повідомляти про акаунти, які порушують їхні правила. Це можна зробити через спеціальну сторінку в Центрі підтримки або через керуванням твітів, вибравши опцію «Поскаржитися на твіт». Скарги на контент допоможуть краще захистити користувачів на певних платформах. Якщо ви побачите твіт чи відповідь, яка вам не подобається, ви можете відписатися від цієї особи. Якщо вона продовжить вас турбувати, ви можете заблокувати користувача. Однак, якщо ви і надалі отримуватимете небажані повідомлення чи погрози, ви можете повідомити про це безпосередньо в підтримку Twitter.

3) Youtube

Команда YouTube запустила кампанії Voice4Good в підтримку позитивного діалогу в інтернеті, щоб показати, що це – платформа для втілення своїх ідей та ведення цікавиї дискусій і не місце для негативу. Для проекту залучили українських влогерів, які розказуватимуть в своїх відео, як боротися з негативом в коментарях і житті, як відрізнити булінг від конструктивної критики, і як не опустити руки початківцю ютуберу і продовжувати займатися улюбленою справою.

4) Ігрові платформи

На більшості популярних ігрових платформ також існують певні обмеження, які дозволяють протидіяти булінгу. Крім того, що гравці можуть самостійно повідомити про порушення, існує ще й автоматизоване виявлення образливої поведінки. До порушників можуть застосовуватися тимчасові або постійні обмеження і видалення з платформи.

Список використованих джерел:

1. Security Bloggers Network syndicated blog from Managed Methods by Katie Fritchen.

2. Выступление начальника информационно-компьютерного отдела департамента образования администрации Владимирской области В. А. Власенко на межрегиональном семинаре «Информационная безопасность несовершеннолетних: диалог государства и гражданского общества», 30 января 2013 года.

3. Солдатова Г. У., Феномены традиционного буллинга и кибербуллинга: сходства и различия. Материал международной конференции, 14–17 февраля 2018.

Ключові слова: кібербулінг, соціальні мережі, підлітки, особиста інформація.

Ключевые слова: кибербуллинг, социальные сети, подростки, личная информация.

Key words: cybersecurity, social networking sites, teenagers, personal information.

Научний керівник: *к.ю.н. доцент Дикий О. В.*

Брусиловский Константин Андреевич
Национальный университет «Одесская юридическая академия»,
студент 2-го курса факультета кибербезопасности
и информационных технологий

СПЕЦИФИКА РАЗРАБОТКИ «СТРАТЕГИЧЕСКИХ ИГР»

Понятие стратегической игры – это один из самых популярных жанров в игровой индустрии. С развитием программного

обеспечения, специализирующегося на разработке игр, стало возможным создавать их без написания кода. С одной стороны, это ограничивает действия разработчиков предоставляемым в соответствующих игровых конструкторах функционалом, а с другой, даёт возможность получить базовые навыки в создании игрового проекта даже не программистам. Понимание игровой конструкции значительно облегчает переход на уровень проектирования игрового процесса, когда возникает желание разработки и реализации собственного игрового проекта.

Разработка игрового стратегического проекта – это трудоемкий процесс, требующий, помимо фантазии и желания авторов соответствующей идеи, профессиональных навыков целой команды разработчиков, в которой есть специалисты в области написания игрового скрипта, создания графического дизайна игры (гейм-дизайнеры и художники), QA специалисты и др.

Начинается все с формирования идеи, поиска стратегии, предварительного анализа рынка, поиск и формирования команды. Детальная разработка концепта игры может потребовать значительного времени. При этом надо определить, является ли данная идея осуществимой, так как на ее создание влияют некоторые факторы. Первый фактор – достаточно ли знаний про основные средства разработки. Второй фактор – создание плана реализации и обсуждение его с командой для полноценного понимания объемов работы, предстоящей перед каждым участником команды. На этапе препродакшн составляется документация (концепт, feature-list, art-style doc, бюджет, бизнес-план, проектный план, запланированными заданиями для каждого участника команды разработчиков, построение процессов для согласования работы команды) [1]. Самый незаменимый документ – это концепт, который позже «перерастает» в геймдизайн-документ [2]. Только после его разработки можно переходить к этапу разработки визуальной части игры.

Дизайнеры стратегии определяют вместе со всей командой разработчиков стиль графической визуализации. Распространенно при разработке стратегий используют векторную графику, реализуемую с помощью математических примитивов (точек, отрезков, прямых, кривых и т.д.). Популярным программным обеспечением, используемым при создании векторных изображений, является Adobe Illustrator, благодаря удобному интерфейсу и легкости в изучении. Кроме этого, зачастую для реализации векторной графики используют программу Paint Tool Sai, не уступающую по популярности в использовании AI. Для детальной прорисовки основных объектов стратегии используют пиксельную графику – форму визуализации на уровне пикселей в виде двухмерных наборов пикселей для элементов цифрового изображения. Для реализации пиксельной графики профессионалы используют чаще всего Aseprite, Pyxel Edit и др. [3]

После реализации графической части необходимо создать звуковое сопровождение к игре (звуковые эффекты, музыка, а также при необходимости озвучка), поскольку это добавит игре эмоциональный окрас. Готовые звуки можно найти на различных онлайн источниках или же создать их с помощью специализированных редакторов звуков Bfxr и Diforb, популярных благодаря большому функционалу реализации звуковых эффектов и удобному интерфейсу.

Важным аспектом при создании стратегии является решение о том, будет ли игра использовать искусственный интеллект (ИИ), поскольку он позволит существенно увеличить количество возможных сценариев и сделает возможным мультипользовательскую игру с виртуальными игроками. Примерами популярных стратегических игр, использующих ИИ, являются Warcraft, StarCraft, Command & Conquer.

При разработке игры стратегического жанра важно грамотно обозначить возможные пошаговые действия будущих игроков в рамках четко выделенного (или неопределенного) промежутка времени на один ход (в зависимости от

сложности игры), так как стратегические игры требуют детальной проработки, а жанр стратегической игры предусматривает разработку тактики сражения с противником, накопление и использование ресурсов игры [3].

Ключевым моментом проектирования стратегии является выбор игрового движка, поскольку он него зависит «механика» игры, темпы и последовательность воспроизведения анимации и звукового сопровождения. Использование готового игрового движка существенно упрощает разработку игрового контента, удешевляет их производство и сокращает время до запуска новых игр.

Из наиболее популярных движков можно выделить [4]:

– Unity 3D – пожалуй, один из самых популярных среди движков разработчиков-новичков, благодаря своей легкости в использовании, выгодной лицензионной политике, совместимости с разными платформами и операционными системами, быстрому отлавливанию ошибок. По сути, Unity 3D можно назвать игровым конструктором с компонентно-ориентированным подходом, поскольку он позволяет конструировать компьютерные игры максимально просто и комфортно, создавая объекты (героев игры) и различные компоненты (визуальное отображение персонажей и способы управления ими), рисовать карты и расставлять объекты в реальном времени, создавать сложные анимации и коллизии между объектами, тестировать их. При всех своих достоинствах проблемой движка Unity является медлительность, а созданные с его помощью стратегии довольно «тяжеловесны», что особенно критично для мобильных платформ. Для оптимизации используемой памяти и расширения функционала игровых объектов целесообразно озаботиться разработкой на C# своих скриптов и внедрением их в проект;

– Unreal Engine – популярный среди профессионалов движок с широким ассортиментом инструментов и плагинов, совместимостью с различными платформами. Движок содержит множество инструментов, которые облегчают разработку

трехмерных AAA-проектов, особенно шутеров и приключенческих экшенов, поддерживает множество форматов текстур, позволяет изменять объекты в реальном времени, выбирать источники освещения, добавлять различные эффекты для достоверной анимации персонажей при разработке игр, а открытый исходный код на языке C++ движка дает возможность вносить в него изменения при необходимости [5]. К минусам Unreal Engine можно отнести некоторую сложность к привыканию в использовании инструментов из-за специфической эргономичности интерфейса. Кроме того, для того чтобы добиться плавности картинки в Unreal Engine надо потрудиться над оптимизацией производительности;

– GameMaker Studio – кроссплатформенный движок для создания 2D игр с применением собственных графических объектов. Несмотря на возможность работы с 3D, в GameMaker она неудобна. Благодаря простоте и удобству в освоении, предпочтение этому движку в основном отдают начинающие разработчики;

– CryEngine 3 – движок с продвинутыми возможностями по разработке видеоигр и поддержкой передовых технологий, включая DirectX 12, Vulkan API, VR, написание скриптов на C#, попиксельное освещение в реальном времени, карты отражений, детализированные текстуры, туман, поверхности с бликами, реалистичную физику, продвинутую анимацию и многое, многое другое. CryEngine позволяет создавать игры с фотореалистичной графикой, превосходящие по качеству картинки игр на Unreal Engine 4 или Unity [6]. Недостатками движка являются отсутствие хорошей техподдержки (поскольку движок в игровой индустрии относительно недавно), определённая сложность в освоении и работе с ним, ограничения в разработке сетевых игр.

Разработка игры (продакшн) – это самый длинный этап, на котором в полном объёме реализуется возможностями и фичи игры. Результатом данного этапа является версия игры, готовая к демонстрации пользователям.

Финальный этап разработки (релиз) включает тестирование и шлифование игры, оптимизацию под различные устройства, версии игры для различных платформ. Результатом данного этапа является публикация финальной версии игры в магазинах. После этого часть команды остается следить за техподдержкой игры и отзывами игроков для отлавливания возможных багов, а также формирования списка пожеланий и идей для дальнейших обновлений.

Список использованных источников:

1. Высотина А. Каков процесс создания игры. URL: https://yandex.ru/q/question/games/privet_kto_mozhet_opisat_protsess_igry_ot_f26eb748/?utm_source=yandex&utm_medium=wizard&answer_id=14b19138–826c-49cc-a85c-630aa8118a0b#14b19138–826c-49cc-a85c-630aa8118a0b (дата обращения 05.11.2020).

2. Создание игры от идеи до продвижения после релиза. URL: https://tproger.ru/blogs/game-development-from-idea-to-post-release/ (дата обращения 05.11.2020).

3. Создание стратегической. URL: https://pikabu.ru/story/sozdanie_strategicheskoy_igryi_5856851 (дата обращения 05.11.2020).

4. Топ-10 игровых движков. URL: https://zen.yandex.ru/media/id/5dbd35d495aa9f00b1854aa6/top10-igrovyh-dvijkov-5dc9d23b4eb2430b60f6d40a (дата обращения 05.11.2020).

5. Движок Unity – особенности, преимущества и недостатки. URL: https://cubiq.ru/dvizhok-unity/ (дата обращения 05.11.2020).

6. Движок CryEngine – особенности, преимущества и недостатки. URL: https://cubiq.ru/dvizhok-cryengine/ (дата обращения 05.11.2020).

Ключові слова: етапи розробки ігор, ігровий движок, стратегія.
Ключевые слова: этапы разработки игр, игровой движок, стратегия.
Keywords: stages of game development, game engine, strategy.

Науковий керівник: *к.т.н., доц. Трофименко О. Г.*

Борумбєй Богдан Ігорович
Національний університет «Одеська юридична академія»,
студент 3-го курсу факультету кібербезпеки
та інформаційних технологій

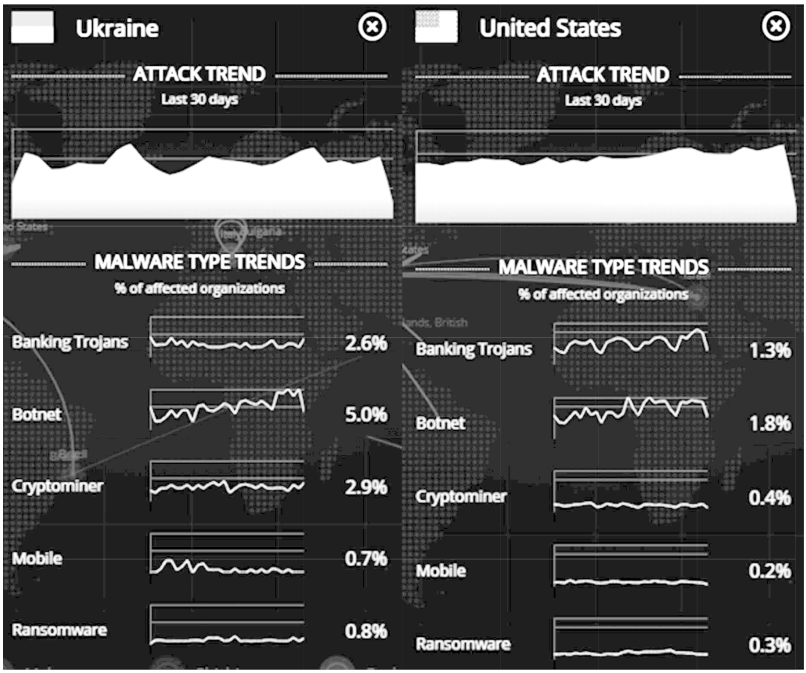
Борумбєй Тетяна Ігорівна
Національний університет «Одеська юридична академія»,
студентка 4-го курсу факультету кібербезпеки
та інформаційних технологій

ПРОБЛЕМЫ КИБЕРПРОСТРАНСТВА В УКРАИНЕ

Термин «диджитализация» начали употреблять еще в 2019 году. Он означает автоматизацию всех бытовых процессов, используя интернет-технологии. С каждым днем появляются новые идеи, разрабатываются платформы, которые автоматизируют процессы, требовавшие к себе особого внимания. Сейчас достаточно зайти на определенную платформу и решить возникшую проблему за считанные секунды. Но так ли все просто? Каждая из платформ требует от пользователя регистрации или даже верификации, соответственно данные пользователя сохраняются в базе данных для дальнейшей авторизации. Данные требуют некой конфиденциальности от вторых и в особенности от третьих лиц. Этому посвящен целый раздел в конвенции об обеспечении международной информационной безопасности. Но на сколько хороша информационная безопасность платформ, которые мы используем на территории Украины?

Анализируя статистику службы безопасности Украины можно сказать, что с начала 2020 года было заблокировано 2,5 тысячи веб-ресурсов, которые использовались в преступных целях, и деятельность 20 хакерских группировок [3]. Также СБУ нейтрализовала 460 киберинцидентов и кибератак на органы государственной власти и критически важные объекты инфраструктуры. [3] Не считая официально

зарегистрированные кибератаки, описанные выше инциденты можна умножить приблизительно в 2 раза. В первую очередь приведенные данные говорят о том, что информационная безопасность и киберпространство Украины, мало защищённые от кибератак. По статистике интерактивной карты киберугроз ThreatCloud World Cyber Threat Map, созданной компанией Check Point, за последний месяц Украина превосходи по количеству кибератак даже США (Схема 1). Система постоянно анализирует сайты в сети на наличие ботов, каждый день обнаруживая, в среднем, более миллиона типов вредоносных программ. Если учитывать то, что представленная платформа регистрирует явна не все кибератаки, данные показатели являются приблизительными и фактически могут быть увеличены в несколько раз.



(Схема 1) [1]

Проблемы уязвимости большинства платформ в частности на территории Украины связаны с отсутствием проверки на проникновение коммерческих проектов перед выгрузкой их в сеть. Многие компании очень часто отказываются привлекать к разработке «продукта» специалистов, что чревато для пользователей и в особенности для компаний, ведь в этом случае страдает экономическая составляющая компаний и качество разработки. Кроме этого уязвимостям способствует исходный код платформы и использование устаревших технологий в особенности в Украине, так как найти разработчика, который использует старые технологии, намного дешевле, чем нанимать квалифицированного специалиста.

Огромное количество процессов автоматизируется и можно только представить сколько конфиденциальной информации «сливается» в сеть. Поэтому внедрение таких обязательств как тестирование платформ на проникновение следует применять как обязательную составляющею информационной безопасности. Уязвимости киберпространства можно разделить на несколько видов:

1. Компьютерная неграмотность. Связана с большим количеством кибермошенников которые пользуются неграмотностью людей с целью получения от потенциальной цели информации или денежного вознаграждения. Как пример, к данной категории можно отнести интернет рассылки. Так для получения доступа к системе компании киберпреступнику достаточно сделать рассылку с вредоносной ссылкой или какой-либо вирусной программой на почты всех сотрудников, притворяясь, скажем, налоговой службой. Вероятность, что один из 100 сотрудников нажмет на эту ссылку, достаточно велика и киберпреступнику уже не составит труда получить желаемую информацию.

2. Присутствие популярных уязвимостей, включая:

• IDOR (Insecure Direct Object Reference, небезопасные прямые ссылки на объекты) – уязвимость, которая позволяет получить несанкционированный доступ к веб-страницам или

файлам. Самый распространенный случай IDOR – когда злоумышленник перебирает предсказуемый идентификатор и получает доступ к чужим данным.

• XSS – Cross Site Scripting (межсайтовое выполнение сценариев). Когда происходит XSS-атака, в веб-страницу встраивается вредоносный код. И как только посетитель сайта откроет эту страницу, начнёт выполняться какой-либо неприятный сценарий. Чаще всего под вредоносным кодом подразумевается внедрение html-тегов или скриптов на JavaScript.

• SQL-инъекция – это атака, направленная на сайт или веб-приложение, в ходе которой пользователь может обходным путём получить информацию из базы данных с помощью SQL-запросов. В случае успешной атаки пользовательские данные интерпретируются как часть SQL-кода запроса, и таким образом изменяется его логика.

Решение проблем, связанных с уязвимым киберпространством Украины можно решить, используя различные нововведения в нынешнею систему. В качестве распространения информации пользователи, развивая свои знания в сфере информационной безопасности и компьютерной грамотности, могут использовать средства массовой информации, узнавая про основы социальной инженерии, веб-угрозы, различные киберприступления такие как: кардинг, фишинг, методы шифрования информации и данных и т.д. Также можно поспособствовать полной переквалификации преподавательского состава всех высших учебных заведений для обеспечения качественного образования студентов и выпуска квалифицированных кадров. Еще одним решением проблемы уязвимости киберпространства является использование и внедрение новых технологий для разработки платформ. Важным аспектом для предотвращения похищения информации является введение неких «правил» в правовом поле. В Украине реализация информационной защиты с помощью законодательства находится на достаточно низком уровне. Именно данные решения поспособствуют и организуют максимальную безопасность киберпространства.

Подводя итоги, можно сказать, что на данном этапе так называемая «диджитализация» важный процесс, однако крайне незащищенный, ведь это не просто автоматизация привычных человеку действий. Для правильного использования информации защиты данных пользователю необходима защита на уровне закона, но кроме этого знание и понимание процессов, развитие компьютерной и медиаграмотности.

Список використаних джерел:

1. MAP. ThreatCloud World Cyber Threat Map [Електронний ресурс]. Режим доступу до ресурсу: https://threatmap.checkpoint.com/.

2. Артём Мышенков. Популярные уязвимости сайтов: чем опасны и как их избежать [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://cmsmagazine.ru/journal/items-popular-site-vulnerabilities/.

3. Кулеш С. Статистика: кількість кібератак за 2020 рік «СБУ: У 2020 році було нейтралізовано 20 хакерських угруповань і 460 кібератак на критично важливі об'єкти» [Електронний ресурс] / С. Кулеш. – 2020. – Режим доступу до ресурсу: https://itc.ua/news/sbu-v-2020-godu-bylo-nejtralizovano-20-hakerskih-gruppirovok-i-460-kiberatak-na-kriticheski-vazhnye-obekty/.

Ключові слова: уразливості кіберпростору, інформаційна безпека, кібернетична безпека, застарілі технології, уразливості, уразливості при веб-розробці, уразливості інформаційної безпеки, захист від вразливостей.

Ключевые слова: уязвимости киберпространства, информационная безопасность, кибернетическая безопасность, устаревшие технологии, уязвимости, уязвимости при веб-разработке, уязвимости информационной безопасности, защита от уязвимостей.

Keywords: cyberspace vulnerabilities, information security, cyber security, outdated technologies, vulnerabilities, vulnerabilities in web development, information security vulnerabilities, protection against vulnerabilities.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Колосенко Андрій Андрійович,
Національний університет «Одеська юридична академія»
студент 3-го курсу факультету кібербезпеки
та інформаційних технологій

Коляда Анастасія Миколаївна,
Національний університет «Одеська юридична академія» студентки
4-го курсу факультету кібербезпеки та інформаційних технологій

Сарокіна Владислава Володимирівна
Національний університет «Одеська юридична академія»
студентки 4-го курсу факультету кібербезпеки
та інформаційних технологій

РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД

Серед сучасних тенденцій розвитку суспільства значної уваги заслуговує глобальна інформатизація практично всіх сфер життєдіяльності людини, включаючи економіку, державне управління, науку, мистецтво.

Перетворення суспільства в інформаційне змінило статус інформації в цілому. На сьогодні вона може бути як засобом забезпечення безпеки, так і загрозою та небезпекою. До прикладу, позитивним моментом можна вважати те, що автоматизація процесів документообігу значно спрощує дану процедуру і пришвидшує її, а застосування банківських карток звільняє людей від необхідності користуватися готівкою. Та в той же час такий стрімкий стрибок технічного рівню стає поштовхом для появи значної кількості проблем. Для реалізації можливостей комп'ютеризації необхідна прив'язка приватної інформації до рахунків чи особистих кабінетів. І саме з цього починають проявлятись усі негативні сторони медалі під назвою «діджиталізація».

Усі незаконні дії, які певним чином посягають на конфіденційність, цілісність чи збереженість інформації в інформаційних системах і мережах та які носять корисливий і

хуліганський характер, прийнято вважати кіберзлочинами. До основних видів таких можна віднести розповсюдження шкідливого програмного забезпечення, крадіжка номерів кредитних карт і банківських рахунків, злом паролів, порушення авторських прав. Крім того, варто зазначити, що кількість подібних злочинів набирає обертів і зростає щороку, оскільки для скоєння злочинів такого виду не потрібне залучення значних фізичних чи фінансових витрат, і натомість реалізація даних дій приносить кіберзлочинцям величезних прибутків. Навіть не зважаючи на той факт, що рівень комп'ютерної безпеки підвищується і регулярно удосконалюється, все ж знаходяться особи, яким під силу оминути і обманути систему. Саме тому кіберзлочини вимагають оперативного реагування і кваліфікованого розслідування [2].

Важливо відмітити, що сучасний кіберпростір не обмежений ніякими категорійними рамками (часу, простору і т.д.). Тож, хакерські атаки можуть бути здійсненні з будь-якої точки світу на будь-який об'єкт. Саме тому слід пам'ятати, що дана проблема не має локального характеру, а набуває глобальних масштабів міжнародного рівня.

У зв'язку з цим виникає потреба у розробці ефективної системи кібербезпеки, яка могла би захистити інтереси країни та вберегти її громадян від злочинних посягань.

В Україні питаннями кібербезпеки та запобіганням кіберзлочинності повинна займатись Кіберполіція України. Проте існує значна проблема, яка полягає у категорії справ, які дійсно потрапляють під розгляд Кіберполіції. Логічним стане припущення, що до таких мали би відноситись абсолютно усі кіберзлочини, проте фактично працює зовсім інакша схема, відповідно до якої Кіберполіція, не маючи достатнього кадрового забезпечення, зосереджує свою діяльність переважно на найгучніших справах (до прикладу, з обігом великих грошових сум), передаючи в той час Національній Поліції всі інші «незначні» справи. Проте, Національна Поліція не вважає справи, пов'язані з кіберзлочинами, перспективними, тому і не спрямовує свої основні ресурси на розслідування таких справ. Крім

того, в Україні не існує уніфікованої бази, де було би закріплено ключові поняття та терміни, не розроблено криміналістичної техніки і тактики, що допомогло би співробітникам Кіберполіції ефективно здійснювати процедуру розслідування кіберзлочинів.

Говорячи про те, хто здійснює розслідування кіберзлочинів на міжнародному рівні, варто згадати ряд інституцій, які безпосередньо залучені до даної діяльності. Так, органи кримінального судочинства займаються питанням запобігання кіберзлочинів та їх розслідуванням, моніторингу та переслідування кіберзлочинців. Залежно від країни, орган кримінального судочинства беруть до розгляду усі справи, пов'язані з кіберзлочинністю. До прикладу, у США залежно від конкретного випадку, кіберзлочини можуть розслідуватись ФБР, Секретною служба США, Центром подання скарг на злочини в Інтернеті, Службою поштової інспекції США або Федеральною торговою комісією [3].

Наступним суб'єктом здійснення розслідування кіберзлочинів виступають органи національної безпеки. В різних країнах залучаються різні відомства даного типу, проте об'єктом, над яким вони працюють зазвичай виступають кіберзлочини. Наприклад, розвідувальне відомство повинно здійснювати розслідування кіберзлочинів, які мають певний зв'язок з їхньою організацією, наприклад, ті, чия діяльність спрямована проти його[1] мереж, співробітників або даних; або ж були виконані розвідниками.

Приватні охоронні органи також мають важливе значення у боротьбі з кіберзлочинністю, особливо під час розслідування. У той час як уряди та національні агентства управляють власними мережами, серверами та додатками, приватні охоронні органи складають лише незначну частину величезної інфраструктури та коду, що постійно використовується приватними компаніями, проектами, організаціями та приватними особами по всьому світу. З огляду на це, не дивно, що приватні

[1] розвідувального відомства

експерти з кібербезпеки, дослідницькі компанії та сині команди[1] відіграють важливу роль у питанні запобігання, моніторингу, пом'якшення та розслідування будь-якого виду злочинів кібербезпеки проти мереж, систем або даних, що працюють на сторонні приватні центри даних, мережі, сервери або звичайні домашні комп'ютери. Широкий спектр кіберзлочинів, розслідуваних приватними агентствами, не знає меж і включає, але не обмежується, зламом, деформацією, розповсюдженням вірусів та шкідливих програм, DDoS-атаками, інтернет-шахрайством, викраденням особистих даних та соціальною інженерією [1].

Аналізуючи все вищезгадане, варто відмітити, що питання забезпечення кібербезпеки та реалізація розслідування кіберзлочинів на теренах України покладено на Кіберполіцію. Проте, завдяки недосконалій системі визначення та реагування на кіберзлочини, функції, передбачені до виконання Кіберполіцією, здійснюються не повною мірою та ще і з делегуванням певних функцій та справ Національній поліції. Проте, міжнародна практика, сформована на основі досвіду США, показує, що варіант залучення більшої кількості діючих і компетентних органів-суб'єктів з розслідування кіберзлочинів, дійсно допомагає вивести процес передбачення, виявлення та розкриття злочинів у сфері інформаційної безпеки та може бути здійснено на достатньому рівні, необхідному для зменшення кількості кіберзлочинів.

Отже, розслідування кіберзлочинів в Україні та в інших провідних країнах світу значно різниться, а стан розвитку боротьби України проти кіберзлочинів все ж залишає бажати кращого. Саме тому, дані факти повинні слугувати черговими поштовхами до активного перейняття світового досвіду на державному рівні, з метою подальшого підвищення рівня протидії та розслідування кіберзлочинів.

---

[1] Синя команда – *(інф.безпека)* – внутрішньокорпоративна група спеціалістів із забезпечення безпеки, яка захищає компанію від справжніх зловмисників.

Список використаних джерел:

1. Ануфрієв М. І. Міжнародно-правові засади співробітництва у боротьбі з кіберзлочинами / М. І. Ануфрієв, О. М. Кісілевич-Чорнойван // Наше право. – 2017. – № 3. – С. 45–50. – [Електронний ресурс] – Режим доступу до ресурсу: http://nbuv.gov.ua/UJRN/Nashp_2017_3_11.

2. Кравцова М. А. Понятие киберпреступности и ее признаки / М. А. Кравцова // Часопис Київського університету права. – 2015. – № 2. – С. 320–324

3. Сироїд Т. Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю. / Т. Л. Сироїд // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. – Харків: Права людини, 2014. – С. 194–196.

Ключові слова: кіберзлочини, розслідування, міжнародний досвід.

Ключевые слова: киберпреступления, расследование, международный опыт.

Keywords: cybercrime, investigation, experience different country on the international level.

Науковий керівник: *к.т.н., доц. Бойко В. Д.*

Раєв Олександр Діомидович
Національний університет «Одеська юридична академія»
студент 3-го курсу факультету кібербезпеки
та інформаційних технологій

ДОСЛІДЖЕННЯ ТА БОРОТЬБА З СКАМОМ НА ПЛАТФОРМІ STEAM

Скам – одна з найпопулярніших на сьогодні шахрайських схем, що дозволяє виманювати у користувачів великі суми грошей. Суть скам-процесу полягає у розсилці поштових листів, у яких повідомляється заздалегідь неправдива інформація [1].

Скам на платформі Steam одна з найбільших проблем даної платформи, так як кількість людей, які займаються шахрайством зростає щодня, тому що не потрібно мати особливих навичок у програмуванні або багато коштів для розвитку цього процесу. Проте, такі користувачі-скамери не несуть занадто багато небезпеки, тому що акаунт в Steam можна заблокувати за скаргами інших користувачів.

Більшою загрозою для користувачів платформи є групи шахраїв із різними заданими цілями, які вони структуровано виконують, наприклад:

Скам-програміст – це одна з головних фігур групи, що займається написанням програмного забезпечення для користувачів-скамерів, яке спрощує та пришвидшує їхню незаконну роботу. Програмне забезпечення для скам-процесу повинне містити у собі такі пункти як:

– Пошук «клієнта», тобто відсіювання усіх неплатоспроможних користувачів;

– Забезпечення стану безпеки, а саме Proxy чи VPN;

– Способи отримування особистих даних – це може бути як фальшивий веб-сайт, так і захоплення клавіатури пристрою та т.і.

Скамери – це шахраї, що займаються розсилкою скам-повідомлень користувачам платформи, ними також використовуються соціальна інженерія та програмне забезпечення.

Більшість роботи користувачів-скамерів – це соціальна інженерія, а головне для шахрая, щоб користувач за вказівкою виконував їхні вимоги, а саме: завантажив одну із шкідливих програм, або оприлюднив свої особисті дані.

До незаконного процесу долучаються шахраї, які роблять фейк-акаунти для користувачів-скамерів – тому що дуже часто їхні акаунти блокують, а так як акаунт повинен бути схожим на «живий», необхідно використовувати велику кількість акаунтів хибного призначення, щоб було простіше увійти у довіру до користувача Steam та надалі керувати його обліковим записом.

Більшість такої роботи виконується за допомогою спеціальних користувачів-ботів в Steam, які роблять загальну видимість «живого» облікового запису (кількість проведених годин у грі, або геймерський рівень ігрового акаунта).

Одна з найпопулярніших шахрайських схем користувачів-скамерів – це примусити середньостатичного користувача платформи Steam відвідати замаскований хибний веб-сайт, щоб він ввів свої особисті данні від власного акаунта, що дає змогу втілити незаконне проникнення у цей акаунт (але навіть в такій ситуації шахраї не мають змогу втілити щось невідворотне, тому що у цієї структури немає прав Адміністратора над обліковим записом), наступним кроком є те, що шахраї очікують вдалої нагоди отримати більше прав над акаунтом, це займає деякий проміжок часу, наприклад, місяць. Через місяць користувач платформи може забути про прихованого користувача-скамера, у якого збільшується кількість прав над акаунтом, що дає йому змогу змінювати зовнішній вигляд акаунта, пересилати особисті файли (ігрові речі) з акаунта, але все знову може відбутися тільки з дозволу власника, який вимагається незаконним шляхом, обманом. Потім користувач-скамер може змінити зовнішній вигляд акаунта звичайного користувача і написати, що його обліковий запис зникає через деякий проміжок часу, наприклад тому, що на цей акаунт поскаржилися, надалі шахрай рекомендує «клієнту» здійснити продаж своїх особистих файлів (ігрових речей) чи надіслати їх іншому користувачу, далі спрацьовує інтернет-перехоплення файлів, користувач платформи думає, що файли надходять до адресата, але насправді процес проходить у такому плані, що користувач платформи дозволяє шахраю забрати собі файли (ігрове майно) без прямого дозволу власника.

При нападі шахраїв на платформі Steam необхідно дотримуватися певних правил користування своїм акаунтом, а саме:

– Перевіряти всі веб-сайти, які ви відвідували (приділяти особливу увагу веб-адресі, тому що шахраї можуть повність скопіювати зовнішній вигляд платформи, окрім деяких відмінностей);

– Нікому не повідомляти свої особисті дані, навіть якщо спілкування йдеться з довіреною особою;

– Не завантажувати підозрілі чи неперевірені файли.

У випадку, якщо вас намагалися ввести в оману, потрібно поскаржитися Адміністрації платформи та спробувати максимально довго затримувати співбесідою шахрая, щоб користувач-скамер витратив більше часу на розмову з вами та втратив пильність. Завдяки затримці часу, Адміністрація швидше знайде та заблокує підозрілий акаунт.

Якщо дотримуватись усіх правил, то є великий шанс, що скам-процес для користувача платформи пройде без незаконних витрат та не відтвориться знову.

Список використовуваних джерел:

1. itua.info [Електронний ресурс] – Режим доступу до ресурсу: https://itua.info/software/27672.html.

Ключові слова: Скам, акаунт, користувач, Steam.
Ключевые слова: Скам, аккаунт, пользователь, Steam.
Keywords: Scam, account, user, Steam.

Науковий керівник: *д. ф-м. н., д.ю.н., професор Василенко М. Д.*

Стратієвська Аліна Олександрівна
Національний університет «Одеська юридична академія»
студентка 2-го курсу, факультету кібербезпеки
та інформаційних технологій

БІЛИЙ ХАКІНГ ЯК НОВИЙ ІНСТИТУТ ДЛЯ ПІДТРИМКИ КІБЕРБЕЗПЕКИ

Актуальність розглядаємої теми полягає у висвітленні інформації по білий хакінг як засіб підтримки високого рівня кібербезпеки з метою формування сучасного інформаційного громадського суспільства. Збільшення рівня кіберзлочинності, реалізації засобів та методів кібертероризму у багатьох сучас-

них конфліктах, потребує формування структури дотримання безпеки України у кіберпросторі.

Варто вказати, що хакер це та людина, яка намагається одержати заборонений доступ до комп'ютерних мереж та програм, зазвичай з метою отримання конфіденційної інформації. Хакерів також називають досвідченими комп'ютерними програмістами або користувачами, які зламують програми.

Щодо білого хакінгу, то це один із міжнародних сучасних трендів кібербезпеки. Все це проявляється через власну раціональність та ефективність. Наприклад, такі глобальні системи як Google, Facebook, Amazon – розпочали свої власні програми зі взаємної роботи з чесними хакерами. Щодо України, то дану практику мають тільки конкретні приватні фірми.

Сьогодні в умовах швидкого вдосконалення ІТ-технологій на міжнародній арені, проблеми кібербезпеки та кіберзахисту відносяться не лише до органів державної влади, однак і до всіх громадян нашої країни, котрі мають смартфони або користуються сучасним комп'ютером чи планшетом. Сьогодні ринок інтернет послуг та сервісів у галузі кібербезпеки має бути загально відкритим для приватного сектору в межах державно-приватного партнерства.

Яскравим прикладом сучасної боротьби з кіберзлочинністю, є те, що органи досудового розслідування визначили, що «Єдина судова інформаційно-телекомунікаційна система» не відповідає сучасним вимогам Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», постанови КМУ від 12.04.2002 № 522 «Про затвердження порядку підключення до глобальних мереж передачі даних», НД ТЗІ 2.5–010–03 «Вимоги до захисту інформації WEB сторінки від несанкціонованого доступу», прийнятих наказом ДСТСЗІ СБ України від 02.04.2003 № 33, та має дуже багато чутливих місць для несанкціонованого доступу [1; 2]. Оскільки правові визначені вимоги безпеки роботи інформаційно-телекомунікаційних систем та ЄСІТС не були прийняті відповідно до сучасних вимог, це призвело до блокування, знищення

та виведення з ладу у період з 24.12.2018 по 25.01.2019 судової системи України.

Проте, на сьогоднішній день з функціонування сучасних технологій та комп'ютерних систем кількість різновидів хакерів збільшилась. У ситуації коли хакер стає на неправову дорогу – він стає кракером (або як ще називають зломщиком, людиною, котра вривається в чужу комп'ютерну систему, через електронні мережі, визначає паролі та офіційні ключі комп'ютерних систем або іншим чином навмисно ламає комп'ютерну безпеку [3]. Проте, функціонування всіх хакерів та кракерів є схожим за методами і завданнями їх діяльності, однак існує серйозна розбіжність у меті їх функціонування. Сучасні хакери застосовують уразливість комп'ютерних структур для реалізації нападів на дані системи. Головна мета і завдання хакера – використати комп'ютер для підбору слабких точок в структурі безпеки та проінформувати розробників даної структури про це, а також визначити конкретні передумови та вимоги відносно рівня безпеки інформаційних структур [4].

Тому, у багатьох державах здійснюється легалізація праці хакерів. Їх усе частіше називають «білими» хакерами, які працюють на великі організації та державні органи влади. Наприклад, Британська секретна служба здійснює підбір на роботу молодих хакерів-самоучок, оформивши, як повідомляє інтернет-видання «Die Welt», інтернет-змагання, переможець якого має шанс одержати посаду в секретній службі. Функціонування даних осіб, котрі отримали роботу, полягає у цілеспрямованому встановленню дій, які хоч і мають ознаки протиправного діяння, однак учасники, котрі їх вчиняють, не підлягатимуть кримінальному переслідуванню та покаранню. Тому, залишається абсолютна більшість потенційних спеціалістів, котрі не залучаються до схожої законної роботи та прагнуть заробити гроші на цій неправовій діяльності.

Отже, на сьогодні визначену особу молодого хакера описує наявність активної та цілеспрямованої життєвої позиції, оригінальність думок та власної поведінки, акуратність, уважність,

зосередженість уваги на баченні результату, передбаченні та керівництвом управлінні процесами, їх дії дуже обережні та супроводжуються відмінним маскуванням.

Список використаних джерел:

1. Закон України Про захист інформації в інформаційно-телекомунікаційних системах від 094.07.2020 року. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.
2. Постанова КМУ від 12.04.2002 року № 522 Про затвердження Порядку підключення до глобальних мереж передачі даних. URL: https://zakon.rada.gov.ua/laws/show/522–2002-п#Text.
3. Анализ представлений о мотивации хакеров: [Електронний ресурс]. – Режим доступу: http://www.mytests.ru /articles/353.
4. Біленчук П. Д. Криміналістична характеристика способів скоєння комп'ютерних злочинів / П. Д. Біленчук // Наукові розробки академії по вдосконаленню практичної діяльності та підготовки кадрів органів внутрішніх справ. – К., 2017. – 271 с.

Ключові слова: хакінг, хакер, кракери, мережа, дані, кібербезпека.

Ключевие слова: хакинг, хакер, кракеры, сеть, данные, кибербезопасность.

Keywords: hacking, hacker, crackers, network, data, cybersecurity.

Науковий керівник: *доцент Задерейко О. В.*

Титиевский Виталий Олегович
Национальный университет «Одесская юридическая академия»
студент 1-го курса факультета кибербезопасности и информационных технологий

ПЕРСПЕКТИВЫ РАЗВИТИЯ DATA SCIENCE В УКРАИНЕ

Информационные технологии развиваются с невероятной скоростью, лишь за последние 20 лет всё изменилось до неузнаваемости. Ничто не стоит на месте, прямо сейчас мы на пороге «IT-революции». С каждым годом появляется всё больше и больше новейших технологий, наук, которые

полностью меняют каждого из нас и нашу жизнь. Одна из таких наук – Data Science.

Data Science – наука, которая изучает анализ, обработку большого количества данных с помощью программного обеспечения. Специалист по обработке данных (Data Scientist) представляет собой сотрудника, который работает с огромным объёмом неструктурированных данных, находит с этого объёма полезную информацию и делает прогнозы. Современному бизнесу не хватает радикальных прогрессивных решений, именно Data Science может помочь справиться со столь важным решением. Чтобы стать специалистом по обработке данных необходимы знания в области программирования, в частности необходимы навыки программирования в Python или R. Обязательным навыком для специалистов является SQL. Но этого мало, специалист по обработке данных должен уметь здраво проводить анализ информации и соответственно делать правильные выводы. Не менее важно, что специалист по обработке данных это тот человек, который является связующим между всеми участниками проекта. Пока что, Data Science, как сфера деятельности, известна далеко не всем, но эта профессия уже является одной из самых перспективных и высокооплачиваемых.

Термин «Data science» возник лишь во второй половине 20-го века. Впервые он был упомянут в 1974 году в книге Петера Наура, в которой автор указал, что Data Science это отдельная дисциплина. Термин стали широко употреблять через некоторое время – в конце 20-го столетия, этому поспособствовала публикация статьи Bell Labs американского информатика Уильяма Кливленда. Термин набирает популярность и в наше время, этому способствует востребованность и высокая оплата специалистов в этой области.

На сегодняшний день мы заполняем огромное количество данных в интернете: сайты, информация из поисковиков, соц. сети, и т.д. Для хранения этих данных используются специальные базы данных, но данных стало слишком много, чтобы

анализировать их с помощью людей. Наука о данных помогла в решении этой трудной проблемы. Простейшим примером служит всеми известный видео-хостинг «YouTube». Мы часто видим рекламу, в которой мы находим для себя интересную информацию, а всё из-за того, что мы недавно искали подобную информацию в поисковике. Именно таким образом работает технология Data Science не только в «YouTube», а и во многих других видео-хостингах, браузерах, соц. сетях. Наука о данных уже имеет большое значение во всем мире, это подтверждается тем, что зарубежные университеты, школы запускают программы по подготовки сотрудника в этой сфере.

Data Science в Украине имеет огромные перспективы развития. Украинцы уже давно закрепили за собой звание одних из самых квалифицированных специалистов по всему миру. На данный момент в нашей стране насчитывается более 1000 IT-компаний. Многие из них уже сумели проделать огромную работу в сфере Data Science. Наука о данных уже становится неотъемлемой частью бизнес-компаний, её использование даёт преимущество над конкурентами. Некоторые специалисты по обработке данных работают в банках, в одном из украинских банков труд специалиста оценивается от 1500 долларов. Предприниматели всё больше интересуются специалистами Data Science, таким образом специалистов в этой сфере становится соответственно всё больше, ведь спрос порождает предложение. По данным журнала Forbes, предприниматели тратят миллиарды долларов на специалистов в сфере Data Science. Таким образом, можно с уверенностью сделать вывод, что Data Science – непростая, но очень востребованная и высокооплачиваемая профессия.

Для развития науки о данных в Украине организовываются различные конференции, создаются сообщества, также поддерживаются связи с иностранными партнёрами. Это отличный опыт как для нас, так и для иностранных партнёров. Существует большое количество курсов по подготовке Data Scientist, стоит лишь ввести в поисковике 3 заветных

слова: «Курсы Data Science». Мы делаем всё для развития этой сферы в нашей стране, это «отпечатывается» на результатах. Украинские IT-компании начинают набирать популярность на мировом рынке. Отличным примером служит компания Archer Software, которая стала известна на весь мир, после того как их купила крупная американская компания – Cprime. Это отличный шаг, который показывает, что наши компании двигаются в правильном направлении. И это не единственная украинская компания, купленная другой зарубежной компанией. Следовательно, мы можем отметить активное развитие Data Science в нашей стране, украинские специалисты стараются не отставать от зарубежных и даже где-то их превосходить. Именно из-за хорошей квалифицированности так много украинцев работает в известных зарубежных IT-компаниях. С уверенностью могу сказать, что все приложенные усилия никогда не будут напрасны. Я считаю, что Украина имеет шансы стать лидером в сфере Data Science. Всё зависит от каждого из нас.

Список использованных источников:

Ключові слова: наука про дані, компанія, інформаційні технології, партнерство.

Ключевые слова: наука о данных, компания, информационные технологии, партнёрство.

Keywords: data science, company, information technologies, partnership.

Научный руководитель: *д. ф-м. н., д.ю.н., професор Василенко М. Д.*

РОЗДІЛ 4.
ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Виходець Юрій Олександрович
начальник Управління протидії кіберзлочинам в Одеській області
Департаменту кіберполіції Національної поліції України

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ В ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ КАК СТРУКТУРНЫЙ ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ АБСОЛЮТНОЙ БЕЗОПАСНОСТИ

1. На сегодняшний день информационная инфраструктура общества достигла колоссальных размеров. Такая информационная среда представляет собой сегментированную часть мирового механизма взаимодействия человечества. Как и в любом другом направлении, в сфере высокотехнологичных разработок присутствуют сектора, именуемые сегментами среды. К таким сегментам можно отнести: сегмент сотовой и мобильной связи; сегмент разработки настольных и мобильных компьютеров и суперкомпьютеров; сегмент создания и поддержки обслуживающих слоёв информационной инфраструктуры и другие. Для компаний, работающих в вышеупомянутых сегментах информационной среды, приоритетными направлениями развития механизмов абсолютной безопасности являются:

• Создание и тестирование устройств, для достижения безотказной работы;

• Обеспечение информационной безопасности, включая техническую безопасность;

- Разработка технологий комфортной работы.

Сохранение целостности и безопасности информации достигается благодаря информационным технологиям, основанным на протоколировании, а сущность протоколов состоит во внедрении в них различных алгоритмов сильного шифрования.

2. Наиболее ярко необходимость протоколирования просматривается в сегменте сотовой, компьютерной и транспортной инфраструктурах, отвечающих за сохранение и безопасную передачу конфиденциальной и персональной информации.

3. Для достижения наивысшей (абсолютной) безопасности при передаче данных, необходимо совокупное использование криптографических протоколов, а внутри них – симметричных и ассиметричных шифров. Криптографическое протоколирование необходимо в транспортных обслуживающих слоях информационной инфраструктуры, состоящее из набора приоритетов пользователей, правил распределения ролей, механизмов идентификации и аутентификации источника данных, отравителя и получателя, системы проверок подлинности пользователей благодаря технологиям ЭЦП.

4. В ходе данного исследования была предложена разработка такого криптографического протокола транспортных слоёв информационного сегмента, который обеспечивает целостность передачи данных, а также безопасную их транспортировку между субъектами сети – пользователями, серверами, другими ЭВУ, обеспечивающими работоспособность сети, и/или пользующимися услугами такой сети. За передачу информации о пользователях будет отвечать протокол Диффи-Хелмана, с разработанной защитой против атаки MIM, так же, данный протокол будет отвечать за передачу ключей доступа и идентификацию; алгоритм RSA 2048 bits будет отвечать за конфиденциальность данных, анонимность сторон передачи информации и невозможность прочтения данных в случае перехвата; за скорость определения экранов безопасности будет отвечать симметричный алгоритм AES128 bits;

за разграничение ролей и доступа будет отвечать специально усиленная система безопасности Белла-ЛаПадуллы.

5. Таким образом, используя предложенный протокол безопасности, можно говорить о том, что он представляет собой основу целостной информационной технологии, работающей на основании криптографического протоколирования и сильного шифрования для обеспечения абсолютной безопасности. Данная технология может быть использована в любой сегментированной области информационной инфраструктуры, использующей высокую степень безопасности данных в транспортных слоях передачи конфиденциальных данных.

Ключові слова: криптографічний протокол, інформаційна інфраструктура, кібербезпека.
Ключевые слова: криптографический протокол, информационная инфраструктура, кибербезопасность.
Keywords: cryptographic protocol, information infrastructure, cybersecurity.

Василенко Микола Дмитрович
Національний університет «Одеська юридична академія»
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, доктор юридичних наук,
професор

Новіков Вячеслав Пантелійович
Національний університет «Одеська юридична академія»
доцент кафедри кібербезпеки, к.т.н, доцент

Рачук Валерій Олександрович
Національний університет «Одеська юридична академія»
асистент кафедри кібербезпеки

БЕЗПЕКА ТА ВИКЛИКИ СУЧАСНОСТІ: РИЗИКИ ТА КІБЕРБЕЗПЕКА В ПЕРІОД ПАНДЕМІЇ

Інформація, яка надходить з різних країн світу свідчить про те, що в результаті пандемії з великим процентом ймовірності очікуються ризикові економічні та політичні негаразди.

З появою коронавірусу (COVID-19) додаткові проблеми з'явилися майже у всіх країнах і в усіх владних структурах, а урядові рекомендації, що стосувалися COVID-19, призвели до безпрецедентного переходу співробітників на дистанційний режим роботи.

Все це разом з різким скороченням персоналу і фінансовою кризою викликали стрімке зростання комп'ютерної злочинності. Так, аналітиками компанії Group-IB, міжнародної компанії, основним напрямком діяльності якої є розробка методів і засобів запобігання кіберзагроз в реальному часовому масштабі, позначені основні тенденції комп'ютерних злочинів в період пандемії COVID-19, на тлі різкого збільшення зростання числа кіберзагроз. Наприклад, в одному з основних напрямків комп'ютерної злочинності, на перший план висуваються методи фінансових шахрайств на базі соціальної інженерії при надзвичайно активній експлуатації теми COVID-19. Зараз це проявляється найчастіше в різкому збільшенні шкідливих розсилок, перемиканні операторів вірусів-шифрувальників на найширшу тематику і більш вишукану цільову вибірковість, а також активний рекрутинг в злочинні спільноти нових учасників.

Однією з головних поточних тенденцій цифрової трансформації сучасного періоду провідні світові аналітики одностайно називають розвиток дистанційних способів вчинення злочинів, при яких відсутній фізичний контакт між зловмисниками та їх жертвами – злочини пішли з офлайну в онлайн. Такі трансформації неминуче призводять до різкого збільшення числа кіберризиків, і зокрема, до зростання всіляких інших ризиків в середовищі простих користувачів ПЕОМ.

Проте також важливим залишається проведення необхідних заходів для забезпечення зниження ризиків в цілому, і кіберризиків зокрема, в цих виняткових обставинах. Через те, під час пандемії безперервна діяльність, в основному, відбувається завдяки використанню віддалених операцій, у світі з'явилась величезна кількість «фішингових» кампаній. Загальновідомо,

що фішинг являє собою « різновид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів – логінів і паролів » [1]. Це досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень усередині різних сервісів, наприклад, від імені банків або усередині соціальних мереж. У листі часто міститься пряме посилання на сайт, зовні невідмітний від сьогодення, або на сайт з редиректом. Після того, як користувач потрапляє на підробну сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленій сторінці свої логін і пароль, які він використовує для доступу до певного сайту, що дозволяє шахраям отримати доступ до облікових записів та банківських рахунків. У той час як сьогодні в багатьох країнах запроваджувалися заходи, щоб допомогти жертвам COVID-19 і обмежити зараження, хакери використовують кризу і продовжують свої дії для здійснення цілеспрямованих кібератак на підприємства, зокрема, на робочі місця. У період кризи хакери намагаються використовувати увагу, яку приділяють вірусам, і зв'язаними з ними панічно ефекту для проведення фішингових кампаній, видаючи себе за оповіщення, що зв'язані з COVID-19 (див. [1]). Отже, майже всі випадки можливих загроз базуються на розумінні та використанні ризиків та ризикових ситуацій. Водночас в умовах необхідності створення безпеки в інформаційно-комунікаційних системах, оцінка та якісний аналіз інформаційних ризиків дозволяє визначити необхідний рівень захисту інформації, здійснити його підтримку і розробити стратегію розвитку інформаційної структури системи. Мається на увазі, що це стосується самої компанії або підприємства. Оцінка та аналіз інформаційних ризиків виступають необхідною умовою при створенні системи керування ризиками і формуванні плану забезпечення стабільної роботи підприємства, а також при забезпеченні безперервності роботи та відновлення бізнесу. В широкому сенсі, у разі дослідження інформаційної безпеки, ризик часто

відображається імовірністю функціонально (стохастично) пов'язаними з нею поняттями. В цьому випадку можливий вимір результату визначається ймовірністю матеріальних та інших втрат через вірогідність появи несприятливого результату або події. Зустрічається також визначення ризику як дії або діяльності, реалізація якої ставить під загрозу задоволення будь-якої досить важливої потреби. В окремих джерелах ризик трактується як міра небезпеки, що характеризує ймовірність її появи й розміри пов'язаного з нею шкоди. Зустрічаються і визначення ризику, які відображають його як небезпеку вибору з двох або більше альтернативних варіантів дій та передбачає хоча б мінімальне збереження вже досягнутого раніше.

При дослідженні технічних ризиків, виділяють їх базові витоки: ризик розглядають як вимірювану або розраховану в деяких межах ймовірність отримання можливих результатів; ризик пов'язують з настанням певної події (як правило, не сприятливої); поняття ризику розкривається через практичну діяльність суб'єкта; ризик розкривається через незалежну від суб'єкта діяльності подію, наступ якої, кількісно можливо оцінити; при цьому, часто акцент робиться на кількісну та якісну оцінку ризику – «міру ризику»; поняття «ризику» розкривається через невизначеність; ризик відображається ситуацією можливості вибору з двох або з певної визначеної множини варіантів дії; ризик сприймається як небезпека, частота витрати і втрати, всебічна характеристика ситуації, а також комплексний аналіз деякого функціоналу заданого на множині вірогідних значень (декотрої сумарної величини). В цьому разі при обговоренні поняття «ризику», можна виділити одну характеристику, яка зустрічається у всіх визначеннях, наведених вище та об'єднує їх. Це є ніякий функціонал події, яка має відбутися і яка пов'язана з імовірністю, дією або діяльністю, мірою, частотою, вибором певних рішень, невизначеністю, з втратами, небезпекою і т.д. Пов'язані з коронавірусною пандемією карантинні заходи і режими самоізоляції

призвели до різкого зростання різних онлайн-сервісів – в це число входять в тому числі онлайн-магазини, онлайн-послуги різного роду і сервіси онлайн-зв'язку (зокрема – онлайн-конференції). Багато сервісів запускалися і масштабувалися без урахування заходів безпеки – в спробі довести пропозицію до рівня стрімко висхідного попиту. Це призвело до розширення «поверхні атаки» – можливостей для широкого спектра атак, а масштабування і запуск нових сервісів призвів до проявів нових вразливостей. Результатом чого було різке зростання кіберзлочинів, що корелює із зростанням попиту на онлайн-сервіси. Навіть якщо взяти тільки програми відеоконференцій, які в інтернет-просторі зарекомендували себе з найкращої сторони: Zoom, Skype, Discord, Google Hangouts, TrueConf, MyOwnConference, Mind, GoToMeeting, VideoMost, Proficonf, то в будь-якому разі, провівши аналіз інформації стосовно реалізації та впливу кіберзагроз на вищевказані програми телеконференцій, ще до введення в дію карантинно-обмежувальних заходів, пов'язаних з пандемією, ми побачимо реально наявні та дієві кіберзагрози в «мирний» час. Отже, ризики стали послідовними взаємопов'язаними процедурами, які входять у процес управління, а оцінка ризику передбачає дослідження стану, ситуації (сценаріїв) з наявними ознаками небезпеки, невизначеності та/або випадковості. Найефективнішим методом її здійснення є забезпечення юридичного підґрунтя та багатофакторне проєктування або прогнозування. На етапі оцінки ризиків формується стратегія управління ризиками, а оскільки повністю уникнути ризиків у більшості випадків неможливо, то вагоме значення має вирішення питання допустимості (прийнятності, виправданості) ризику, яке потребує подальшого дослідження та обґрунтування. Оцінка ризику, що використовують в технічних системах, розглядається як процес ідентифікації інформаційних ресурсів системи і загроз цих ресурсів, а також можливих втрат, заснований на оцінці частоти виникнення подій і розмір збитку. Аналіз ризику

розкривається як процес ідентифікації ризиків, визначення їх величини і виділення областей, що вимагають захисту. Таким чином, зазначені вище ризики мають принципову робочу «онлайн» складову, що дозволяє віднести їх до ризиків з великим людським фактором ризику, внаслідок якого в умовах коронавірусу користувачами робляться «вирішальні» помилки, породжені страхом і невпевненістю через багаточасове «онлайн» спілкування. Саме воно, на нашу думку, сприяє появі втоми у людей та формує «швидкісні помилки» через обмеження у часі. Активізується при цьому і проблема захисту персональних даних та стрімке збільшення їх крадіжок. Отже, необхідно на майбутнє проводити подальше удосконалення кібербезпеки, що спотворить умови протистояння найбільш вагомим викликам сучасності – пандемії в прояві COVID-19.

Список використаних джерел:

1. Василенко М. Д., Козін О. Б., Козіна М. О., Рачук В. О. Кіберризики в муніципальному господарстві в період пандемії: збитки та боротьба за кібербезпеку. Науково-технічний збірник «Комунальне господарство міст». Серія: технічні науки та архітектура. Харків, 2020. Т. 3. Вип. 156. С. 80–87.

Ключові слова: ризик, кібербезпека, «онлайн», невизначеність, оцінка, пандемія, COVID-19.

Ключевые слова: риск, кибербезопасность, «онлайн», неопределенность, оценка, пандемия, COVID-19.

Keywords: risk, cybersecurity, «online», uncertainty, assessment, pandemic, COVID-19.

Бойко Віктор Дмитрович
Національний університет «Одеська юридична академія»,
кандидат технічних наук, доцент кафедри кібербезпеки

Василенко Микола Дмитрович,
Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, професор

ВІДКРИТІ СИСТЕМИ І ПРОТОКОЛИ ВЗАЄМОДІЇ В КОНТЕКСТІ КІБЕРБЕЗПЕКИ «РОЗУМНОГО МІСТА»

Останнім часом отримали популярність концепції розвитку «розумного міста». Існує кілька різних визначень цього терміну (див. [1]). Така ситуація пояснюється тим, що сфера питань впровадження ІТ-технологій у практику урбаністики є порівняно молодою. Сам по собі термін «розумне місто» має кілька різних визначень і перетинається з близькими за значенням термінами («цифрове місто», «інтелектуальне місто» і так далі) – детально еволюцію терміну можна простежити по роботі [2].

В якості точки відліку виникнення ідеї «розумних міст» зазвичай вказують книгу [3], в якій був використаний термін «розумне зростання» («smart growth»). Пізніше, термін «розумне місто» («smart city») був запропонований в роботі [4], який по сути є подальшим розвитком [5].

Теперішня концепція «розумного міста» бачиться як точка сходження декількох паралельних процесів, при якій інтеграція міських інформаційно-комунікаційних систем виходить на новий рівень. З таких тенденцій можна виділити наступні:

- насичення населення індивідуальними засобами комунікації (персональні комп'ютери, смартфони, планшети),
- розвиток загальноміських комунікаційних мереж (високошвидкісний мобільний інтернет),
- розвиток інтелектуальних систем управління виробництвом (АСУ ТП / ISC),

- розвиток «Інтернету речей» (IoT),
- поява інтегральних загальноміських мереж управління і спостереження за трафіком,
- поява «розумних квартир» і «розумних будинків».

В цілому, щбільшення насиченості ІТ міською інфраструктурою має в майбутньому привести до якісної переходу від розрізнених «цифрових островів» до «цифровим кластерів», а від них до «розумних міст». Накопичення цифрових технологій призведе до переходу кількості в якість і в майбутньому можна буде говорити про «розумне місто», як про цілісну, єдину інформаційну екосистему (див. [6]), в якій Інформаційні технології відіграють ключову роль.

При цьому такий перехід здійснюється самопливом, без централізованої стратегії, з некваліфікованим персоналом. Нові технології часто впроваджуються і розгортаються без жодного тестування на безпечність. Розробники віддають перевагу простоті і легкості розгортання безпеки системи. Це призводить до збільшення потенційних ризиків і загроз як інформаційній інфраструктурі розумного міста, так і функціюванню (а іноді і існуванню) розумного міста в цілому.

Відсутність єдиної міської служби кібербезпеки призводить до того, що інциденти в різних ділянках міської та суміжних інфраструктур, обробляються запізно і без загальної координації.

Технічна підтримка систем «розумного міста» утруднена і часто запізнюється. Як було зазначено вище розробники промислових та інфраструктурних інформаційних систем часто запізнюються з реакцією на нові загрози. Причини такої ситуації можна розділити на суб'єктивні і об'єктивні. До суб'єктивних, наприклад, може бути віднесений погляд розробників на міські та промислові системи, як на менш пріоритетні і другорядні в порівнянні з очевидними мішенями для атак, наприклад з фінансово-банківським сектором. Відповідно, на стадії розробки менше уваги і ресурсів приділяється забезпеченню безпеки і захисту від вторгнень.

Можна виділити кілька джерел потенційних загроз і ризиків для міської інформаційно-комунікаційної інфраструктури, які існують вже зараз і будуть наростати в майбутньому.

Глибока інтеграція міських інформаційно-комунікаційних систем – від смартфона рядового користувача до системи управління міським електротранспортом і АСУ ТП системи енергопостачання – потенційно збільшує «поверхню атаки» для зловмисників. Кожен доданий в систему елемент має свої власні уразливості, при цьому його інтеграція в загальний простір «розумного міста» означає, що зловмисник, використовуючи ці уразливості, може отримати доступ до загальноміської інфраструктури ([7]). Загальна складність системи призводить до того, що атака може породжувати різні види «ланцюгових реакцій», коли вихід з ладу одного сегмента (наприклад, управління міською енергосистемою) може вивести з ладу суміжні сегменти (наприклад, систему управління дорожнім рухом).

У більшості впроваджуваного апаратно-програмного забезпечення постійно знаходять уразливості. При цьому процес усунення сильно уповільнений і розтягнутий у часі в порівнянні з призначеним для користувача програмним забезпеченням – це особливо стосується пропрієтарного програмного забезпечення, підтримка якого здійснюється розробником без участі спільноти («community»), а значить свідомо відстає від виявлення нових загроз.

Непропорційно великий сегмент технологій покладається на бездротові рішення. При цьому існує досить багато різних протоколів взаємодії, далеко не всі з яких відповідають стандартам безпеки. Така ситуація полегшує зловмиснику доступ до об'єкта атаки, відкриває додаткові уразливості в інформаційних системах, ще сильніше розширюючи поверхню атаки.

Великою проблемою є широке використання неефективних технологій, зокрема побудованих за принципом «secure by obscure», а також таких, що використовують «повітряний зазор» як виключний засіб захисту. Дослідження атаки Stuxnet

показує, що сучасне шкідливе програмне забезпечення досить легко долає «повітряний зазор» («air gap»).

Поширеною практикою є USB Drop attack – коли зараження відбувається через флеш-накопичувачі, вільно або мимоволі підключаються до системи. Один з варіантів такого зараження навіть передбачає використання спеціального пристрою для атаки. Такий пристрій замасковано під звичайний флеш-накопичувач, проте всередині містить іншу апаратну начинку, яка спрацьовує при підключенні «помилкової флешки» в usb-порт. Таким чином, в сучасних реаліях навіть повне відключення від зовнішніх мереж зв'язку не гарантує безпеку. При цьому прагнення до створення air gap часто призводить до зниження загальної ефективності системи і підвищення витрат на її експлуатацію. Це особливо актуально для «розумного міста», де більшість систем розраховані на збір і обробку інформації в оперативному режимі і втрачають цінність для «офлайнових» контекстів. У цьому випадку організація «air gap» створює більше проблем, ніж вирішує.

Також до об'єктивних загроз належать, наприклад, складнощі з експлуатацією вже впроваджених інформаційних систем, які забезпечують експлуатацію критичних ділянок інфраструктури. Зупинка або перебої в таких системах через невдале оновлення можуть спричинити значні збитки, якщо не матеріальні втрати. Тому, оновлення систем виконується рідко і з оглядкою на можливі наслідки.

Додатковим джерелом загроз є наявність в загальній системі ділянок, що обслуговуються застарілими системами з незакритими вразливостями. Заміна таких систем зазвичай відкладається до тих пір, поки не окупляться вкладення або поки в бюджеті не з'являться кошти. При цьому їх розробники можуть вже давно зняти системи з обслуговування – а це означає, що для виявлених в процесі експлуатації вразливостей і помилок не буде випущено оновлень. При цьому, завдяки загальній інтеграції систем «розумного міста», наявність в структурі

«острівців архаїки» піддає ризику не тільки ці ділянки самі по собі, але і відкриває зловмиснику шлях до інших систем.

Чисто технічні джерела ризиків і загроз, доповнюються проблемами на організаційному рівні – відсутністю в міській структурі Єдиного центру реагування на кіберзагрози інфраструктурі, загальною бюрократизацією процесу, низькою кваліфікацією обслуговуючого персоналу, закритістю міських систем для спільноти розробників.

Вихід з ладу об'єктів інфраструктури може бути як результатом цілеспрямованої (таргетованої) атаки зловмисника (Stuxnet), так і побічним ефектом від загальної глобальної атаки на інформаційну систему. Прикладом останнього є епідемія WannaCry і Petya, які, поширившись по комп'ютерних мережах «зачепили» банківський сектор і енергетику.

Перераховані вище джерела загроз означають, що подолання захисту таких систем – питання часу. При цьому додаткову небезпеку становить те, що з деякого моменту часу намітився тренд, при якому все більше атак інтелектуальних систем проводиться не з метою самоствердження зловмисника, а з метою заробітку грошей на наслідках подолання захисту.

Об'єктом атак дедалі частіше стають об'єкти промислової та міської інфраструктури. На такі атаки з'явився попит, а це свідчить в найближчому майбутньому, що можна очікувати значне збільшення пропозиції (див. [8] і оцінку у [9]).

При цьому метою таргетованої атаки не обов'язково повинно бути виведення з ладу будь-якого об'єкта або керівної системи. Все більше атак робиться для отримання приватної і не підлягаючої розголошенню інформації (наприклад після атаки на Korea Hydro & Nuclear Power Co., Ltd. (KHNP), зловмисники отримали доступ до креслень та інструкцій для атомних реакторів [10]).

Пропрієтарні, закриті вихідні коди, протоколи взаємодії і формати даних виглядають досить логічним рішенням особливо у випадках, коли розробник бере на себе поставку і розгортання системи «під ключ», а також забезпечує подальшу

технічну підтримку, проте на практиці породжують цілий спектр проблем.

Перша з них – «vendor lock-in» – прагнення постачальників послуг замкнути клієнта на себе, монополізувавши надання послуги. Це відкриває розробнику можливість надалі вносити небажані і невигідні зміни в умови поставки послуги. Як правило, на цьому етапі в організацію і розгортання системи вже вкладені досить великі кошти, тому відхід від розробника стає невигідним, що змушує миритися з новими умовами.

Друга – можлива наявність «чорних ходів» («backdoors»). Широко поширена практика, коли розробник залишає в системі «чорний хід» – свідомо ослаблене місце в системі, про який відомо тільки розробнику і яке розробник може використовувати для технічної підтримки за запитом клієнта – наприклад для відновлення втрачених клієнтом ключів для входу в систему або випадково видалених даних. Зазвичай офіційно декларується саме ця причина.

Однак, на практиці, в системах із закритим вихідним кодом наявність «бекдорів» залишається прихованим і їх експлуатація розробниками ніяк не може бути проконтрольована, що відкриває перед розробником широкі можливості для збору конфіденційної інформації та експлуатації системи в своїх інтересах.

Третя проблема полягає в тому, що «бекдор» відносно легко може бути виявлений при аналізі системи зловмисником – і використаний ним у своїх цілях. Багато зломів засновані саме на використанні свідомо закладених в систему розробником (самостійно або на вимогу клієнтів) вразливостей.

Таким чином сучасні тренди вказують на висхідний інтерес зловмисників до «розумних міст», при цьому самі системи «розумного міста» ще недостатньо відповідають вимогам безпеки та захисту від зовнішніх загроз. При розробці, плануванні впровадженні та розгортанні «розумного міста» треба передбачати комплексну систему захисту, яка відповідала б вимогам відкритості, розширюваності та децентралізації й не

покладалася б на застарілі та неефективні методи захисту («air gap», пропрієтарні протоколи, «secure by obscure» і так далі). На наш погляд цим вимогам відповідає широке використання програмного забезпечення з відкритими вихідними кодами, що використовує відкриті стандарти зберігання, передачі й перетворення інформації та широко залучає сучасні криптографічні засоби (асиметричну криптографію з відкритими ключами) і засоби забезпечення цілісності та децентралізації зберігання даних (блокчейн).

Використання відкритих стандартів для «розумного міста» і для його систем безпеки не тільки полегшує загальну внутрішню організацію міських підсистем – «розумних будинків», підприємств, транспорту, міської інфраструктури та окремих пристроїв, але і потенційно робить можливим створення «розумних регіонів», «розумних країн» і так далі – за аналогією з наявними зараз телефонними та інформаційними мережами. На прикладі телефонних та інформаційних мереж можна показати, що збільшення розмірів і охоплення мережі підвищує як загальну цінність, так і цінність окремих її сегментів.

Перераховані вимоги можуть здатися досить жорсткими, але в принципі досяжні на поточному рівні розвитку інформаційних технологій. Існують і досить поширені відкриті системи і протоколи взаємодії. При цьому основний шлях захисту даних у відкритих системах в даний час бачиться у використанні засобів асиметричної криптографії з відкритими ключами – можна послатися на класичний приклад PGP/GnuPG, однак зразковою реалізацією такої системи на наш погляд є специфікація шифрування носіїв LUKS, яка дає приклади хорошої організації захисту даних і зручного для користувача управління ключами.

Список використаної літератури:

1. Perätalo S., Ahokangas P. (2018). Toward smart city business models. Journal of Business Models. Vol. 6, no. 2, 65–70.

2. Cocchia A. (2014). Smart and digital city: A systematic literature review. Smart city, 13–43.

3. Bollier D. (1998). How smart growth can stop sprawl: A fledgling citizen movement expands. Essential Books, 90.

4. Komninos N. (2006). The architecture of intelligent cities. Intelligent Environments. – IET, Vol. 6. 53–61.

5. Schuler D. (2001). Digital cities and digital citizens. Kyoto workshop on digital cities, 71–85.

6. Deren L., Zhenfeng S., Xiaomin Y. (2011). Theory and practice from digital city to smart city [j]. Geospatial Information, Vol. 6, 002.

7. Cerrudo C. (2015). Hacking smart cities. RSA conference, 2–18.

8. Zygiaris S. (2013). Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. Journal of the knowledge economy, Vol. 4, no. 2, 217–231.

9. Friis K., Muller L. P., Gjesvik L. (2018). Cyber-weapons in international politics: Possible sabotage against the norwegian petroleum sector. NUPI Report. Retrieved from https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018–3.pdf

10. Lee K.-b., Lim J.-i. The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the korea hydro & nuclear power co., ltd. // KSII Transactions on Internet & Information Systems. – 2016. – Vol. 10, no. 2. – P. 857–880.

11. Bossi, S., & Visconti, A. (2015, December). What users should know about full disk encryption based on LUKS. In *International Conference on Cryptology and Network Security* (pp. 225–237). Springer, Cham.

12. Visconti, Andrea, et al. (2019). «Examining PBKDF2 security margin – Case study of LUKS.» *Journal of Information Security and Applications* 46: 296–306.

Ключові слова: розумне місто, відкрите програмне забезпечення, відкриті формати даних, відкриті протоколи взаємодії, загрози і ризики, повітряний зазор, безпеку, пропрієтарні протоколи.

Keywords: smart city, open software, open data formats, open communication protocols, threats and risks, air gap, security, proprietary protocols.

Ключевые слова: умный город, открытое программное обеспечение, открытые форматы данных, открытые протоколы взаимодействия, угрозы и риски, воздушный зазор, безопасность, проприетарные протоколы.

Бакуніна Олена Валеріївна
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат фіз.-мат. наук, доцент

ОБРАБОТКА СИГНАЛОВ И КИБЕРБЕЗОПАСНОСТЬ В НЕКОТОРЫХ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИХ СИСТЕМАХ: ХАОС-ГЕОМЕТРИЧЕСКИЙ ПОДХОД

Использование методов теории хаоса рассматривается как эффективный альтернативный метод шифрования информации, обеспечивающий высокий уровень кибербезопасности сложной информации. Опубликовано достаточно большое количество работ в этом направлении, но до сих пор отсутствует полное понимание всех математических, вычислительных, информационных и технологических аспектов проблемы (см., [1; 2] и ссылки в них).

В своей работе мы развиваем новый подход к проблемам обработки хаотических сигналов и информационной безопасности, основанный на широком использовании методов современной теории динамических систем и теории хаоса. Подход основан на использовании таких методов, как хаотический вейвлет-анализ, метод взаимной информации, корреляционный интегральный анализ, анализ показателей Ляпунова, метод суррогатных данных в версии [2]. В качестве примера приведены некоторые данные о топологических и динамических инвариантах (размерность Каплана-Йорка, показатели Ляпунова, энтропия Колмогорова) временных рядов хаотических сигналов, генерируемых в лазерной технологической системе типа [1].

Список використаних джерел:

1. C. Mirasso et al, Optoelectronic devices for optical chaos communications, Proc. SPIE5248, Optoelectronic Devices for Lightwave Communication, US (2003).

2. A. V. Glushkov et al, Chaos-geometric attractor and quantum neural networks approach to simulation chaotic evolutionary dynamics

during perception process, Advances in Neural Networks, Fuzzy Systems and Artificial Intelligence, Ser.: Recent Adv. in Computer Engineering, Ed. J. Balicki (WSEAS Pub.), Vol.21, 143 (2014).

Ключові слова: кібербезпека, інформаційні системи, хаос-геометричний підхід

Ключевые слова: кибербезопасность, информационные системы, хаос-геометрический подход

Keywords: cybersecurity, information systems, chaos-geometric approach

Задерейко Александр Владиславович
Национальный университет «Одесская юридическая академия»,
доцент кафедры информационных технологий,
кандидат технических наук, доцент

АНАЛИЗ УТЕЧЕК ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

Повсеместное использование мобильных приложений для оперативного по-лучения информации и мгновенной коммуникации значительно увеличивает вероятность утечки персональных данных пользователей. Любые мобильные при-ложения социально-медийной направленности дают разработчикам легальный доступ к приватному спектру данных о пользователе. Перечень собираемой информации определяется лицензионным соглашением к каждому устанавли-ваемому мобильному приложению, которое большинство пользователей не изучают и «по умолчанию» соглашаются с условиями их использования.

Это обстоятельство определяет небходимость проведения комплекса экспериментальных исследований по изучению интернет-трафика мобильных приложений (см. рис. 1) [1]:

- фиксации всех входящих и исходящих интернет-соединений с удаленными доменами;
- определение доменов, с которыми устанавливаются «сторонние соединения[1]»;

[1] Под сторонними соединениями подразумеваются исходящие и входящие соединения мобильных приложений, которые устанавливаются с доменами, не имеющими прямого отношения к официальным доменам мобильных приложений.

• получение информации о доменах, с которыми устанавливаются «сторонние соединения»;

• блокировку входящих и исходящих «сторонних соединений» мобильных приложений с обязательной проверкой сохранения их работоспособности.

Рис. 1. Обмен данными мобильных приложений с доменным пространством Интернет

Цель исследования – изучить исходящие и входящие соединения мобильных приложений для популярных социальных сетей и мессенджеров с доменным пространством Интернет.

Объект исследования – мобильная операционная система Android 10, мессенджеры Whatsapp, Viber, Telegram, мобильные приложения Facebook, Instagram.

Средства исследования – мобильное программное обеспечение – сетевой экран No Root Firewall[1].

Интернет-провайдер – компания «Интертелеком – Украина».

Результаты исследования

В результате 120-ти дневной фиксации трафика мобильных приложений для коммуникации пользователей был зафиксирован перечень IP-адресов сторонних хостов (доменов), с которыми они выполняют обмен данными (см. табл. 1).

[1] **NoRootFirewall**–https://play.google.com/store/apps/details?hl=ru&id=app.greyshirts.firewall

Таблица 1.

Мобильные приложения		Сторонние IP адреса (домены)	Блокировка IP адресов	Работоспособность мобильного приложения (+ / -)
Мессенджеры	Telegram	*.1e100.net:443	√	+
		dns.google:443		
		149.154.167.*:5222		
		149.154.165.*:5222		
		91.108.56.192:5222		
		104.16.248.249:443		
	Whatsapp	*.static.sl-reverse.com:5222	√	+
		*.static.sl-reverse.com:443		
		*.fbcdn.net:443		
		*.1e100.net:443		
		157.240.14.53:5222		
		169.63.76.65:5222		
	Viber	*.compute-1.amazonaws.com:4244	√	+
		*.deploy.static.akamaitechnologies.com:443		
		*.googleusercontent.com:443		
		*.r.cloudfront.net:443		
		s3-website.eu-central-1.amazonaws.com:80		
		*.1e100.net:443		
		78.154.185.26:443		

Таблица 1. Продолжение

Мобильные приложения		Сторонние IP адреса (домены)	Блокировка IP адресов	Работоспособность мобильного приложения (+ / -)
	Instagram	78.111.180.97:443	√	+
		78.26.240.33:443		
		79.124.240.161:443		
		*.facebook.com		
		*.fbcdn.net		
		*.1e100.net:443		
	Facebook	*.compute-1.amazonaws.com:4244	√	
		*.fbcdn.net:443		
		*.1e100.net:443		
		*.utel.net.ua:443		
		*.vps-default-host.net:443		
		ua*.host.hit.gemius.pl:443		
		es49.mirohost.net:443		
		*.r.cloudfront.net:443		
		*.eu-west-1.compute.amazonaws.com:4244		
		*.clients.your-server.de:443		
		*.ip.kyivstar.net:443		
		*.pl-sh.host4.biz:443		
		*.te.net.net:443		
		*.dialup.umc.net.ua:443		

Примечание*: В таблице 1, * – отмечаются динамически изменяющиеся части доменных имен.*

Анализ входящих и исходящих соединений мобильных приложений позволил выявить домены сторонних интернет-ресурсов, к которым обращаются мобильные приложения и мессенджеры (см. табл. 1). Информация, полученная из

открытых источников об этих доменах позволила установить следующее:

• Домен **sl-reverse.com** – подключен к ns-серверам1: *networklayer.com*, *softlayer.net*. Принадлежит веб-платформе CSC Digital Brand Services, специализирующейся на цифровом управлении брендами и цифровом маркетинге;

• Домен **1e100.net** – подключен к ns-серверам *google.com*. Принадлежит корпорации Google [2];

• Домен **googleusercontent.com** – подключен к ns-серверам *google.com*. Принадлежит корпорации Google [2];

• Домен **akamaitechnologies.com** – подключен к ns-серверам: *akamaistream.net*. Принадлежит компании Akamai Technologies – провайдеру платформы доставки контента и приложений для акселерации доступа к интернет-ресурсам.

• Домен **cloudfront.net** – подключен к ns-серверам: *awsdns-35.org*, *awsdns-07.co.uk*, *awsdns-52.com*, *awsdns-19.net*. Принадлежит корпорации Amazon, специализирующейся на предоставлении услуг в облачных сервисах на основании анализа интернет-трафика.

• Домен **fbcdn.net** – подключен к ns-серверам: *facebook.com*. Принадлежит социальной сети Facebook. Используется для обслуживания доставки статического контента (видео и фото из CDN2).

• Домен **clients.your-server.de** – подключен к ns-серверам: *ns.second-ns.com*, *ns1.your-server.de*, ns3.second-ns.de.

• Домен **pl-sh.host4.biz** – подключен к ns-серверам: *curt.ns.cloudflare.com*, *kiki.ns.cloudflare.com*. *cloudflare.com*. Принадлежит организации «Host4Biz sp. z o.o.», оказывающей услуги хостинга. Находится под управлением, ns-серверов принадлежащим корпорации CloudFlare Inc, предоставляющей услуги CDN и сервера DNS.

---

[1] **NS-сервер** – Name Server (DNS-сервер), преобразующий доменные имена, с которыми работают пользователи, в понятные компьютерам IP-адреса или в обратном направлении.

[2] **CDN (content delivery network)** – сеть доставки контента, – это распределенная сеть серверов, используемых для ускорения доставки запрашиваемого контента с ближайшего к пользователю сервера.

• Домен **es49.mirohost.net** – принадлежит организации Internet Invest, Ltd, регистратору доменных имён и крупнейшему хостинг-провайдеру в Украине.

• Домен **net.net** – принадлежит организации Bodis, LLC. Оказывающей услуги по монетизации и управлению доменным трафиком.

• Домен **kyivstar.net** – принадлежит интернет-провайдеру Киевстар.

• Домен **umc.net.ua** – принадлежит интернет-провайдеру Ukrainian Mobile Communications.

• Домен **utel.net.ua** – принадлежит интернет-провайдеру Укртелеком.

• IP адрес **78.154.185.26** – принадлежит интернет-провайдеру – Eurotranstelecom Ltd (Украина).

• IP адрес **78.111.180.97** – принадлежит интернет-провайдеру LLC Renome-Service (Украина).

• IP адрес **79.124.240.161** – принадлежит интернет-провайдеру Lifecell (Украина).

Выводы

1. Мобильные приложения и мессенджеры устанавливают соединения и ведут интенсивный обмен данными со сторонними доменами (серверами), владельцы которых, представлены компаниями, оказывающими услуги по транзиту, сбору, накоплению, обработке, и монетизации доменного трафика мобильных приложений с использованием облачных технологий. Такой обмен данными с высокой долей вероятности может привести к не контролируемому пользователями сбору их персональных данных.

2. Мобильные приложения Facebook и Instagram устанавливают соединения со сторонними интернет-провайдерами Украины, а также с доменами, принадлежащими компаниям, специализирующимся на монетизации доменного трафика.

3. Все исследуемые мобильные приложения устанавливают соединения с доменами, принадлежащими корпорации Google (домен – 1e100.net). Помимо этого:

• Месенджер Telegram осуществляет попытку перенаправления своего трафика через DNS сервера корпорации Google (домен – dns.google).

• Месенджер Viber устанавливает дополнительное соединение с сервисом анализа контента корпорации Google (домен – googleusercontent.com).

4. Блокировка зарегистрированных соединений мессенджеров Telegram, Whatsapp, Viber и приложений Facebook и Instagram на сторонние сервера, не вызывает потерю их работоспособности и позволяет:

• исключить несанкционированный пользователями сбор персональных данных;

• полностью сохранить функциональность и работоспособность мобильных приложений;

• сократить передачу интернет-трафика пользователя на 50–70%, что позволит сократить расходы пользователей на оплату услуг Интернет-провайдеров мобильного трафика.

Список используемых источников:

1. Задерейко О. В. Аналіз вірогідних витоків конфіденційної інформації користувачів у мобільних застосунках / О. В. Задерейко, Н. І. Логінова, О. Г. Трофименко // Графічні технології моделювання об'єктів, процесів та явищ: зб. тез доп. Міжнар. наук.-практ. конф. (м. Одеса, 23–24 квіт. 2020 р.) / МОН України; Військова академія. – Одеса, 2020.

2. Google: зловещая черта. [Електронний документ]. – URL: https:// zadereyko.info/video/google_zloveshaya_cherta.htm.

Ключові слова: витоки даних, збір даних в мобільних додатках, збір даних в месенджерах, збір даних.

Ключевые слова: утечки данных, сбор данных в мобильных приложениях, сбор данных в мессенджерах, сбор данных.

Keywords: data leaks, data collection in mobile apps, data collection in messengers, data collection.

Кухаренко Сергій Вікторович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук

СУЧАСНІ ТИПИ КІБЕРЗАГРОЗ

У сучасному суспільстві комп'ютери використовуються практично у всіх областях діяльності. Досить часто виникає необхідність захисту важливої інформації. Великі організації мають в своєму складі фахівців з кібербезпеки (служба захисту інформації) але у організації невеликого або середнього розміру питання безпеки інформації залишають на потім.

На жаль, не існує готових рецептів на всі випадки життя і немає підходів, однаково придатних для всіх організацій, щоб убезпечити себе хоча б від найбільш вірогідних ризиків. Спробуємо виділити основні типи загроз кібербезпеки, на які необхідно звернути особливу увагу. З огляду на те, що захист від атак на мережевий периметр приділяється дуже велика увага і практично будь-який пристрій, яке ви купуєте і встановлюєте у себе в офісі або вдома, наприклад мережевий маршрутизатор або домашній WiFi роутер, вже мають базові засоби захисту.

Спробуємо звернути увагу на ті загрози і методи їх усунення, які виражені не так явно або їх важливість, як правило, недооцінюється.

Виділимо п'ять основних типів кіберзагроз: програми-вимагачі, цільові кібератаки, DDoS-атаки, фішинг і внутрішні загрози, пов'язані з діяльністю інсайдерів і людськими помилками.

Згідно з останнім звітом «Verizon 2020 Data Breach Report: Money Still Makes the Cyber-Crime World Go Round» [1] з кіберзлочинності, 86% атак фінансово мотивовані: зловмисники або безпосередньо вимагають гроші у жертви, або виконують сторонній замовлення, наприклад, конкурентів чи інших недоброзичливців.

Найбільшою мірою сьогодні схильні до атак оператори зв'язку, фінансові організації, ритейл-мережі і промисловий сектор. Крім того все більше привертає уваги кіберзлочинців малий і середній бізнес. Це пояснюється тим, що конкуренція в ньому досить висока, а можливості кіберзахисту і оцінки ризиків часто обмежені. Посилює проблему масовий перехід на віддалену роботу, через що периметр мережі організації поширився на будинки співробітників і їх особисті пристрої.

Отже на мій погляд можливо виділити наступні основні типи кіберзагроз на даний час, такі як: програми-вимагачі, цільові кібератаки, DDoS-атаки, інсайдерські загрози та фішинг.

Програми-вимагачі

Віруси-вимагачі шифрують дані на комп'ютері користувача і вимагають викуп за можливість відновити доступ до них. Зазвичай пропонується заплатити викуп криптовалютою. Проникнувши в корпоративну мережу, віруси-вимагачі здатні блокувати відразу велику кількість комп'ютерів.

Найбільш схильні до атак з метою вимагання телекомунікаційні компанії, інтернет-провайдери, освітні установи, урядові і технологічні організації.

У кіберзлочинності спостерігається тенденція до спеціалізації і співпраці. Об'єднуючи зусилля, зломщики успішно справляються з системами захисту великих організацій, розділяючи виручку.

Для повноцінного захисту від вимагачів потрібно не тільки сучасне програмне забезпечення, а й системна профілактика, що включає оцінку ризиків, установку міжмережевих екранів, створення резервних копій, розробку сценаріїв реагування на різноманітні події та інші заходи.

Цільові кібератаки

В останні роки кіберзлочинці перейшли до більш цілеспрямованих атак, зосереджуючись на конкретних галузях з їх характерними уразливими місцями. Зростання частки цілеспрямованих атак зумовлений низкою причин. По-перше, зловмисники жадають не витрачати час на компа-

нії, які не гарантують їм грошову прибуток. По-друге, щорічно з'являються нові групи зловмисників, які спеціалізуються на атаках класу APT (advanced persistent threat – різновид складних кібератак з метою отримання несанкційованого доступу до інформаційних систем жертви та встановлення прихованого доступу до неї з метою використання або контролю в майбутньому).

Цільова атака полягає в тому, що спочатку зловмисники шукають спосіб потрапити в корпоративну мережу: збирають інформацію, шукають уразливості організації (не тільки цифрові, але й фізичні), вивчають розклад, маршрути, слабкості, цікавлять співробітників та інше. Потім здійснюється власне проникнення: зловмисники можуть надіслати на конкретного співробітника фішинговий лист, вкрасти телефон співробітника для вилучення будь-яких корпоративних паролів, втертися в довіру компанії під виглядом підрядника або проникнути в офіс в якості кур'єра. Метою на цьому етапі є прихована установка програмного забезпечення на корпоративній техніці.

На останньому кроці діючи вже зсередини компанії, зловмисники підбираються до інформації, яка їх цікавить і викрадають її в обхід засобів захисту. Потім, як правило, зловмисники замітають сліди, щоб атака не була виявлена.

В цільової атаці можуть використовуватися будь-які інші кіберзлочинні методи – фішинг, вимагання та інше.

Запобігання цільових атак – складне завдання. Однак сучасні засоби захисту при їх правильному і комплексному використанні дозволяють зрозуміти, що відбувається якась неавторизована активність. Кожен користувач повинен спочатку пройти ідентифікацію, тобто довести системі, що це він, а потім авторизацію, тобто отримати строго певні права в системі.

Для запобігання цільових атак потрібне строгий і чіткий розподіл прав доступу всередині компанії і дотримання принципу мінімальної достатності: тобто виконуються лише ті дії, які потрібні для необхідних процесів.

DDoS-атаки

DDoS-атака – це атака на будь-яку обчислювальну систему (наприклад, сервер) з метою вичерпати її апаратний ресурс шляхом величезної кількості одночасних звернень до неї. Коли система не справляється з обробкою цих звернень, відбувається відмова в обслуговуванні (Denial of Service) і система виходить з ладу.

DDoS-атаки становлять небезпеку в першу чергу для компаній, діяльність яких безпосередньо пов'язана з інтернетом (електронна комерція), а також для операторів зв'язку.

Останнім часом зловмисники використовують для своїх ботів пристрої інтернету речей (IoT), тобто, наприклад, побутові прилади з підключенням до інтернету: принтери, розумні колонки, кондиціонери, системи освітлення в розумному будинку та інше. Виробники IoT-пристроїв, як і користувачі цих пристроїв, найчастіше не приділяють уваги їх безпеки, тому заразити IoT-пристрій відносно просто.

Для боротьби з DDoS-атаками застосовують DDoS-фільтри, що дозволяють вибірково відсікати зайві звернення до сервера, що йдуть від ботів. Профілактика DDoS-атак включає розумну мінімізацію контактів системи з іншими пристроями: доступ до системи повинен бути закритий для портів, протоколів і додатків, взаємодія з якими не передбачено.

Інсайдерські загрози

Велика група загроз, джерелом яких є власні співробітники. Поширена в організаціях, де відсутній контроль за наданням прав доступу високого рівня, а також відсутні розмежування з прав доступу до інформаційних ресурсів.

Інсайдерські загрози можуть бути пов'язані як зі злим умислом, так і з випадковими діями, з людською помилкою.

Для боротьби необхідно реалізовувати принцип мінімальної достатності: працівнику треба давати тільки ті права, які йому потрібні для виконання робочих обов'язків. Крім того, також допоможуть системи і методи, які аналізують поведінку користувачів. Вони побудовані на технологіях штучного

інтелекту і здатні до навчання на основі статистики, постійно моніторять активність співробітників на робочих місцях. Якщо ті відхиляються від заздалегідь заданих сценаріїв діяльності, то формуються оповіщення для служби безпеки, яка може заблокувати ту чи іншу дію.

В останні роки зловмисники все частіше використовують передові технології, такі як штучний інтелект, і застосовують методи соціальної інженерії, тобто експлуатують уразливість людської психології.

Фішинг

Це вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних. Найчастіше приманкою є електронний лист, здатний зацікавити одержувача, а гачком – закладений в цей лист шкідливий виконуваний файл або гіперпосилання на нього.

На даний час, це може бути посилання на свіжу статистику по темі, що стосується Covid, або якусь іншу актуальну інформацію, яка цікава багатьом користувачам [2].

Небезпека фішингу в тому, що головний елемент в ньому не технічний, а психологічний. Зловмисники знають, що людину обдурити легше, ніж машину. Сучасні засоби захисту дозволяють в автоматичному режимі у всіх файлах, які передаються поштою або через інтернет, аналізувати посилання в процесі відкриття і переривати цей процес, якщо фіксують запуск виконуваних файлів.

Висновки

Ці фактори, серед інших, говорять про те, що базове розуміння кіберзагроз необхідно перемістити з професійної області ІТ-фахівців в область загального знання. Кожен співробітник повинен мати певне уявлення про сучасні загрози, а тим більше керівник, який ставить завдання фахівцям з кібербезпеки.

Список використаних джерел:

1. Отчет Verizon Business 2020 о расследовании утечек данных (DBIR2020) [Електронний ресурс]. – Режим доступу:

https://www.securitymagazine.com/articles/92415-verizon-2020-data-breach-report-money-still-makes-the-cyber-crime-world-go-round

2. Global Threat Landscape Report [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/Threat-Report-H1–2020.pdf

Ключові слова: Кібербезпека, кіберзлочинність, кібератака, порушення даних.

Ключевые слова: кибербезопасность, киберпреступность, кибератака, нарушение данных.

Keywords: cybersecurity, cybercrime, cyberattack, data breach

Онацький Олексій Віталійович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки та інформаційних технологій,
кандидат технічних наук, доцент

Красношлик Олександр Юрійович
Національний університет «Одеська юридична академія»,
студент 3 курсу спеціальності 125 – Кібербезпека

ПРОТОКОЛ АВТЕНТИФІКАЦІЇ НА ОСНОВІ АСИМЕТРИЧНОГО АЛГОРИТМУ ШИФРУВАННЯ

Автентифікація – це процедура перевірки автентичності суб'єкта котрий входить в систему та пред'являє свій ідентифікатор. Основним міжнародним стандартом з криптографічних протоколів автентифікації є стандарт Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії ISO/IEC9798 – Information technology – Security techniques – Entity authentication, що складається з шести частин [1]:

– ISO/IEC9798–1:2010 Part 1: General;

– ISO/IEC9798–2:2019 Part 2: Mechanisms using authenticated encryption;

– ISO/IEC9798–3:2019 Part 3: Mechanisms using digital signature techniques;

– ISO/IEC9798–4:1999 Part 4: Mechanisms using a cryptographic check function;

– ISO/IEC9798–5:2009 Part 5: Mechanisms using zero-knowledge techniques;

– ISO/IEC9798–6:2010 Part 6: Mechanisms using manual data transfer.

На основі проведеного аналізу стандартів ISO/IEC9798 побудована загальна схема класифікації криптографічних протоколів автентифікації і ідентифікації, яку представлено на рис. 1.

Протоколи автентифікації «запит-відповідь» з використанням асиметричних криптосистем можна розділити на дві групи: протоколи з використанням електронного цифрового підпису та протоколи з використанням криптосистем з відкритим ключем [2]. В роботі запропонований протокол взаємної автентифікації на основі асиметричного алгоритму шифрування RSA.

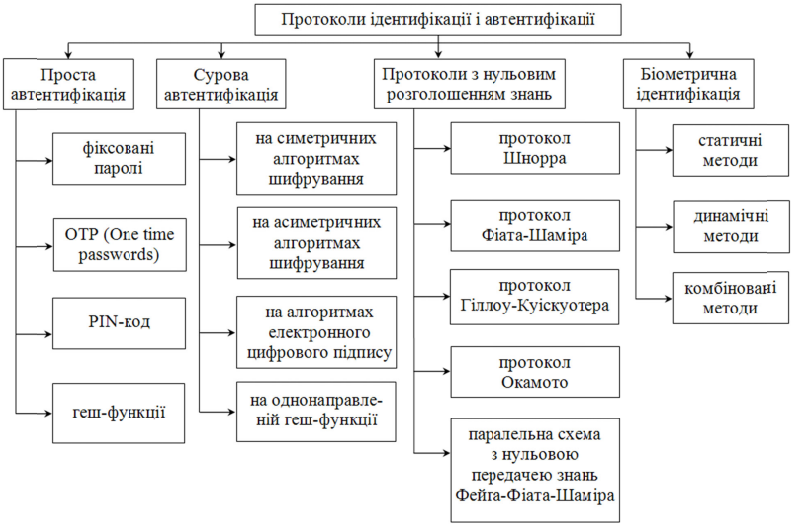


Рис. 1. Загальна схема класифікації протоколів автентифікації і ідентифікації

Криптосистема RSA [3; 4] одна з широко використовуваних криптосистем з відкритим ключем. Криптограма обчислюється за правилом $C \equiv M^e \pmod{n}$, де n – добуток двох великих простих чисел p і q, e – ключ зашифровування (відкритий ключ), M – повідомлення. Розшифрування виконується за правилом $M \equiv C^d \pmod{n}$, де d – ключ розшифрування (секретний ключ), C – шифртекст (криптограма). Ключова пара (e, d) пов'язана між собою рівнянням $ed \equiv 1 \pmod{\varphi(n)}$, де $\varphi(n)$ – функція Ейлера $\varphi(n) = (p - 1)(q - 1)$. Пара чисел (n, e) робиться відкритим ключем, числа d, p, q – секретними.

Реалізація протоколу взаємної автентифікації на основі асиметричного алгоритму шифрування RSA представлений на рис. 2, де e_a, e_b – відкрити ключі; d_a, d_b – секретні ключі; ID_a, ID_b – ідентифікатори; r_a, r_b – випадкові числа абонентів A та B. Деталі реалізації протоколу представлені на рис. 2 в виді трьох кроків. Взаємна автентифікація абонентів A та B виконується після кожного кроку перевірної рівності отриманих значень.

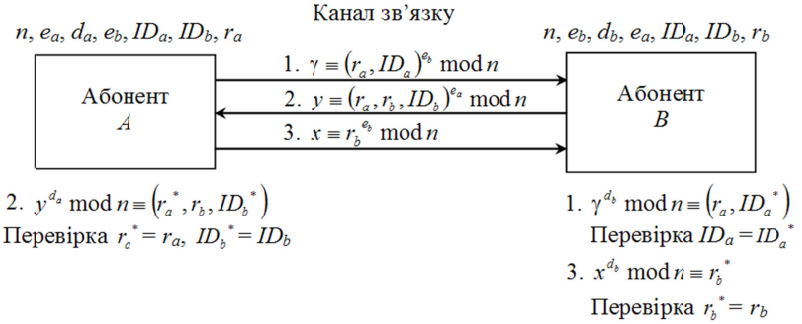


Рис. 2. Протокол взаємної автентифікації на основі алгоритму RSA

Однак для правильної роботи протоколу обов'язково використовувати ідентифікатори сторін в іншому випадку можливо атака «людина по середині» (man in the middle – MITM) [5; 6],

приклад реалізації атаки MITM представлена на рис. 3. Крім того можлива атака при використанні загального модуля якщо значення (r_a, ID_a) = (r_a, r_b, ID_b) будуть однакові (сервер – абонент *B* повинен виключити виконання даного рівняння) [3; 4; 6].

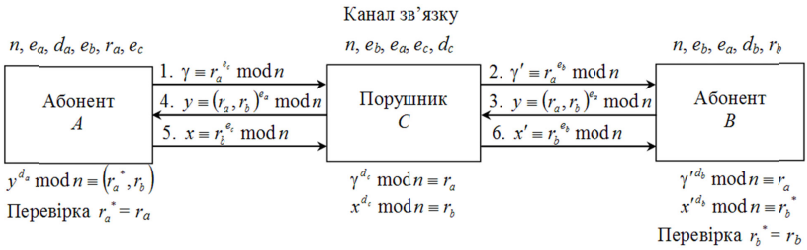


Рис. 3. Приклад реалізації атаки MITM на протокол взаємної автентифікації (ідентифікатори сторін A та B відсутні)

В роботі наведено математичне обґрунтування, приклад розрахунку, які показують, що запропонований протокол взаємної автентифікації на основі алгоритму RSA працює коректно та технічно реалізуємо.

Список використаних джерел:

1. ISO/IEC 9798. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standards.html

2. Виклик-відповідь (автентифікація). [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Виклик-відповідь_(автентифікація)

3. Бернет С. Криптография. Официальное руководство RSA Security / Бернет С., Пэйн С. – М.: Бином-Пресс, 2002. – 384 с.

4. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C / B. Schneier. – Wiley, 2015. – 784 p.

5. Атака посредника. [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Атака_посредника.

6. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – 816 p.

Ключові слова: автентифікація, криптографічний протокол, криптосистема з відкритим ключем, шифрування, шифртекст.
Ключевые слова: аутентификация, криптографический протокол, криптосистема с открытым ключом, шифрования, шифртекст.
Keywords: authentication, cryptographic protocol, public key cryptosystem, encryption, ciphertext.

Баландіна Наталія Миколаївна
Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки

Василенко Микола Дмитрович
Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, доктор юридичних наук,
професор

ДЕЯКІ НОТАТКИ ЩОДО МАТЕМАТИЧНИХ МОЖЛИВОСТЕЙ В МОДЕЛЮВАННІ ЗАХИСТУ ІНФОРМАЦІЇ

Сучасний стан захисту інформації посприяв розвитку досліджень, які пов'язані з інтелектуалізацією обчислень в галузі підтримки прийняття рішень в кібербезпеці та в захисті інформації в цілому для різних інформаційних систем і технологій. Сьогодні продовжують розроблятися нові методи та моделі для підтримки прийняття рішень щодо вибору і реалізації стратегії захисту інформаційних процесів. В роботі наведено спробу встановлення деяких реальних дій обмежень в питанні математичних можливостей при моделюванні захисту інформації. Очевидно, що моделі захисту інформації являють собою складову частину загального процесу моделювання. І тут моделювання системи полягає у побудові образу системи, адекватного з точністю до цілей моделювання системи, яка проєктується, і в отриманні за допомогою побудованої моделі потрібних характеристик реальної системи з метою побудови захисту. Оскільки інформаційні системи змінюються

в часі та мають зміни в середовищі, наприклад в умовах КОВІД-19, треба користуватися динамічними моделями для нелінійних систем, а як добре відомо, що модель представляє собою теж систему, то, безумовно, модель може бути також нелінійною. Формально нелінійність моделі може бути виражена у структурі рівнянь, що використовуються, а знаходження їхніх розв'язків, щонайменше, у чисельному вигляді, в деяких випадках може бути цілком здійсненною задачею. Основну увагу при побудові нелінійних конкурентних моделей нині приділяють аналізові принципових внутрішніх взаємодій динамічних систем на основі логістичних моделей. Моделювання динаміки розвитку на основі диференціальних логістичних рівнянь широко використовується для моделювання найрізноманітніших як природних, так і соціальних процесів. Відзначимо, що при цьому в загальному випадку весь процес моделювання можна поділити на дві складові частини: побудова моделі та реалізація моделі з метою отримання потрібних характеристик системи.

В загальному вигляді основне призначення моделей визначається як створення умов для об'єктивної оцінки загального стану інформаційної системи з точки зору міри уразливості або рівня захищеності інформації в неї. Потреба в таких оцінках, зазвичай, виникає під час аналізу загальної ситуації, з метою відпрацювання стратегічних рішень під час організації захисту інформації, яка відносить ще й до складних систем. Найчастіше для моделювання складних систем застосовують диференціальні рівняння, які описують динаміку зміни станів таких систем. Як правило, це система рівнянь першого порядку, що має вигляд, представлений в [1].

Створення сучасних систем інформаційної безпеки на практиці може задовольнятися трьома формальними методами побудови моделей: кібернетичним підходом, системною динамікою та теоретично-множинним підходом. Сучасні технології роботи з великими даними майже завжди потребують створення математичних можливостей, що визначають

процес пошуку та оброблення інформації. Навіть при дотриманні усіх основних принципів побудови моделей (інформаційної достатності, доцільності, здійсненності, множинності моделей, агрегації, параметризації, із застосуванням методології інтеграційного (багаторівневого) моделювання важко досягти бажаних результатів. В результаті розробники практично завжди пропонують програмні продукти, які мають велику кількість уразливостей. Це дозволяє зловмисникам будувати складні алгоритми атак, що можуть досягати своєї мети різними способами, в залежності від ситуації в кіберпросторі. На практиці для реалізації атак у мережному середовищі зазвичай використовуються троянські програми, кінцевою метою яких є впровадження у програмний код атакованої системи додаткових прихованих функцій. Негараздом є те, що зазвичай факт втручання може бути виявлений вже після здійснення атаки. При цьому такі несанкціоновані втручання до інформаційної системи не мають чітко визначеної часової закономірності, а їх тривалість є недостатньою для належного реагування. Таким чином, задача полягає у створенні такої стратегії боротьби, яка б дозволяла визначати зловмисні дії вже на перших кроках реалізації кібератак. Однією з умов створення ефективної системи захисту стає володіння інформацією про всі слабкі місця кібератаки, а також розуміння формальних моделей організації сучасних атак у середовищі експлуатації інформаційних систем. І самі моделі, і визначення переліку уразливостей ґрунтується на постійному моніторингу можливих джерел загроз, з точки зору їх мотивів та наявності ресурсів для реалізації цих загроз, а також аудиту системи захисту на наявність у ній уразливостей. Відповіді на ці питання дає використання «ромбоподібної» моделі, яка наведена у [2]. Саме вона породжує ланцюжок «кібервбивств». Відповідно до результатів [2] зловмисник атакує інформаційний ресурс, керуючись своїми мотивами, а не планом вторгнення. Ця модель враховує чотири основних елементи: супротивника і його ресурси, інфраструктуру,

здатність до нападу і ціль. Для прогнозування дій порушника найчастіше використовується модель послідовних вторгнень [3]. Порушник крок за кроком виконує спроби подолання системи захисту, намагаючись подолати механізми захисту через уразливості там, де він їх знаходить. Основними елементами моделі послідовних вторгнень є індикатори, під якими розуміється будь-яка інформація, що об'єктивно описує кожний етап вторгнення. Отже, послідовність вторгнення включає сім етапів: розвідку, озброєння, доставлення, виконання, створення «чорного входу», установка таємного каналу і зловмисні дії щодо об'єкта атаки. Попри тип обраної моделі атак, автоматизація процесів протидії нападу на інформаційну систему з боку зовнішнього кібернетичного середовища передбачає створення досить складного програмного коду. Ця робота зазвичай розпочинається із розроблення великої кількості формальних алгоритмів, що потребує використання усталеного математичного апарату. Саме через це, ще на початку розвитку мережного середовища, коли атаки на інформацію були досить простими, для визначення їх архітектури використовували графові моделі [4]. Графи атак являють собою концептуальні діаграми і використовуються для аналізу можливих шляхів реалізації конкретної загрози, які структурно вони представляють собою багаторівневі деревоподібні структури, що мають дочірні елементи з одним коренем. У випадку опису сучасної атаки вони мають тисячі вузлів і шляхів подолання механізмів захисту. Тому генерація графів для атак у складних мережах є дуже складною в обчислювальному сенсі. На основі проведеного аналізу наявних моделей реалізації мережних атак можна зазначити, що перевага має надаватись таким, які дозволяють, по-перше, оцінити вірогідність нападу з боку можливих джерел загроз, по-друге, визначити стратегію розпізнавання атаки на початку спроби її реалізації порушником безпеки. Модель повинна легко піддаватись формальному опису для подальшого її використання у процедурах автоматизації управління захистом.

Список використаних джерел:

1. Малков С.Ю. Математическое моделирование исторической динамики: подходы и модели. М.: РГСУ. 2004. 188 с.

2. Caltagirone S., Pendergast A., Betz C. The diamond model of intrusion analysis. DTIC Document, Tech. Rep. 2013. 21 P.

3. Hutchins E. M., Cloppert M. J., and Amin R. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research. 2011. Vol. 1. P. 80-82.

4. Schneier B. Attack trees. Dr. Dobbs journal. 1999. Vol.24. No. 12. P. 21-29.

Ключові слова: інформаційна безпека, кібербезпека, модель, динамічні системи, нелінійність, методи, кібератаки.

Ключевые слова: информационная безопасность, кибербезопасность, модель, динамичные системы, нелинейность, методы, кибератаки.

Keywords: information security, cybersecurity, model, dynamic systems, nonlinearity, methods, cyber attacks.

Орлов Сергей Вячеславович

Національний університет «Одеська юридична академія»,
старший преподаватель кафедры информационных технологий

ПРОБЛЕМА УДЛИНЕНИЯ ТЕКСТА В СИСТЕМАХ ШИФРОВАНИЯ НА ОСНОВЕ КОНЕЧНОГО АВТОМАТА И АВТОМАТА С МАГАЗИННОЙ ПАМЯТЬЮ

Удлинение текстов при шифровании является одной из важных характеристик любой системы шифрования. Шифрование контента все большего объема характерно для современных технологий. Это не только обмен видео, в том числе потокового, но и реализация блок чейн технологий и многое другое. В связи с этим все более важной характеристикой систем шифрования становиться ее способность не очень сильно увеличивать объем информации при шифровании.

Рассмотрим систему шифрования построенной на основе контекстно свободной и регулярной грамматик предложен-

ную в работе [1]. В ней предлагается использовать для шифрования каждой из букв регулярную грамматику. Известно, что каждой регулярной грамматике можно поставить в соответствие конечный автомат [2]. Достаточно просты правила для преобразования регулярных грамматик в конечные автоматы. Эффективная реализация подобной системы шифрования предполагает использование именно конечных автоматов при кодировании символов. Например, детерминированный конечный автомат для кодирования буквы «А», в виде таблицы переходов, может выглядеть следующим образом:

Табл. 1

Конечный автомат для кодирования «А»

$КА_1$-автомат кодирования буквы «А»							
«А”	a	b	c	d	e	f	g
S_0	S_3	S_0		S_2		S_3	
S_1			S_5		S_2		«Допустить»
S_2		S_3			S_1	S_5	
S_3	S_0	S_4					S_0
S_4			S_5	S_2	S_3		S_1
S_5			S_2	S_0			

Этими автоматами будут генерироваться регулярные языки L(КАi). При таком алгоритме шифрования одна буква в исходном тексте будет зашифрована строкой из нескольких символов. В данном случае из множества {a, b, c, d, e, f, g}. Для приведенного автомата удлинение зашифрованного текста может быть и 10 раз. Так как в автомате есть возвраты в предыдущие состояния. Известно, что проблема кодирования, декодирования регулярных языков Р-полная. Взлом подобного шифра тоже является Р-полной задачей. Крипто стойкость такой системы шифрования не высокая. Поэтому в работах [1; 3] предлагается проводить отсеивание части полученных кодирующих строк при помощи контекстно свободной грамматики.

На самом деле удобнее, на практике, воспользоваться автоматом с магазинной памятью. Так как известно, что каждой контекстно свободной грамматике можно поставить в соответствии автомат с магазинной памятью. Полученный, таким образом, язык позволяет добиться устойчивости к взлому на уровне NP-полных задач [4].

Для контролируемого и гарантированного удлинения текста менее чем в 2 раза предлагается кодировать символы алфавита в двоичной системе при помощи таблиц переходов ограниченного размера. При этом будем строить матрицу переходов таким образом, чтобы в ней не было возвратов в предыдущие состояния. Например, матрица для кодирования «А» может выглядеть в этой системе следующим образом **КА1*** – конечный автомат кодирования буквы **«А»**:

Табл. 2.

Конечный автомат для двоичного кодирования «А», с контролируемым удлинением

«А»	0	1
S_1	S_2	
S_2	S_5	S_3
S_3	S_4	S_5
S_4	S_5	
S_5		S_6
S_6		Допустить

В соответствии с этой таблицей переходов символ «А» может быть закодирован любой бинарной строкой, словом из языка L(**КА1***), который может быть описан множеством {0011,01111,010011}. Предложим кодировать остальные буквы алфавита подобными автоматами, придерживаясь следующих правил:

1. Количество строк состояний в КА возьмем минимум – 6.

2. Функции выхода, «Допустить» может быть расположены начиная с 4 строки состояния.

3. Функции переходы можно не менять для каждого нового символа слишком часто (для автоматизации генерации таблиц перехода).

4. В таблице переходов будут отсутствовать переходы на предыдущие состояния.

5. Пустые клетки конечного автомата означают выход – «Отвергнуть».

6. Сгенерированные конечными автоматами языки L(КАi) не должны пересекаться, содержать одинаковые слова для кодировки разных символов.

Например, букву «Б» можно закодировать конечным автоматом следующего вида:

Табл. 3.

Конечный автомат для двоичного кодирования «Б», с контролируемым удлинением

«Б»	0	1
S_1	S_2	
S_2	S_5	S_3
S_3	S_4	S_5
S_4	S_5	
S_5		Допустить

В соответствии с этой таблицей переходов символ «Б» может быть закодирован следующими бинарными строками, словами из множества L(**КА2***) = {001,0111,01001}. Очевидно, что эти языки, множества не пересекаются.

Для шифрования букв латинского алфавита потребуется 5 бит, а кириллицы 6 бит. Очевидно, что после шифрования

строка может быть длиннее на бит лишь в редких случаях. Максимальное удлинение зашифрованного текста в приведенном примере будет 1/6. Иногда зашифрованный текст может быть даже короче исходного. Однако при наличии кодирующего множества, языка L(**KAi***) хотя бы размером в 2 слова для каждой буквы мы гарантировано получим удлинение зашифрованного текста хотя бы на 1 бит. Иначе невозможно будет добиться не пересекающихся кодирующих множеств для всех символов алфавита. Поэтому, для реализации системы шифрования как правило потребуется таблица переходов с большим количеством состояний-строк.

В вышеприведенной системе шифрования, при существенном уменьшении коэффициента расширения зашифрованного текста может понизиться крипто стойкость. Очевидно возможность кодировать один и тот же символ разными битовыми словами повышает крипто стойкость системы шифрования. Корреляция крипто стойкости и коэффициента удлинения зашифрованного текста для данной системы шифрования недостаточно изучена. Предполагается, что уже при небольшом коэффициенте расширения, например, 1,5 или 2 она не существенна.

Список использованных источников:

1. Кондакова С. В., Орлов С. В, «Пример построения возможно односторонней функции на основе контекстно-свободной и регулярных грамматик», сборник научных трудов «Науковий часопис НПУ імені М. П. Драгоманова. Серія 1. Фізико-математичні науки», вып.13(2), 2012, С. 77–84.

2. Джон Хопкрофт, Раджив Мотвани, Джеффри Ульман. Введение в теорию автоматов, языков и вычислений, Introduction to Automata Theory, Languages, and Computation. – М.: «Вильямс», 2002, 528с

3. Орлов С. В., Система шифрования на основе контекстно зависимых и регулярных грамматик, 3 международная конференция «Компьютерная алгебра иинформационные технологии», ОНУ, Украина, 20–25 августа 2018 г., С. 113–116.

4. М. Герри, Д. Джонсон, «Вычислительные машины и трудно разрешимые задачи», М.: Мир, 1982., 419 с.

Ключові слова: кінцеві автомати, автомати з магазинною пам'яттю, система шифрування.
Ключевые слова: конечные автоматы, автоматы с магазинною памятью, система шифрования.
Keywords: finite-state machine, pushdown automaton, encryption system.

Онацкий Алексей Витальевич
Национальный университет «Одесская юридическая академия»,
преподаватель кафедры кибербезопасности,
кандидат технических наук, доцент

Поляков Дмитрий Владимирович
Одесская национальная академия связи им. А. С. Попова,
студент 7 курса специальности 125 – Кибербезопасность

Дубовой Ярослав Владимирович
Одесская национальная академия связи им. А. С. Попова,
студент 6 курса специальности 125 – Кибербезопасность

ПРОТОКОЛ АУТЕНТИФИКАЦИИ НА ОСНОВЕ КРИПТОСИСТЕМЫ NTRU

Протоколы аутентификации можно рассматривать как вид интерактивного доказательства знания. Интерактивное доказательство – понятие теории сложности вычислений, составляющее основу понятия доказательства с нулевым разглашением (zero-knowledge proof – ZKP) [1…3]. Широкое распространение получили криптографические протоколы ZKP на базе ассиметричного шифрования, наиболее известными являются: Fiat–Shamir, Schnorr, Okamoto, Guillou–Quisquater, Brickell–McCurley, Feige–Fiat–Shamir [1 … 3].

Целью работы является разработка протокола ZKP на основе криптосистемы NTRU (Nth-degree TRUncated polynomial

ring) [4], которая стойкая к атакам, осуществляемым на квантовых компьютерах (рис. 1). Криптосистема NTRU основана на решетчатой криптосистеме (lattice cryptosystem), в которой используются операции над кольцом усеченных многочленов степени, не превосходящей $n - 1$. В системе шифрования NTRU используем следующие обозначения: n – размерность кольца многочленов; p и q – натуральные взаимно простые числа НОД$(p, q) = 1$.

Пусть числа n, p, q известны участникам информационного процесса; $g(x)$ – многочлен в кольце $Z[X]/(q, X^n - 1)$ предварительно согласован; $f(x)$ – многочлен в кольце $Z[X]/(X^n - 1)$, причем для многочлена $f(x)$ существуют обратные многочлены $F_p(x)$ и $F_q(x)$. Абонент A вычисляет значения открытого ключа $Y_a(x) = F_q(x)g(x)$, который передает абоненту B вместе с заявкой γ. Абонент B выбирает случайный многочлен $r(x)$, сообщение $M(x)$ и вычисляет запрос – $y(x) = pY_a(x)r(x) + M(x)$, который передает абоненту A. Абонент A определяет $M(x) = (F_p(x)(f(x)y(x)(q, x^n - 1))(p, x^n - 1)$ и передает ответ – $X(x) = f(x)M(x)h(x)$ абоненту B. Абонент B проверяет равенство $Y_a(x)X(x) = \gamma M(x)g(x) = h(x)M(x)g(x)$.

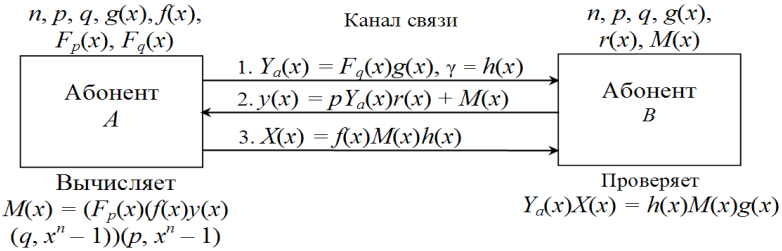


Рис. 1. Протокол аутентификации на основе криптосистемы NTRU

Полнота протокола. Абонент A расшифровывает сообщение $M(x)$, пользуясь своим секретным ключом. Докажем, что абонент A может расшифровать $M(x)$. Абонент A получает

от абонента B запрос $y(x) = (M(x) + pY_a(x)r(x))(q, x^n - 1)$, так как $Y_a(x) = (F_q(x)g(x))(q, x^n - 1)$, то $y(x) = (M(x) + pF_q(x)g(x)r(x))(q, x^n - 1)$.

Умножим левую и правую части равенства $y(x)$ на $f(x)$ по модулю q:

$$(f(x)y(x))(q, x^n - 1) = (f(x)(M(x) + pF_q(x)g(x)r(x)))(q, x^n - 1);$$

$$(f(x)y(x))(q, x^n - 1) = (f(x)M(x) + pg(x)r(x))(q, x^n - 1).$$

Умножим левую и правую части полученного равенства на $F_p(x)$:

$$(F_p(x)(f(x)y(x)(q, x^n - 1))(p, x^n - 1) = (F_p(x)(f(x)M(x) + pg(x)r(x))(q, x^n - 1))(p, x^n - 1) =$$

$$= (F_p(x)(f(x)M(x)(q, x^n - 1))(p, x^n - 1) + (F_p(x)pg(x)r(x))(q, x^n - 1))(p, x^n - 1) = M(x).$$

Абонент A расшифровал $M(x)$. Абонент A знает значения $f(x)$ и $F_p(x)$, поэтому он в состоянии ответить на любые запросы абонента B. При этом проверяющий абонент B убеждается в справедливости соотношения

$$Y_a(x)X(x) = F_q(x)g(x)f(x)M(x)\gamma(x) = h(x)M(x)g(x).$$

В работе приведено математическое обоснование, пример расчета, которые показывают, что предложенный протокол, на основе алгебраической структуры полиномиального кольца, работает корректно и технически реализуем. Стойкость протокола ZKP NTRU обеспечивается трудностью нахождения кратчайшего вектора в заданной числовой решетке, что в свою очередь делает протокол устойчивым к атакам на квантовых компьютерах.

Список использованных источников:

1. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C / B. Schneier. – Wiley, 2015. – 784 p.
2. Молдовян А. А. Протоколы аутентификации с нулевым разглашением секрета / А. А. Молдовян, Д. Н. Молдовян, А. Б. Левина. – СПб: Университет ИТМО, 2016. – 55 с.
3. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – 816 p.
4. NTRU [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/ wiki/ NTRUEncrypt

Ключевые слова: аутентификация, криптографический протокол, решетчатая криптосистема, алгебраическая структура полиномиального кольца, шифрование.

Ключові слова: автентифікація, криптографічний протокол, решітчаста криптосистема, алгебраїчна структура поліноміального кільця, шифрування.

Keywords: authentication, cryptographic protocol, lattice cryptosystem, algebraic structure of a polynomial ring, encryption.

Толокнов Анатолій Арнольдович
Національний університет «Одеська юридична академія»,
асистент кафедри інформаційних технологій

ОГЛЯД І КЛАСИФІКАЦІЯ ОСНОВНИХ ПОГРОЗ WEB-ЗАСТОСУНКІВ

З ростом кількості та значення різних веб-сервісів в суспільному житті, наприклад, таких як банківські послуги, покупка товарів он-лайн та ін., також зростає значення забезпечення їх безпеки. Ефективність забезпечення безпеки може зростати якщо знати звідки чекати загрози. Попереджений – значить озброєний – прислів'я, зміст якого полягає в тому, що будучи попереджений про близьку небезпеку (або можливість такої), людина тепер до неї підготовлена і може з нею впоратися. Це в рівній мірі відноситься і до web-застосунків.

У даному невеликому огляді ми розглянемо основні загрози web-застосунків, а також наведемо приклади їх класифікації.

Повний список загроз безпеки веб-сайтів можна розглянути в розділі «Категорія: атаки» (Open Web Application Security Project) [1]. Також проект OWASP представляє стандартизований список топ 10 основних загроз web-застосунків, які повинні братися до уваги розробниками, перш ніж приступати до створення web-застосунків [2].

Крім цього Консорціум безпеки web-застосунків (WASC), www.webappsec.org, міжнародна організація, що об'єднує професіоналів в області безпеки web-застосунків, випустила

документ Threat Classification v2.0, що представляє собою класифікацію вразливостей і атак, які можуть завдати шкоди веб-сайту, інформації, яка ним обробляється або його користувачам [3]. Документ, в першу чергу, буде корисний для фахівців в області безпеки web-застосунків як довідкове керівництво.

З точки зору забезпечення безпеки інформації, що циркулює в автоматизованих (комп'ютерних) системах, вказуються такі важливі властивості інформації: конфіденційність, цілісність, доступність [4].

Зазначені властивості інформації є базовими для побудови будь-якої системи захисту інформації, незалежно від виду і характеристик об'єкта інформатизації.

Конфіденційність (*information confidentiality*) – суб'єктивно визначена властивість інформації, яка вказує на необхідність введення обмежень на коло суб'єктів, що мають доступ до неї. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила її отримання або ознайомлення з нею.

Цілісність (*information integrity*) – властивість інформації, яка полягає в її існуванні в незмінному вигляді на певному проміжку часу. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації та/або видалення.

Доступність (*information availability*) – властивість інформації бути наданою своєчасно і безперешкодно всім суб'єктам, які мають для цього належні повноваження. Інформація зберігає доступність, якщо протягом певного проміжку часу легітимним (авторизованим) користувачам немає відмови (блокування) в її отриманні.

У [5] пропонується наступна класифікація загроз безпеки web-застосунків:

1. Загрози, пов'язані з експлуатацією вразливостей в коді web-застосунка:
    a. SQL-ін'єкції
    b. XSS атаки
    c. PHP-ін'єкції
    d. Підробка міжсайтових запитів – CSRF

2. Мережеві атаки
    a. Атаки на браузер клієнта web-застосунка
    b. Перебір паролів і атаки на систему аутентифікації користувачів
    c. Відмова в обслуговуванні сервісів web-застосунків
    d. Сканування мережі
    e. Виклик виняткових ситуацій
3. Загрози випадкового характеру
    a. Збої і відмови програмно-апаратних засобів
    b. Стихійні лиха
4. Шахрайство
    a. Спам-розсилки
    b. Фішинг
    c. Відмова від зобов'язань у вчинених діях
    d. Порушення авторського права

Ось деякі з основних загроз для web-застосунків [6]:

XSS (Cross-Site Scripting – Міжсайтовий скриптинг) це термін, який використовується для опису типу атак, які дозволяють зловмисникові впроваджувати шкідливий код через веб-сайт в браузери інших користувачів. Оскільки впроваджений код надходить в браузер з сайту, він є довіреним і може виконувати такі дії, як відправка авторизаційного файлу cookie користувача зловмисникові. Коли у зловмисника є файл cookie, він може увійти на сайт, нібито б він був користувачем, і зробити все, що може користувач, наприклад, отримати доступ до даних кредитної картки, переглянути контактні дані або змінити пароль.

SQL-ін'єкції дозволяють зловмисникам виконувати довільний код SQL в базі даних, дозволяючи отримувати, змінювати або видаляти дані незалежно від дозволів користувача. Успішна ін'єкційна атака може підробити посвідчення, створити нові посвідчення з правами адміністратора, отримати доступ до всіх даних на сервері або знищити / змінити дані, щоб зробити їх непридатними для використання.

Підробка міжсайтових запитів (Cross-Site Request Forgery – CSRF) дозволяють зловмиснику виконувати дії,

використовуючи облікові дані іншого користувача, без його відома або згоди.

Інші поширені атаки / уразливості включають:

Clickjacking. У цій атаці зловмисник перехоплює кліки, призначені для видимого сайту верхнього рівня, і направляє їх на приховану нижче сторінку. Цей метод можна використовувати, наприклад, для відображення законного сайту банку, але захоплення облікових даних для входу в невидимий <iframe>, контрольований зловмисником.

Відмова в обслуговуванні (DoS) – зазвичай досягається за рахунок наповнення цільового сайту підробленими запитами, так що доступ до сайту порушується для законних користувачів. Запити можуть бути просто численними або окремо споживати великі обсяги ресурсів (наприклад, повільне читання або завантаження великих файлів).

Обхід каталогів (файл і розкриття). У цій атаці зловмисник намагається отримати доступ до частин файлової системи веб-сервера, до яких у нього не повинно бути доступу.

Включення файлу. У цій атаці користувач може вказати «ненавмисний» файл для відображення або виконання в даних, переданих на сервер.

Впровадження команд. Атаки з впровадженням команд дозволяють зловмиснику виконувати довільні системні команди в операційній системі сервера.

7 найпоширеніших типів кібератак на web-застосунки у 2020 році [7]:

1. атака з використанням SQL-ін'єкції,
2. атака міжсайтового скриптинга (XSS),
3. атака типу відмова в обслуговуванні (DoS) / розподілена відмова в обслуговуванні (DDoS),
4. атака впровадження команд ОС,
5. атака з використанням LDAP-ін'єкції (Lightweight Directory Access Protocol – Полегшений протокол доступу до каталогів),
6. атака грубої сили (brute force attack),
7. атака нульового дня.

Необхідно не забувати про дотримання базових заходів безпеки при розробці та підтримці роботи сайту: оновлювати CMS і її компоненти; регулярно міняти паролі; відмовитися від використання застарілих протоколів; налаштувати і використовувати HTTPS/HSTS.

Список використаних джерел:

1. List of Attacks / Open Web Application Security Project. [Електронний ресурс] URL: https://owasp.org/www-community/attacks/ (дата звернення: 8.11.2020).

2. Top 10 Web Application Security Risks / Open Web Application Security Project. [Електронний ресурс] URL: https://owasp.org/www-project-top-ten/ (дата звернення: 8.11.2020).

3. The WASC Threat Classification v2.0 / The Web Application Security Consortium. [Електронний ресурс] URL: http://projects.webappsec.org/w/page/13246978/Threat%20Classification (дата звернення: 8.11.2020)

4. Емельянов С. Л. Проблема защиты информации от утечки и пути ее решения: моногр. / С. Л. Емельянов. – Одесса: Фенікс, 2011. – С. 18.

5. Оладько В. С., Микова С. Ю., Нестеренко М. А. Технологии защиты интернет-технологий и web-приложений / *Международный научный журнал*, № 8, 2015. С. 81–85.

6. Веб-безопасность / MDN Web docs. [Електронний ресурс] URL: https://developer.mozilla.org/ru/docs/Learn/Server-side/First_steps/%D0%92%D0%B5%D0%B1_%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C (дата звернення: 8.11.2020)

7. Top 7 Most Common Types of Cyberattacks on Web Applications in 2020 / Penta Security, 2020–03–19 [Електронний ресурс] URL: https://www.pentasecurity.com/blog/top-7-common-types-cyberattacks-web-applications/ (дата звернення: 8.11.2020)

Ключові слова: інформаційна безпека, інтернет, загрози й атаки на web-застосунки.

Ключевые слова: информационная безопасность, интернет, угрозы и атаки на web-приложения.

Keywords: information security, internet, threats and attacks on web applications.

Пастернак Юрій Юрійович
Національний університет «Одеська юридична академія»,
студент 1-го курсу магістратури факультету кібербезпеки
та інформаційних технологій

СПОСІБ ВИКОРИСТАННЯ ЕЛЕМЕНТАРНИХ КЛІТИННИХ АВТОМАТІВ ДЛЯ ШИФРУВАННЯ ДАНИХ

Клітинні автомати – це дискретна модель, набір клітинок що формують решітку значень, які залежать від стану клітини в момент часу та стану клітин-сусідів. Клітинні автомати, незважаючи на простоту опису їх клітин, як складових частин, можуть мати дуже складну поведінку. Кожна клітина в кожен момент часу може мати один з кінцевої множини станів. Однорідний бінарний клітковий автомат з двома можливими станами, в якому стан клітини в кожен момент часу залежить лише від її особистого стану і стану суміжних з нею клітин в минулий момент часу називають елементарним автоматом [1]. Кожна клітина автомату може приймати значення 0 чи 1. В кожен момент часу кожна клітина може мати різне значення. Це дає можливість використати множину значень клітин у якості ключа для XOR-шифрування. Таким ключем може виступити n-ітерація зміни значень клітин. У цій ситуації виникає проблема кінцевості автомату та теоретичної можливості розшифрування даних за допомогою повернення до його початкового стану.

Спосіб використання алгоритму буде наступним: спочатку необхідно розбити строку інформації, яку необхідно зашифрувати на окремі символи, а потім код кожного окремого символу необхідно розташувати в клітини автомату. Після цього використовується правило переходу станів та через n-число ітерацій автомату результат його еволюції необхідно використати як код символу. Таку процедуру необхідно повторити для кожного символу строки інформації. У результаті отримується зашифрований текст. Загрозою розкриття такого шифру може бути метод грубої сили, завдяки якому можна

розшифрувати текст, повернувши автомат до первинного значення (особливо враховуючи існування лише 256 елементарних кліткових автоматів[2]). Звісно, навіть у такій ситуації розшифрування займе дуже велику кількість часу, але метод можна ускладнити, наприклад, використовуючи його лише як один з етапів шифрування. Також можна використати еволюцію іншого клітинного автомату для повторного шифрування вже зашифрованої інформації. Враховуючи існування 256 елементарних клітинних автоматів, процедуру можна провести 256 раз. В такій ситуації метод грубої сили, скоріш за усе, втратить можливість розшифрувати інформацію через виникнення так званого «комбінаторного вибуху».

Станом на сьогодні клітинні автомати активно використовуються в багатьох сферах наукових досліджень – в фізиці, хімії, біології тощо. В моделях клітинних автоматів вдається доволі точно відтворювати велику кількість природніх явищ завдяки моделюванню процесів, які лежать в їх основі. В цих дослідженнях значною перевагою є регулярна структура решітки клітин автомату, однак в криптографії така регулярність стає недоліком у питанні криптостійкості. Недолік виправляється за рахунок математичного збільшення можливих комбінацій для шифрування та збільшення кількості часу, необхідного для методу грубої сили, але разом зі збільшенням часу, необхідного для дешифрування даних, збільшується і час, необхідний для шифрування.

Останнім часом спостерігається зростання уваги до клітинних автоматів в сфері криптографічних досліджень. Це пояснюється самою природою клітинних автоматів, їх паралельністю та циклічністю. Це дозволяє використовувати їх для одночасної обробки великої кількості процесів. Таким чином, використовуючи паралельні процеси для кожного окремого символу строки, що шифрується, можливо позбавитись проблеми, необхідності занадто великої кількості необхідних ресурсів для шифрування інформації. Таким чином, враховуючи стрімкий розвиток технологій та виникнення нових

обчислюваних можливостей, складнощі використання клітинних автоматів стають все менш актуальними.

Список використаних джерел:

1. Cellular Automata. Stanford Encyclopedia of Philosophy [Електронний ресурс] – Режим доступу до ресурсу: https://plato.stanford.edu/entries/cellular-automata/.

2. Index to Elementary Cellular Automata [Електронний ресурс] – Режим доступу до ресурсу: https://oeis.org/wiki/Index_to_Elementary_Cellular_Automata.

3. Elementary Cellular Automaton [Електронний ресурс] – Режим доступу до ресурсу: https://mathworld.wolfram.com/ElementaryCellularAutomaton.html.

Ключові слова: криптографія, клітинні автомати, шифрування, елементарні клітинні автомати

Ключевые слова: криптография, клеточные автоматы, шифрование, элементарные клеточные автоматы

Keywords: cryptography, cellular automata, encryption, elementary cellular automata.

Науковий керівник: *к.т.н. доцент Бойко В. Д.*

Васильєв Богдан Георгійович
Національний університет «Одеська юридична академія»
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

SQL-ІН'ЄКЦІЯ ТА ЇЇ НЕБЕЗПЕКА

SQL-ін'єкція-це хакерська техніка, яка була виявлена більше п'ятнадцяти років тому і до сих пір доводить свою руйнівну ефективність сьогодні, залишаючись головним пріоритетом безпеки баз даних.

Є багато негативних наслідків SQL-ін'єкції, наприклад, 21 лютого 2014 року на форумі Організації Об'єднаних Націй з управління інтернетом стався витік даних 3215 облікових записів. У серпні 2014 року в Мілуокі компанія комп'ютерної безпеки Hold Security повідомила, що виявила крадіжку

конфіденційної інформації майже з 420 000 веб-сайтів за допомогою SQL-ін'єкцій. У жовтні 2015 року атака з використанням SQL-ін'єкції була використана для крадіжки особистих даних 156 959 клієнтів з серверів британської телекомунікаційної компанії TalkTalk, використовуючи її вразливість в застарілому веб-порталі [1].

Також вона була використана напередодні президентських виборів 2016 року в США для компрометації особистих даних 200 000 виборців штату Іллінойс, а також в гучних атаках проти таких організацій, як Sony Pictures, PBS, Microsoft, Yahoo, Heartland Payment Systems і навіть ЦРУ [2].

SQL-ін'єкції є одним з найбільш часто використовуваних векторів веб-атак, які використовуються з метою отримання конфіденційних даних з організацій. Вкрадені кредитні картки або списки паролів, часто відбуваються через вразливості SQL-ін'єкцій.

SQL-ін'єкція – це метод, який зловмисники застосовують для вставки SQL-запиту в поля введення, а потім обробляють в базовій базі даних SQL. Ці недоліки потім можуть бути використані, коли форми введення дозволяють згенерувавши користувачем SQL-операторам безпосередньо запитувати базу даних.

Для прикладу беремо типовий сценарій, візьмемо типову форму входу, що складається з поля користувача / електронної пошти і поля пароля. Після відправки реєстраційної інформації вона об'єднується з SQL-запитом на веб-сервері користувача. У PHP команді пишеться наступним чином (див. рис. 1):

```
<?PHP
 $query = " SELECT * FROM users WHERE username = '". $_POST ['имя
пользователя']. "'";
 $запрос .= "И пароль = '". $_POST ['пароль']. "'";

 ?>
```

Рис. 1.

Так, він відправляється на сервер, щоб перевірити, чи було йому дано дійсне ім'я користувача з відповідним паролем. Ім'я користувача «Джеймс» з паролем «1111» призведе до цієї команди (див. рис. 2):

```
Выберите * из пользователей, где имя пользователя= 'Джеймс' и
пароль= '1111'
```

Рис. 2.

Але якби поставили щось на кшталт «james '; -», запит виглядав би так (див. рис. 3):

```
Выберите * из пользователей, Где username= 'james'; -- 'и password=
'1111'
```

Рис. 3.

В цьому випадку зловмисник використовує синтаксис коментарів SQL. Що залишився код після послідовності подвійного тире (–) не виконуватиметься. Це означає, що SQL буде (див.рис. 4):

```
Выберите * из пользователей, Где username= 'james';
```

Рис. 4.

Потім він поверне призначені для користувача дані, введені в поле пароля. Цей крок може дозволити обійти екран входу в систему. Зловмисник також може піти далі, додавши ще одну умову вибору, 'або 1 = 1', яке призведе до наступного запиту (див. рис. 5):

```
Выберите * из пользователей, Где username= 'james' или 1=1;
```

Рис. 5.

Запит повертає непорожній набір даних для будь-якого потенційного входу в систему з усією базою даних таблиць «користувачі».

Вищенаведений злом показав значний недолік безпеки для будь-якого сайту, але це лише невеликий приклад того, що він може зробити. Більш просунуті зломи дозволять зловмисникові запускати довільні оператори, завдаючи набагато більший збиток. Так, це може призвести до:

– витоку особистих даних, таких як кредитні картки, паспорти та інш;

– перерахування аутентифікаційних даних користувача, що дозволяють використовувати ці логіни на інших сайтах;

– пошкодження бази даних, виконання команд ОС, віддалені / вставлені дані і зруйновані операції для всього веб-сайту.

Це не повний перелік негативних наслідків.

Успішна атака на базу даних, яка управляє веб-сайтом або веб-додатком, така як атака обходу входу в систему SQL-ін'єкції, потенційно може дати хакеру широкий спектр повноважень, від зміни вмісту веб-сайту («псування») до захоплення конфіденційної інформації, такий як облікові дані облікового запису або внутрішні бізнес-дані. Список команд SQL-ін'єкції по суті такий же, як і список команд бази даних, включаючи потенційно катастрофічні, такі як DROP TABLE.

Отже, зловмисники можуть використовувати уразливості SQL-ін'єкцій для обходу заходів безпеки додатків. Вони можуть обійти перевірку автентичності та авторизацію веб-сторінки або веб-додатки і отримати вміст всієї бази даних SQL. Вони також можуть використовувати SQL-ін'єкцію для додавання, зміни і видалення записів в базі даних.

Уразливість SQL-ін'єкції може вплинути на будь-який веб-сайт або веб-додаток, що використовує базу даних SQL, таку як MySQL, Oracle, SQL Server або інші. Злочинці можуть використовувати його для отримання несанкціонованого доступу до ваших конфіденційних даних: інформації про клієнтів, особистих даних, комерційної таємниці, інтелектуальної власності та ін. Атаки SQL-ін'єкцій є однією з найстаріших, поширених і небезпечних вразливостей веб-додатків.

Але, насправді є багато речей, які власники веб-сайтів можуть зробити, щоб запобігти ін'єкціям SQL. Хоча в мережевої безпеці немає такого поняття, як надійне рішення, але на шляху спроб впровадження SQL можуть бути поставлені величезні перешкоди.

Список використаних джерел:

1. SQL injection [Електронний ресурс] // Wikipediaen – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/SQL_injection.

2. Paul Rubens. How to Prevent SQL Injection Attacks [Електронний ресурс] / Paul Rubens // eSecurityPlanet. – 2018. – Режим доступу до ресурсу: https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks.html.

Ключові слова: SQL-ін'єкція, веб-атака, база даних, конфіденційних даних, зловмисники.

Ключевые слова: SQL-инъекция, веб-атака, база данных, конфиденциальных данных, злоумышленники.

Keywords: SQL injection, web attack, database, sensitive data, attackers.

***Науковий керівник**: к.т.н., доцент Кухаренко С. В.*

Дрига Артем Вадимович
Національного університету «Одеська юридична академія»,
студент 1-го курсу факультету кібербезпеки
та інформаційних технологій

АКТУАЛЬНІСТЬ РОЗРОБКИ КРИПТОСТІЙКИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Нині випадкові числа використовуються в ІТ-розробках різної спрямованості. Послідовності випадкових та псевдовипадкових чисел широко застосовують при реалізації моделювання складних систем та об'єктів, у задачах чисельного аналізу, при розробленні комп'ютерних ігор, в онлайн-сервісах для створення різних паролів, генеруванні електронних підписів для електронного документообігу тощо. Крім того, псевдовипадкові випадкові числа (ПВЧ) і відповідно генератори псевдовипадкових чисел (ГПВЧ) використовуються в задачах захисту даних від несанкціонованого доступу в системах криптографії та інформаційної безпеки: при тестуванні ефективності алгоритмів шифрування, генеруванні унікальних ідентифікаторів, контролі цілісності даних, хешуванні даних, породженні синхронних потокових шифрів і потокових шифрів, що самосинхронізуються, формуванні сигналів, які забезпечують приховану передачу даних, та інших задачах. Саме тому можна стверджувати, що від якості та ефективності методів формування випадкових та псевдовипадкових послідовностей, специфіки відповідних генераторів таких чисел залежать характеристики криптографічних підсистем систем безпеки, позаяк при використанні ненадійного процесу генерації ключів, вся криптосистема в цілому є вразливою.

Генератори псевдовипадкових послідовностей (ГПВЧ), відповідно до стандарту NIST Special Publication 800–90A, можуть бути засновані на використанні функцій хешування, які є необоротними або односторонніми функціями перетворень [1]. Детерміновані алгоритми ГПВЧ генерують майже незалежні один від одного і числа, які підкоряються заданому

розподілу (зазвичай рівномірному) [2]. У такому алгоритмічному (програмному) генераторі задають початкові значення, на базі яких і створюються псевдовипадкові послідовності. Очевидно, що здобута внаслідок таких операцій послідовність не є повною мірою випадковою, оскільки визначається формулою і початковим числом. Хоча для більшості прикладних задач такі ПВЧ цілком прийнятні, проте вони мають свої недоліки. ГПВЧ можна вважати ненадійним, якщо він має:

– надто короткий період генерації послідовності;

– члени послідовності, які недостатньо непередбачувані та незалежні від попередніх.

Щоб ГПВЧ вважався надійним, його алгоритм повинен:

– генерувати послідовність чисел, які мають бути максимально незалежними один від одного та непередбачуваними;

– мати можливість відтворити раніше створену послідовність чисел;

– витрачати тільки ту частину пам'яті комп'ютера, яка необхідна для вирішення поставленої мети.

Суттєвою перевагою програмних ГПВП є «нульова» собівартість, позаяк у вільному доступі є численні бібліотеки для різного програмного оточення.

На відміну від алгоритмічного ГПВЧ, апаратні (фізичні) генератори формують істинно випадкові числа на основі опрацювання вимірюваних, хаотично змінюваних параметрів при протіканні певних фізичних явищ (різного роду шумів, фотоелектричних фотоефектів, квантових явищ тощо) [4]. Попри те, що послідовності, створені цим генератором, можна вважати цілковито випадковими, вони мають низку недоліків, з-посеред яких головними є складність реалізації (такі генератори зазвичай є окремими пристроями) та повільна швидкість їхньої роботи (кількість згенерованих чисел в секунду), у порівнянні з програмним ГПВЧ. Також апаратні генератори залежать від протікання фізичних явищ – при затуханні, генератор деградуватиме. Саме тому їх треба тестувати на статистичну випадковість перед кожним використанням.

Сучасні тенденції побудови таких генераторів використовують різні квантові процеси для генерації випадкових чисел, опису їх імовірнісних схем з позицій квантової фізики. Найбільш відмітною характеристикою квантового ГВЧ є науковий доказ випадковості його вихідних послідовностей, що є гарним рішенням для криптографії та інших сфер застосування, де критично важливою є якість випадкових послідовностей. Проте суттєвим недоліком квантового підходу у пошуку рішень ГВЧ є необхідність застосування доволі габаритних фізичних рішень без можливості їх мініатюризації до рівня застосування сучасних технологій виробництва мікросхем [5].

Проблема створення швидкого, ефективного ГПВЧ, позбавленого традиційних недоліків, є доволі складною, проте актуальною задачею, адже від якості роботи ГПВЧ залежить точність результатів. Наприклад, генерація ключів безпеки, методи шифрування та дешифрування – все це опосередковано залежить від якості та надійності роботи ГПВЧ. Позаяк безпека криптосистеми зосереджена на ключі, то при використанні ненадійного процесу генерації ключів, вся криптосистема в цілому стає вразливою. Перспективним напрямом досліджень є розроблення ГПВЧ, які генеруватимуть послідовності випадкових чисел, максимально наближені до дійсно випадкових послідовностей.

Список використаних джерел:

1. NIST Special Publication 800–90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. 2012. URL: http://csrc.nist.gov/ publica-tions/nistpubs/800–90A/SP800–90A.pdf. (дата звернення: 01.11.2020).

2. Методы генерации случайных чисел / В. С. Гончарук, Ю. С. Атаманов, С. Н. Гордеев. *Молодой ученый.* 2017. № 8(142). С. 20–23. URL: https://moluch.ru/archive/142/40025/ (дата обращения: 01.11.2020).

3. Слеповичев И. И. Генераторы псевдослучайных чисел: учебн. пособие. 2017. Саратов: СГУ, 2017. 118 с.

4. Bardis N.G., Markovskyi A. P., Doukas N., Karadimas N. V. True Random Number Generation Based on Environmental Noise Measurements for Military Applications. *Proceedings of the 8th WSEAS International Conference on Signal Processing, Robotics, and Automation*. 2009. P. 68–73.

5. Гріненко Т.О., Нарєжній О. П. Квантові генератори випадкових чисел в криптографії. *Системи обробки інформації*. 2015. Вип. 10(135). С. 86–89.

Ключові слова: послідовності псевдовипадкових чисел, генератор псевдовипадкових чисел.

Ключевые слова: последовательности псевдослучайных чисел, генератор псевдослучайных чисел.

Keywords: sequences of pseudorandom numbers, pseudorandom number generator

***Науковий керівник**: к.т.н., доц. Трофименко О. Г.*

Дроздов Богдан Михайлович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

СИСТЕМА ІДЕНТИФІКАЦІЇ З ЕЛЕМЕНТАМИ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ

Охорона всякого об'єкта включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках значущим кордоном буде система управління контролю доступом (СУКД) на об'єкт.

Якісно організована із застосуванням новітніх технічних засобів СУКД дозволить вирішувати цілий ряд завдань. До числа особливо головним можна віднести наступні:

- протидія індустріального шпигунства;
- протидія розкраданню;
- протидія саботажу;

- протидія умисного пошкодження матеріальних цінностей;
- контроль робочого часу;
- контроль своєчасності приїзду і звільнення працівників;
- охорона конфіденційності інформації;
- регулювання потоку відвідувачів;
- контроль в'їзду та виїзду транспорту.

Крім цього, СУКД є бар'єром для «цікавих». При реалізації певних СУКД застосовують різні методи і реалізують їх пристрої для ідентифікації і аутентифікації особи. Слід зазначити, що СУКД є одним з особливо розвинених секцій ринку безпеки як в Україні, так і за кордоном.

За даними ряду експертів річний прихід ринку СУКД становить більше двадцять п'ять відсотків. Число фахівців, що працюють в галузі технічних систем безпеки, перевищило п'ятсот тис. чоловік.

Як особливо часто використовуваних СУКД можна назвати наступні:

- турнікети звичайні настінні;
- турнікети для проходу в коридорах;
- шлюзові кабіни;
- механічні хвіртки;
- роторні турнікети;
- обертові двері;
- дорожні блокіратори;
- шлагбауми;
- паркувальні системи;
- круглі розсувні двері;
- трехштанговіе турнікети;
- повнозростові турнікети;
- розсувні турнікети.

Головним є питання про засоби інтеграції СУКД з всякий системою безпеки із застосуванням відкритого протоколу. Значущою специфікою ринку СУКД є те, що покупці стали купувати більше дорогі виконавчі пристрої, причому іноземного виробництва.

Іншою специфікою новітніх СУКД є впровадження спецспецтехнології смарт-карти, натомість класичних проксімітікарт, технології далекої ідентифікації (частоти 800–900 МГц і 2.45 ГГц).

Як вже говорилося вище, будь-яка СУКД призначена для того, щоб автоматично пропускати тих, кому цей вхід дозволений, і не пропускати тих, кому вхід заборонений. Всі її інші функції (збереження матеріальних цінностей, контроль і облік робочого часу і ін.) що є результатом основного призначення.

У загальному випадку під СУКД зазвичай розуміють сукупність программнотехніческіх і організаційно-методичних засобів, за допомогою яких вирішується завдання контролю і управління приміщенням підприємства і окремими приміщеннями, а також оперативний контроль за пересуванням персоналу і часу його перебування на території підприємства.

Для багатьох організацій завдання контролю праці, а також підвищення продуктивності і трудової дисципліни є дуже актуальними.

Більшість підприємств бажають платити своїм співробітникам тільки за відпрацьований ними час, виключивши запізнення, передчасні відходи і самовільні відлучки з роботи. Дуже важливо стежити за роботою співробітника протягом робочого часу, адже своєчасне поява не можна назвати гарантією сумлінного виконання всіх обов'язків. Тому варто використовувати вже готові рішення [1].

Багато компаній знають, що таке СУКД і як її використовувати. Вона вже довго допомагає керівникам, співробітникам бухгалтерії і відділу кадрів вирішувати завдання, пов'язані з управлінням доступу і контролем відповідно до Трудового законодавства. Саме системи контролю створюють доказову базу під час трудових спорів, за допомогою якої запобігають зловживання і помилки.

Можна зробити висновок що системи контролю та управління доступом в наш час дуже актуально як в сфері захисту, так і в повсякденному житті. Ми часто стикаємося з

прикладами їх застосування в банках, пропуск в приміщення тощо.

Список використаних джерел:

1. Сабынин В. Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // *Информост – радиоэлектроники и телекоммуникации*, 2001. № 3 (16).

Ключові слова: Система управління контролю доступом, контроль, система безпеки, технічні засоби.

Ключевые слова: Сисетема контроля доступа, контроль, система безопастности, технические средства.

Key words: Access control system, control, safety system, technical means.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Золотоверх Денис Олегович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ОЗНАК КРИПТОСТІЙКИХ ХЕШ-ФУНКЦІЙ

Хеш-функції надзвичайно корисні і з'являються майже у всіх програмах захисту інформації.

Хеш-функція – це математична функція, яка перетворює числове вхідне значення в інше стиснене числове значення. Вхід у хеш-функцію є довільної довжини, але вихід завжди має фіксовану довжину.

Значення, що повертаються хеш-функцією, називаються дайджестом повідомлення або просто хеш-значеннями.

Хеш функціям притаманні наступні ознаки:

Дайджест фіксованої довжини. Кожна хеш функція може приймати на вході повідомлення довільної довжини, та на виході видавати дайджест однієї, чітко визначеної довжини.

Дайджест може мати будь-яку довжину, якщо розглядати на прикладах найпопулярніших імплементацій хеш функцій (SHA-1, MD-5, SHA-2), то довжина блоку становить зазвичай 160, 256 та 512 біт. Але слід зазначити, що одна хеш функція може працювати у різних режимах, маючи різну довжину даджесту.

З попередньої властивості випливає те, що вихідні дані зазвичай містять меншу кількість інформації, а тому хеш функції також називають функціями стиснення.

Функція хешу покриває дані довільної довжини до фіксованої довжини. Цей процес часто називають хешуванням даних.

Як правило обчислення дайджесту є нескладною операцією з точки зору об'ємів обчислювальних ресурсів. Але обчислення вхідного повідомлення, навпаки є дуже складною задачею, що навпаки вимагає величезну кількість обчислювальних ресурсів.

Але для використання хеш функції як методу захисту інформації, до неї ставляться певні вимоги.

Дайджести хеш функції мають бути рівномірно розподілені, тобто хеш значення має генеруватися у вихідному діапазоні з однаковою рівномірністю, тобто діапазоном є усі значення дайджестів, наприклад для MD5 вихідним діапазоном є значення від 00000000000000000000 до ffffffffffffffff, якщо їх представити у 16-рядковому форматі. А кожний біт дайджесту повинен генеруватися з вірогідністю, що наближається до 50% [1].

Хеш функція повинна приймати дані будь-якого формату, зазвичай алгоритми хешування приймаються масив байтів, що забезпечує їх універсальність.

Хеш функція є детерміністичною, вхідне повідомлення завжди генерує один дайджест. Тобто алгоритми хешування не використовують генератори псевдовипадкових чисел, або певні вхідні дані, які неможливо отримати при повторному використанні алгоритму (наприклад часу доби, атмосферного тиску інше). Також не повинно мати значення адреси

пам'яті об'єкта. Припускається використання зерна генерації або вектору ініціалізації, але зазвичай такі механізми не використовуються.

Ефективність хеш функції є досить важливим аспектом, адже окрім криптографічних методів захисту інформації, вони використовуються для зберігання та пошуку даних. Так наприклад при зберіганні даних простіше зберігати ключ значення файлу, адже його обчислення займає визначений проміжок часу, та не зростає зі збільшенням розміру файлу.

Тому хеш-функції повинні обчислюватись досить швидко, на відміну від алгоритмів блокового симетричного шифрування, що є дуже схожими за будовою та принципом дії. Для цього при обчисленні використовується мінімальна кількість інструкцій. Зазвичай для забезпечення швидкості використовуються прості логічні та арифметичні оператори. Але використання операторів множення і особливо ділення використовуються рідко через їх складність реалізації на апаратному рівні [2].

Одним із визначальних атрибутів алгоритмів хешування є наявність колізій. Колізією є випадок, коли дайджест одного повідомлення є ідентичним до дайджесту іншого. Це пов'язано з тим, що при визначеній довжині дайджесту, існує невизначена кількість можливих повідомлень.

Вірогідність колізії, є незначущою, і у криптостійких алгоритмів хеш-функцій наближається до теоретичного мінімуму. Зазвичай при використанні наявність колізій або ігнорується, або вирішується (наприклад додавання солі при зберіганні хеш-таблиці паролів), але також існує можливість використання ін'єктивної хеш-функції [3].

Вірогідність колізії напряму залежить від довжини дайджесту хеш-функції, але великий розмір ключа напряму негативно впливає на швидкість обичлення.

Як вже було зазначено за принципом дії, алгоритми хешування за механізмом дії на алгоритми блокового симетричного шифрування.

Розмір кожного блоку даних змінюється залежно від алгоритму. Зазвичай розміри блоків становлять від 128 до 512 біт. Якщо повідомлення не «заповнює» блок, створюються відступи.

Над кожним блоком здійснюються визначені операції елементарної логіки та арифметики. Перший блок «перемішується» з вектором ініціалізації, що, зазвичай, чітко визначений алгоритмом. Другий блок «перемішується» з першим і т.д.

У криптографічних функціях необхідна наявність лавинного ефекту, його показником є наявність двох істотно різних дайджестів для повідомлень, які відрізняються одним бітом [4].

Отже, це математична функція яка перетворює числове вхідне значення в інше стиснене числове значення. Хеш функція має повертати дайджест сталої довжини, а довжина повідомлення не має значення. Вона повинна бути швидкою та односторонньою.

Криптографічно стійким вважається алгоритм хешування, якщо в ньому наявні такі ознаки, як рівномірність розподілення дайджестів, детерміністичність, наявність лавинного ефекту, а вірогідність колізії є теоретично мінімальною.

Список використаних джерел:

1. Брюс Шнайер, «Прикладна криптографія» 2е видання Тріумф, 2002

2. Брюс Шнайер. «Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові Си» Тріумф, 2002

3. Єршов Ю. Л., Палютін Е. А. Математична логіка: Навчальний посібник. – 3-е, стереотип. изд. – СПб .: Лань, 2004. – 336 с.

4. Кастро та ін., 2005, «Суворий критерій критерію випадковості», Математика та комп'ютери в моделюванні, 2005

Ключові слова: Хеш-функція, колізія хеш-функції, дайджест, шифрування, симетричне шифрування.

Ключивые слова: Хеш-функция, коллизия хеш-функции, дайджест, шифрование, симмнтрическое шифравания.

Key words: Hash-function, hash-function collision, digest, cypher, symmetric cypher.

***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*

Иванова Ирина Александровна
Национальный университет «Одесская юридическая академия»,
студентка 2-го курса факультета кибербезопасности
и информационных технологий

DRIVE-BY ЗАГРУЗКИ

На современном этапе, развития информационных технологий, за персональными данными и возможностью управлять пользовательскими компьютерами, разворачивается настоящая охота. Хакеры создают более сложные и вредоносные вирусы, а специалисты по кибербезопасности строят все более сложную защиту. Несмотря на то, что киберграмотность самих пользователей растет, появляются новые вирусы, заражения которыми сложно избежать. Поскольку некоторые из них хорошо замаскированы, их носителями могут быть, даже официальные сайты и приложения, которыми пользователь постоянно пользуется.

К примеру, группа кибершпионажа под названием Patchwork (или Dropping Elephant) использовала метод drive-by загрузки для создания вредоносного видео-сайта нацеленного на жителей Китая, под названием YoukuTudou. Который загружал и выполнял xRAT троян под видом обновления Adobe Flash Player [1].

Распространение и установка вредоносного кода или программного обеспечения методом Drive-by загрузок, очень привлекает киберпреступников, так как он является более «скрытой» технологией, которая используется операционными системами, приложениями или браузерами для перенаправления пользовательского соединения на сервера с пакетами эксплойтов.

Причин, по которым хакеры при атаках направленных на взлом устройств пользователей используют drive-by загрузку, может быть несколько: кража учетных данных, личной информации, создание ботнетов, заражение других устройств, выведение из строя самого устройства или нане-

сение вреда данным. Всё это легко сделать без наличия необходимого программного обеспечения для защиты операционной системы пользователя, и актуальных версий приложений и браузеров [2].

Существует два основных метода распространения вредоносных программ через загрузку:

1. **Разрешенная загрузка со скрытыми данными.**

Сначала хакер создает носитель для доставки вредоносной программы на устройство пользователя, который может получить замаскированную ссылку, увидеть рекламу или сообщение в ленте социальных сетей, как будто оно было отправлено из источника, которому он доверяет. Это побуждает пользователя перейти по ссылке. И в тот момент, когда веб-страница со встроенным в него эксплойтом открывается, на компьютер или мобильное устройство, устанавливается непреднамеренная загрузка. После установки, хакер успешно проникает в устройство и получает контроль над вашими данными.

Для этого способа хакеры используют метод Bundleverware и Фишинг.

Bundleware – метод объединения разных программ, в том числе и вредоносных, в один загрузочный файл, который на ряду с загрузкой желательной программы, устанавливает вредоносную программу на устройство пользователя.

Фишинг – используется для того, чтобы с помощью сообщений или всплывающих окон, от источников которым пользователь доверяет, заставить пользователя выполнить скачивание. Чаще всего, ссылки на установку вредоносных программ скрыты за ложными уведомлениями о нарушении работы браузера или электронными письмами о взломе аккаунта пользователя.

2. **Неразрешенная загрузка без ведома пользователя.**

Сначала злоумышленник взламывает веб-страницу и помещает туда вредоносный компонент. После этого, пользователи посещают страницу, которая переадресовывает соединение на вредоносный сервер, на котором хранится набор эксплойтов,

которые находят ошибки в пользовательской системе безопасности и выполняют загрузку вредоносного кода.

Этот метод основан на ошибках в программном коде и уязвимостях систем безопасности различных устройств, с которыми для проведения атак, взаимодействуют комплекты эксплойтов.

Комплекты эксплойтов – программное обеспечение, которое предназначено для взлома веб-сервисов или устройств, методом выявления уязвимостей.

Распространенными формами являются эксплойты нулевого уровня (ошибки безопасности, без известных патчей или исправлений). Довольно часто в наборах эксплойтов хранятся небольшие фрагменты кода, которые позволяют незаметно обойти системы безопасности, а затем ввести оставшуюся часть кода для получения необходимого доступа к мобильному устройству или компьютеру [3].

Как и в большинстве аспектов кибербезопасности, лучшей защитой устройств и персональных данных является предосторожность. Для предотвращения drive-by загрузок, важно позаботиться о безопасности устройства. Чтобы сделать это максимально эффективно, пользователь должен следовать следующим советам:

• не использовать учетную запись администратора, для повседневного использования. Так как для установки drive-by загрузок необходимы права администратора.

• устанавливать актуальные обновления для операционной системы и веб-браузер. Потому что в новых версиях исправлены ошибки в системе безопасности. Уязвимостью, которых может воспользоваться пакет эксплойтов.

• не устанавливать ненужные приложения на устройстве. Следует удалять устаревшие приложения, которые больше не получают обновления. Ведь чем больше подключенных модулей установлено, тем устройство более уязвимо для такого вида атак.

• устанавливать программное обеспечение, к которому есть высокий индекс доверия.

• использовать проверенное антивирусное программное обеспечение и поддерживать актуальное обновление антивирусных баз. Важно, чтобы оно отвечало за безопасность устройства, сканировало веб-сайты, а также инспектировало интернет-трафик. Это обеспечит своевременное обнаружение попыток выполнения drive-by загрузок.

• Избегать посещения подозрительных сайтов, которые могут содержать вредоносный код.

• внимательно изучать всплывающие окна, рекламу в приложениях или браузерах, перед тем как выполнять переход на посторонний сайт. Чтобы избежать перехода на вредоносный сайт, обращайте внимание на зернистость фотографии, опечатки или ошибки в грамматике.

• использовать программное обеспечение или расширения в браузерах, которые блокируют рекламу. Это поможет избежать drive-by атак [4].

Список использованных источников:

1. Drive-by Download. [Электронный документ]. URL: https://www.trendmicro.com/vinfo/ru/security/definition/drive-by-download.

2. Drive-by загрузки. Интернет в осаде. [Электронный документ]. URL: https://securelist.ru/drive-by-zagruzki-internet-v-osade/1139/.

3. What Is a Drive by Download. [Электронный документ]. URL: https://www.kaspersky.com/resource-center/definitions/drive-by-download.

4. Drive By Downloads: What They Are and How to Avoid Them. [Электронный документ]. URL: https://www.exabeam.com/information-security/drive-by-download/

Ключові слова: приховане завантаження, експлойт, кібербезпека.
Ключевые слова: скрытая загрузка, эксплойт, кибербезопасность.
Key words: drive-by download, exploit, cybersecurity.

***Научный руководитель**: к.т.н. доцент Задерейко А. В.*

Коляда Анастасія Миколаївна
Національний університет «Одеська юридична академія»,
студентка 4-го курсу факультету кібербезпеки
та інформаційних технологій

КОРОТКИЙ ОГЛЯД ЯВИЩА ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ ТА ЇХ КЛАСИФІКАЦІЯ

Явище електронних платіжних систем, або систем електронних платежів відносно недавно відрите. Проте, завдяки ряду значущих переваг, набуває все більшої й більшої популярності. Для кожного з нас поняття і призначення таких систем перестало бути чимось новим і ввійшло до переліку звичних і буденних. Так, головним призначенням електронних платіжних систем залишається здійснення онлайн-платежів – оплата товарів та послуг, мобільного зв'язку, комунальних послуг, кабельного та супутникового телебачення, різноманітних послуг провайдерів, онлайн-шопінг.

Електронні платіжні системи використовують платіжним засобом електронні (цифрові) гроші, які являються аналогом готівці. Такий вид платіжного засобу дозволяє миттєво передавати гроші між електронними гаманцями. [2]

Головними методами, що залучені до реалізації безготівкових електронних платежів відносяться кредитні картки, дебетові картки, АСН – сервіс, що контролює транзакції електронних платежів, шляхом використання прямих депозитів, прямих дебетів та електронних чеків. [1]

Такі методи електронних платежів охоплюють три основні типи операцій:

1. Одноразовий платіж від клієнта до постачальника.

Зазвичай використовується, коли ви здійснюєте покупки в Інтернеті на сайті електронної комерції, наприклад Amazon. Ви натискаєте піктограму кошика для покупок, вводите дані своєї кредитної картки та натискаєте кнопку оплати. Сайт обробляє дані вашої кредитної картки та надсилає вам елек-

тронне повідомлення з повідомленням про те, що ваш платіж отримано. На деяких веб-сайтах ви можете використовувати електронний чек замість кредитної картки. Щоб здійснити оплату електронним чеком, ви вводите номер рахунку та номер маршрутизації вашого банку. Постачальник санкціонує оплату через банк клієнта, який потім ініціює електронний переказ коштів (EFT) або друкує чек і надсилає його продавцю.

2. Періодичний платіж від клієнта до постачальника.

Рахунок оплачується регулярно, спланованим прямим дебетом з вашого поточного рахунку або автоматичним стягненням з кредитної картки. Цей тип платежів зазвичай пропонують автомобільні страхові компанії, телефонні компанії та компанії з управління кредитами. Деякі довгострокові контракти (наприклад, у тренажерних залах чи фітнес-центрах) вимагають такого типу автоматизованого графіка платежів.

3. Автоматичний платіж від банку до постачальника.

Використовується, коли ваш банк повинен запропонувати послугу, яка називається Інтернет-оплата рахунків. Ви входите на веб-сайт свого банку, вводите інформацію про постачальника та уповноважуєте свій банк електронним способом перераховувати гроші з вашого рахунку для оплати вашого рахунку. У більшості випадків ви можете вибрати, чи робити це вручну для кожного платіжного циклу, чи автоматично оплачувати рахунки в один день кожного місяця.

Так, не складно зрозуміти, що електронний платіж являється дуже зручним для споживачів. У більшості випадків потрібно лише один раз ввести інформацію про рахунок – наприклад, номер кредитної картки та адресу доставляння. Потім інформація зберігається у базі даних на веб-сервері продавця. Далі при поверненні на веб-сайт, здійснюється тільки процес входу, який використовує вже відоме раніше ім'я зареєстрованого користувача та його пароль. І, в решті решт, завершення транзакція залишається таким же простим, як клік кнопкою миші: необхідно лише підтвердження здійснюваної покупки [1].

Отже, правила користування послугами платіжних систем доволі прості, що і показує доступність даної функції для кожної людини. Так, будь-хто може зареєструвати для себе електронний рахунок. Для цього не вимагається жодних специфічних знань, оскільки усі дії, які необхідно здійснити, являються досить таки інтуїтивними. Наступним вирішальним фактором активного впровадження електронних платіжних систем являється їх мобільність. Завдяки цьому, місце положення користувачів ніяк не впливає на їх здатність здійснення фінансових операцій. Також платежі у мережі характеризують себе як ті, що мають високий рівень оперативності та відзначаються застосуванням стійких криптографічних алгоритмів, що забезпечують безпеку на всіх рівнях процесу електронного обігу коштів у мережі.

Список використаних джерел:

1. Чубенко А. Г., М. В. Лошицький, Д. М. Павлов, С. С. Бичкова, О. С. Юнін. – Держатель електронного платіжного засобу; Довідник учасників СЕП; Система електронних платежів національного банку (СЕП); Користувач платіжної системи; Менеджер програми // Київ: Ваіте, 2018. – С. 211; 224; 615; 363; 395. – [Електронний ресурс] – Режим доступу до ресурсу: http://finmonitoring.in.ua/wp-content/uploads/2018/12/terminologichnij-slovnik_finmonitoring.pdf

2. Про платіжні системи та переказ коштів в Україні: закон України від 05.04.2001 № 2346-III // Відомості Верховної Ради України / Офіційний сайт Верховної Ради України. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2346–14

Ключові слова: система електронних платежів, електронні гроші, покупки.

Ключевые слова: система электронных платежей, электронные деньги, покупки.

Keywords: electronic payment system, electronic money, purchases.

Науковий керівник: *к.т.н., доц. Кухаренко С. В.*

Матковська Інга Олексіївна
Національний університет «Одеська юридична академія»,
студентка 4-го курсу факультету кібербезпеки
та інформаційних технологій

ВИЗНАЧЕННЯ ІНТЕРНЕТ РЕСУРСІВ З ЗАБОРОНЕННИМ КОНТЕНТОМ

Відимо, що процеси глобалізації, в тому числі глобалізації інформаційних технологій, надають необмежені можливості для здійснення впливу на особистість і суспільство. Одним з негативних наслідків розвитку інформаційних технологій є поява і розвиток нової форми злочинності – злочинності в сфері високих технологій, коли комп'ютери або комп'ютерні мережі виступають в якості об'єкта злочинних посягань, а також кошти або способи вчинення злочинів. Проблема кіберзлочинності актуалізувалася в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охопили всі сфери життєдіяльності людини і держави, а глобальна мережа Інтернет стала однією з найбільш швидких складових розвитку телекомунікаційних технологій.

На сьогоднішній день більшість розвинених країн світу вдаються до фільтрації інтернет-контенту і ніякому іншому обмеженню свободи в мережі. Однак цілі, завдання та конкретні механізми реалізації подібних обмежень істотно варіюються. Виділяють саме категорії контенту, які піддаються фільтрації в різних країнах світу. До них відносять: політичний контент; соціально-небезпечну інформацію; контент, пов'язаний з національною безпекою; сайти і сервіси, які порушують економічні інтереси.

Методи цензури контенту в Інтернеті можна розбити на дві категорії: нетехнічні і технічні. До категорії нетехнічних методів відносяться закони, що забороняють публікацію того чи іншого контенту, тиск на інтернет-провайдерів, власників сайтів і користувачів з метою змусити їх прибрати небажані матеріали. До категорії технічних методів відноситься блокування

інтернет-ресурсів за IP-адресою, спотворення DNS-записів, блокування сайтів за URL, пакетна фільтрація, фільтрація через HTTP проксі-сервер, порушення роботи мережі і фільтрація результатів пошуку. Для підвищення ефективності механізмів цензури також активно використовуються різні методи збору інформації в Інтернеті. Через складність і недосконалість технічних інструментів обходу фільтрів до технічних методів вдаються не більше двох відсотків користувачів навіть в тих державах, де фільтрації піддається велика кількість інтернет-ресурсів [2].

Закони, що регулюють Інтернет, визначають методи фільтрації, коли блокується контент, що є спецефічним для кожної держави. Проте, існують групи країн, які переслідують схожі цілі в питаннях інтернет-цензури. Варто привести в приклад континентальну модель, де застосовуються методи фільтрації для блокування контенту. Для континентальної моделі характерна фільтрація соціально-небезпечних ресурсів по чітко позначеним категоріям, а також боротьба з порушеннями авторських прав. Цим методом користуються більшість європейських держав.

Тим самим кіберзлочинність, а саме інтернет ресурси с забороненним контентом визнані глобальною міжнародною проблемою. Найбільші труднощі, що стоять перед правоохоронними органами, полягає в неможливості ефективно координувати свої дії через державні кордони, рамки різних юрисдикцій і законодавчих систем. Протидія кіберзлочинності на увазі цілої системи заходів, що включає в себе аналіз об'єктивних умов, що породжують злочин, механізмів їх здійснення, способів виявлення, припинення, розслідування, досвід судового розгляду. Необхідно також створити ефективні механізми впровадження результатів кримінально-правових і кримінологічних досліджень в законодавчу і нормотворчу практику, а також навчання співробітників правоохоронних органів. В рамках комплексного підходу до боротьби з кіберзлочинністю має бути вирішено ряд загальних і приватних науково-практичних завдань [3].

Незалежно від інтелектуальної бази мислення конкретної людини, специфіки техногенної або соціальної ситуації, в якій він змушений діяти, особливості морально-етичних, моральних установок, ступеня інтенсивності їх відстоювання індивідом всі варіанти прийняття ризикованого рішення об'єднує загальна властивість – вони є реалізацією суб'єктом інтелектуально-особистісних зусиль, спрямованих на зниження рівня невизначеності ситуації. При цьому людина сприймає своє рішення як довільний вибір, здійснений ним відносно вільно (аспект вимушеність присутній завжди, але не завжди пригнічує волю) в рамках певної альтернативи можливих варіантів поведінки. Інформаційна складова цього ризику найбільш вагома у випадках використання прогнозної інформації, дефіциту часу на обробку інформації і ухвалення рішення, в умовах активної інформаційної протидії конкурентів або супротивника. На відміну від інших складових ризику інформаційна складова обов'язково є присутньою в кожній ризиковій події. Змінюється лише її відносна величина.

Достатньо швидко технічні системи захисту все більше й більше удосконалюються за рахунок постійного розвитку сучасних технологій, обліку безлічі потреб, які створюють додаткові ризики. До грамотно відбудованих технічних систем захисту можна тривалий час не підходити і останні будуть справно виконувати свої основні функції та завдання, а люди як і раніше будуть залишатися найбільш вразливою ланкою, коли вони мають доступ до інформації.

Кіберзлочинці користуються тим, що психологічні маніпуляції не вимагають великих витрат і специфічних знань (крім кількох психологічних прийомів), їх можна застосовувати протягом тривалого часу, а ще їх складно виявити. Люди, які володіють цінною інформацією або мають до неї доступ, можна порівняти з доступним плодом: вони на увазі і до них дуже легко дотягнутися [1].

Блокувати інтернет ресурси с забороненним контентом складно, так як цьому сприяє низька інституційна цінність

соціальних медіа в країнах, які продовжують знаходиться в ситуації політичної нестабільності. Дискурс, який показав себе в організації протестного руху, виявився куди менш ефективним після кризових піків. Крім того, відкритий і розширюється громадський дискурс, представлений в соціальних мережах, дозволяє представникам влади відстежувати і аналізувати потенційно кризові явища та запобігання їм.

Значимість оперативного реагування державної влади на порядок соціальних медіа зростає з кожним роком. Поступово це явище втрачає суть феномену і перестає бути надзвичайно популярним об'єктом для вивчення. Соціальні мережі з плином часу стають таким же звичним інструментом мобілізації і значущим фактором при організації масових протестних рухів, як канали традиційних ЗМІ, мобільні засоби зв'язку і безпосереднє «живе» спілкування.

Особливу роль відіграє правильно обрана цільова аудиторія для відповідної інформаційної політики. Наприклад, масове залучення неполітизованих користувачів далеко не завжди приносить бажаний результат. Регулярний моніторинг і аналіз трендів дискусій, виявлення потенційних конфліктів, також важко переоцінити в контексті запобігання кризовим ситуаціям.

Зворотною стороною даної ситуації є силовий сценарій, при якому правоохоронні органи держави отримують полегшений доступ до особистих даних мережевих активістів, підозрюваних в порушенні закону і закликах до масових заворушень.

Тему ризиків в контексті блокувння інтернет ресурсов з забороненим контентом можна продовжуваті і далі, але це все одно не захистить інформаційні технології і апаратуру від зловмісників і шахраїв усіх мастей, так як тотальна мережева цензура (блокування головних ресурсів), яка може бути введена наприклад під час загострення політичної обстановки, не буде гарантувати зниження рівня мобілізації, а навпаки може призвести до ескалації конфлікту поза мережею. Ослаблення соціальних зв'язків у віртуальному просторі дійсно

можуть надати владі тимчасові переваги, але ними треба вміти грамотно скористатися.

Список використаних джерел:

1. Осипенко А. Л. Боротьба зі злочинністю в глобальних комп'ютерних мережах: Міжнародний досвід: монографія. М., 2004. С.185.
2. Ефективне попередження злочинності: в ногу з новітніми досягненнями / Матеріали Десятого Конгресу Організації Об'єднаних Націй з профілактики злочинності і поводження з правопорушниками: A / CONF.187 / 10. Відень, 10–17 квітня 2000 року, п. 5.
3. Будапештська Конвенція про комп'ютерні злочини: [Електронний ресурс]. – Режим доступу: https://rm.coe.int/1680081580

Ключові слова: інтернет ресурси, заборонений контент, кіберзлочин, інформаційні технології.

Ключевые слова: интернет ресурсы, запрещенный контент, киберпреступление, информационные технологии.

Keywords: internet resources, prohibited content, cybercrime, information technology.

***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*

Пальчук Андрій Вікторович
Національний університет «Одеська юридична академія»,
студент 4 курсу факультету кібербезпеки
та інформаційних технологій

РОЗРОБКА КОМПЛЕКСУ ЗАХИСНИХ ЗАХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Конфіденційна інформація входить в сферу підвищеного інтересу конкуруючих компаній. Для недобросовісних конкурентів, корупціонерів та інших зловмисників особливий інтерес представляє інформація про склад менеджменту підприємств, їх статус та діяльності фірми [1].

Термін «безпека інформації» описує ситуацію, яка виключає доступ для перегляду, модерації і знищення даних суб'єктами без наявності відповідних прав. Це поняття включає забезпечення захисту від витоку і крадіжки інформації за допомогою сучасних технологій та інноваційних пристроїв.

Захист інформації включає повний комплекс заходів по забезпеченню цілісності та конфіденційності інформації за умови її доступності для користувачів, що мають відповідні права.

Цілісність – поняття, що визначає збереження якості інформації та її властивостей.

Конфіденційність передбачає забезпечення секретності даних і доступу до певної інформації окремим користувачам.

Доступність – якість інформації, що визначає її швидке і точне знаходження конкретними користувачами.

Мета захисту інформації – мінімізація шкоди внаслідок порушення вимог цілісності, конфіденційності та доступності.

Керівництво підприємства або організації має розробити та впровадити концепцію щодо забезпечення інформаційної безпеки. Цей документ є основоположним для розробки внутрішніх регламентів і системи захисних заходів. Розробку політики безпеки часто доручають запрошеним експертам щодо захисту інформації, здатним провести аудит як інформаційної системи, так і організаційної структури компанії і її бізнес-процесів і розробити актуальний комплекс заходів щодо захисту інформації.

Технічні заходи можуть перешкоджати людям робити несанкціоновані дії, але не можуть перешкоджати їм робити те, що дозволяють їм виконувати їхні робочі функції. Таким чином, щоб запобігти порушенню довіри, а не просто відшкодувати збиток, який виникає, слід залежати, перш за все, від усвідомлення людьми того, що роблять інші люди в організації. Але навіть технічно обґрунтована система з інформованим і пильним управлінням та користувачами не може бути позбавлена всіх можливих вразливостей. Залишковим ризиком

потрібно керувати за допомогою процедур аудиту, резервного копіювання та відновлення, що підтримуються загальною настороженістю та творчими реакціями. Більше того, організація повинна мати адміністративні процедури, щоб доводити особливі дії до відома того, хто може законно дізнатись про доцільність таких дій, і ця особа повинна фактично зробити запит.

Надалі концепція безпеки може стати основою для впровадження DLP-системи та інших програмних продуктів, що вирішують завдання захисту інформаційних ресурсів та інфраструктури компанії.

У концепції забезпечення інформаційної безпеки підприємства визначаються: інформаційні масиви компанії, що підлягають захисту, підстави захисту (встановлені законом або комерційні) [2].

Описуються програмні засоби, фізичні та електронні носії інформації, визначається їх цінність для компанії, критичність зміни або втрати. Цей розділ готується в тісній взаємодії з усіма підрозділами компанії. Система оцінки інформації повинна припускати і установку рівня доступу співробітників до ресурсів; основні принципи захисту інформації.

Зазвичай до них відносяться конфіденційність, комерційна доцільність, відповідність вимогам законодавства. Стратегія забезпечення інформаційної безпеки компанії цілком і повністю будується на цих принципах. Крім того, необхідно визначити політики і правила, ґрунтуючись на яких вибудовується інформаційна система компанії і загальна система захисту інформації; модель загроз інформаційній безпеці, релевантна для компанії в цілому і її окремих бізнес-одиниць, а також модель гіпотетичного порушника. Їм може виявитися конкурент, хакер, але частіше за все інсайдер.

Концепція сама по собі не вирішує завдання відповідальності співробітників компанії за неправомірне поводження з інформацією, в тому числі за її розголошення. Для вирішення цього завдання необхідно впровадити додаткову систему

організаційних заходів захисту інформації, які включають інформування, ознайомлення під розпис, внесення в трудові договори відповідних положень про захист інформації, що становить комерційну таємницю.

Після розробки концепції необхідно приступати до її впровадження. Система пропонованих заходів повинна пройти узгодження у всіх причетних підрозділах компанії, так як питання бюджетування завжди обмежує можливості щодо захисту інформації, складності проведених заходів і придбання програмних продуктів.

Забезпечення безпеки повинно ґрунтуватися на одночасному застосуванні всього комплексу заходів, передбачених законом або пропонованих фахівцями. Технічні та організаційні заходи необхідно співставляти з можливостями організації та інформаційної системи [3].

Система заходів, рекомендована для більшості компаній, перед якими стоїть питання захисту інформації, покликана забезпечити дотримання основних ознак її безпеки:

• доступність відомостей. Під цим визначенням розуміється можливість і для авторизованого суб'єкта в будь-який час отримати необхідні дані, і для клієнтів в регулярному режимі отримувати інформаційні послуги;

• цілісність інформації. Це означає її незмінність, відсутність будь-яких сторонніх, неавторизованих втручань, спрямованих на зміну або знищення даних, порушення системи їх розташування;

• конфіденційність або абсолютна недоступність даних для неавторизованих суб'єктів;

• відсутність відмови або неможливість заперечувати приналежність дій або даних;

• автентичність або можливість достовірного підтвердження авторства інформаційних повідомлень або дій в системі.

До технічних засобів і заходів забезпечення інформаційної безпеки відносяться не тільки програмні продукти, наприклад,

DLP-системи, а й інші інструменти, що знаходяться в розпорядженні компанії [4].

Заходи захисту інформації з технічної точки зору повинні спиратися на модель побудови інформаційної системи підприємства, що дозволяє вибудувати оборону проти зазіхань на конфіденційні відомості.

Встановлення політики безпеки є основною відповідальністю керівництва в організації. Керівництво зобов'язане зберігати та захищати активи та підтримувати якість послуг. З цією метою він повинен запевнити, що операції проводяться розсудливо, зважаючи на реалістичні ризики, що виникають внаслідок надійних загроз. Цей обов'язок може бути виконаний шляхом визначення політики високого рівня безпеки, а потім переведення цієї політики в конкретні стандарти та процедури відбору та виховання персоналу, перевірки та аудиту операцій, складання планів дій на випадок надзвичайних ситуацій тощо. За допомогою цих дій керівництво може запобігти, виявити та відновити втрати. Стягнення залежить від різних видів страхування: резервних копій, резервних систем та сайтів обслуговування, самострахування за рахунок резервів готівки та придбаної страховки для компенсації витрат на стягнення.

Список використаних джерел:

1. Семененко В. А. Информационная безопасность: Учебное пособие. 2-е изд., стереот. – М.: МГИУ, 2005. – 215 с.

2. Гайворонський М.В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с.

3. Дронь М.М., Малайчук В. П., Петренко О. М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.

4. Сороковская А. А. Информационная безопасность предприятия: новые угрозы и перспективы [Электронный ресурс]. – Режим доступа: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032–035.pdf.

Ключові слова: Захист, інформаційна безпека, організація, безпека організації.

Ключевые слова: Защита, информационная безопасность, организация, безопасность организации.
Keywords: Protection, information security, organization, security of the organization.
***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*

Пальчук Андрій Вікторович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

Саніцька Інна Валеріївна
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ IOS: ПРОБЛЕМИ РЕАЛІЗАЦІЇ

Безпека системи є головною складовою зменшення кількості злочинів, здійснюваних у кіберпросторі. Поява сучасних технологій та стрімкий розвиток IT-сфери створює сприятливе середовище для вибору користувачами новітніх засобів для реалізації найрізноманітніших задач, включаючи соціальні мережі та спілкування.

Однією з найбезпечніших мобільних операційних систем вважається iOS. iOS – це мобільна операційна система для смартфонів, електронних планшетів, а також програвачів і деяких інших пристроїв, що розробляється і випускається американською компанією Apple [1].

Оскільки смартфони стають все більш поширеними по всьому світу, компаніям неминуче доводиться боротися з проблемами, пов'язаними з безпекою та конфіденційністю цих пристроїв. технологія збереження конфіденційності вдосконалюється, проблеми з конфіденційністю користувачів не були повністю розглянуті самою технологією. Відповідні регуля-

тивні засоби захисту також відіграють певну роль у захисті конфіденційності користувачів смартфонів. В даний час існує багато прогалин між регулюванням та технологіями: вони не є належним чином поєднані для забезпечення бажаного захисту. Існує перелік поширених проблем захисту персональних даних, обумовлених організаційними і технічними аспектами.

Обробкою персональних даних є будь-яка дія, так звана операція, або сукупність дій, що здійснюються з використанням засобів автоматизації з персональними даними. До обробки входить збір та запис даних, їх систематизація, зберігання, накопичення та оновлення, використання та передача [2].

При зберіганні персональних даних можливі такі помилки як: небезпечне зберігання, витік даних, деякі компоненти операційної системи можуть зберігати чутливі дані, неправильна криптографія, слабка або повністю відсутня захист виконуваних файлів. Щоб зберегти конфіденційні дані програм, користувачі даної операційної системи повинні використовувати служби безпеки, надані компанією самою компанією Apple.

В iOS вбудований механізм шифрування файлів на диску самого пристрою. Таких механізм дозволяє користувачеві віддалено і швидко очистити файлову систему, захищаючи при цьому дані при установці флеш-пам'яті в інший телефон. Якщо встановлений пасскод, прочитати вміст цих файлів без нього неможливо.

Захист файлів реалізована через ієрархію криптографічних ключів. iOS присвоює кожному файлу 256 бітний AES ключ. Дані записуються на накопичувач тільки в зашифрованому вигляді.

AES – симетричний алгоритм шифрування. Уряд США використовує AES з ключем 256 біт для зберігання секретних документів. Симетричність означає, що для шифрування і розшифровки даних використовується один і той же ключ.

В iOS існує кілька класів захисту файлів. Кожен клас захисту має свій крипто-ключ [3].

Ключ файлової системи створюється випадковим способом при першій установці iOS або очищення пристрою. Ключ зберігається в стирається сховище. Коли користувач очищає пристрій опцією Erase all content and settings або віддалено через iCloud, ключ файлової системи видаляється. Тепер всі файли недоступні, система не може розшифрувати метадані, в яких зберігається ключ файлу. Безпечне видалення ключів настільки ж важливо, як і їх створення. Це особливо складно на флеш-накопичувачах, де через зношування дані можуть дублюватися в декількох місцях. Тому в iOS пристрої містять Ефективне сховище (Effaceable Storage). Ця функція дозволяє стирати невеликі блоки даних з пристрою зберігання на найнижчому рівні.

Існує ряд проблем захисту персональних даних в операційній системі iOS. Як правило, персональні дані користувачів при виконанні мережевих запитів зберігаються в кеші HTTP або в Cookies. Крім того, вони розміщуються в додатках, що є небезпечно. Іноді користувачі не встановлюють Passcode або просто проявляють недбалість по відношенню до захисту персональних даних. Саме тому компанія рекомендує звертати увагу на екран авторизації з пінкодом або Touch ID, що служить розблокуванням і захистом персональних даних користувача шляхом зчитування його рис обличчя. Йдеться про додатковий захист даних на рівні користувача інтерфейсу.

З іншого боку, будь-яке шифрування може бути зламано і захист користувачів повністю покладається на компанії, що виробляють продукт техніки, і вони будуть забезпечувати його безпеку лише тому, що це відповідає їх бізнес-інтересам і іміджу.

Натомість сама компанія Apple визнає, що шифрування, яке захищає персональні дані користувачів пристроїв, може бути зламано за допомогою шкідливого програмного забезпечення.

Так, в 2018 році турецький дослідник інформаційної безпеки Мелих Севім знайшов вразливість захисту персональних даних користувачів. В ході його експерименту в iCloud,

система дозволила йому переглядати деякі дані чужих акаунтів в сервісі – наприклад, замітки в облікових записах. Дослідник зміг отримати доступ як до даних випадкових акаунтів, так і цілеспрямовано розкривати інформацію конкретних користувачів – для цього йому потрібно було знати пов'язаний з сервісом номер телефону. Після цієї історії Мелих офіційно звернувся до компанії Apple з проханням переглянути політику конфіденційності та усунути всі можливі проблеми системи, які створили кібернебезпечне та вразливе середовище для користувачів і клієнтів даної компанії. [4]

Список використаних джерел:

1. Офіційний сайт компанії Apple. Електронний ресурс. URL: https://www.apple.com/ru/ios/

2. Яремчук Ю. Є. Комплексні системи захисту інформації: навчальний посібник / Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В. – Вінниця: ВНТУ, 2017. – 120 с.

3. Офіційний сайт компанії Apple. Електронний ресурс. URL: https://www.apple.com/business/resources/docs/iOS_Security_Overview.pdf

4. Офіційний сайт BBC News. URL: https://www.bbc.com/russian/science/2010/12/101229_apple_class_action

Ключові слова: iOS, Apple, персональні дані, операційна система, шкідливе програмне забезпечення, користувачі, криптографія, шифрування файлів.

Ключевые слова: iOS, Apple, персональные данные, операционная система, вредоносное программное обеспечение, пользователи, криптография, шифрование файлов.

Keywords: iOS, Apple, personal data, operating system, malicious software, users, cryptography, encryption of files.

***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*

Попадюк Володимир Володимирович
Національний університет «Одеська юридична академія»,
студент 4 курсу факультету кібербезпеки
та інформаційних технологій

ШИФРУВАННЯ В БАЗАХ ДАНИХ SQL SERVER

Закон вимагає зашифрувати конфіденційну інформацію на рівні бази даних та операційної системи. Як і інші поширені комерційні системи управління базами даних, SQL Server має безліч варіантів шифрування, зокрема на рівні комірки, бази даних та файлів та на рівні передачі через Windows. Ці параметри шифрування забезпечують інформаційну безпеку на рівні бази даних та операційної системи. Крім того, навіть якщо це впливає на інфраструктуру або базу даних SQL Server, вони зменшують можливість несанкціонованого розкриття конфіденційної інформації. Після опису моделі шифрування SQL Server ми представили функцію шифрування, реалізовану в SQL Server, та способи шифрування конфіденційної інформації, що зберігається в базі даних SQL Server.

З'являється все більше повідомлень про втрачений і несанкціонований доступ до конфіденційних даних, а це означає, що безпека баз даних є дуже важливою проблемою для багатьох компаній. Організації, що містять конфіденційну інформацію в базі даних, повинні дотримуватися численних законів, включаючи Gramma-Leach-Bleigh (GLBA), Директиву ЄС про захист даних (EUDPD), Закон про спадкування та підзвітність медичного страхування (HIPAA), стандарт безпеки даних платіжних карток (PCI DSS) та Закон Сарбейнса-Окслі (SOX). Ці закони вимагають шифрування конфіденційної інформації на рівні бази даних та операційної системи.

Крім того, навіть якщо це впливає на інфраструктуру або базу даних SQL Server, вони зменшують можливість несанкціонованого розкриття конфіденційної інформації. Після опису моделі шифрування SQL Server я представив функцію

шифрування, реалізовану в SQL Server, та способи шифрування конфіденційної інформації, що зберігається в базі даних SQL Server.

Модель шифрування SQL Server

Модель шифрування SQL Server в основному забезпечує функції управління ключами шифрування, які відповідають стандарту ANSI X9.17. Стандарт визначає кілька рівнів ключів шифрування, ці рівні використовуються для шифрування інших ключів, а ці ключі використовуються для шифрування фактичних даних.

Головний ключ служби (SMK) є ключем верхнього рівня та родоначальником усіх ключів у SQL Server. SMK – це асиметричний ключ, зашифрований за допомогою API захисту даних Windows (DPAPI). Після зашифрування об'єкта та прив'язки до облікового запису служби SQL Server SMK створюється автоматично. SMK використовується для шифрування головного ключа бази даних (DMK).

Другим рівнем ієрархії ключів шифрування є DMK. Він шифрує симетричні ключі, асиметричні ключі та сертифікати. У кожній базі даних є лише одна DMK.

Наступний рівень містить симетричні ключі, асиметричні ключі та сертифікати. Симетричний ключ є основним засобом шифрування в базі даних. Корпорація Microsoft рекомендує використовувати лише симетричні ключі для шифрування даних. Крім того, SQL Server 2008 та новіші версії мають сертифікати рівня сервера та ключі шифрування бази даних для прозорого шифрування даних.

Шифрування на рівні осередків

Починаючи з SQL Server 2005, можна шифрувати або розшифровувати дані на сервері. Можна зробити це різними способами. Наприклад, можна використовувати один із наведених нижче методів для шифрування даних у базі даних:

- ця ж прохідна фраза використовується для дешифрування даних. Якщо збережені процедури та функції не зашифровані, до фрази очищення можна отримати доступ через метадані.

• Сертифікат. Цей метод забезпечує надійний захист і високу швидкість. Сертифікати можуть бути пов'язані з користувачами; для підписання потрібно використовувати DMK.

• Симетричний ключ. Досить надійний, щоб задовольнити більшість вимог щодо захисту даних та забезпечити достатню продуктивність. Один ключ використовується для шифрування та дешифрування даних.

• Асиметричний ключ. Оскільки для шифрування та дешифрування даних використовуються різні ключі, забезпечується надійний захист. Однак це може негативно позначитися на роботі. Експерти Microsoft не рекомендують використовувати його для шифрування великих значень. Асиметричні ключі можна підписати за допомогою DMK або створити за допомогою паролів.

SQL Server має вбудовані функції для шифрування та дешифрування на рівні комірки. SQL Server має два системних подання, які можна використовувати для отримання метаданих про всі симетричні та асиметричні ключі, які існують в екземплярі SQL Server. Як випливає з назви, sys.symmetric_keys повертає метадані симетричного ключа, а sys.asymmetric_keys – метадані асиметричного ключа. Ще один корисний досвід – це sys.openkeys. Цей поданний каталог містить інформацію про ключі шифрування, відкриті в поточному сеансі.

Прозоре шифрування даних

SQL Server 2008 тепер може використовувати прозоре шифрування для шифрування всієї бази даних. Використовуючи це шифрування, стає можливим захистити базу даних, не змінюючи існуючу програму, структуру бази даних або процес. Це найкращий вибір для задоволення вимог нормативних актів та правил безпеки компанії, оскільки вся база даних зашифрована на жорсткому диску.

Прозоре шифрування даних шифрує базу даних у режимі реального часу, оскільки введення здійснюється у файлі бази даних SQL Server (*.mdf) та файлі журналу транзакцій (*.ldf). Під час резервного копіювання бази даних записи також

шифруються в режимі реального часу, а потім створюється знімок. Дані шифруються перед записом на диск і дешифруються перед вилученням. Цей процес є повністю прозорим для користувачів або програм, оскільки він працює на рівні обслуговування SQL Server.

За допомогою відповідного методу SQL Server використовує ключ шифрування бази даних для шифрування бази даних. Цей асиметричний ключ зберігається в записі завантаження бази даних, тому він завжди доступний під час відновлення.

Ключ шифрування бази даних шифрується за допомогою сертифіката сервера, а сертифікат сервера шифрується за допомогою основної бази даних бази даних DMK. DMK основної бази даних використовує шифрування SMK. SMK – це асиметричний ключ, зашифрований за допомогою Windows DPAPI. Під час першого зашифрування будь-якого об'єкта ключ SMK автоматично генерується та зв'язується з обліковим записом служби SQL Server.

Захист даних в SQL Server

Шифрування – це процес шифрування конфіденційних даних за допомогою ключа або пароля. Шифрування надійно захищає дані та зменшує можливість несанкціонованого розголошення конфіденційної інформації, оскільки без належного ключа або пароля дані будуть зайвими. SQL Server має безліч режимів шифрування, включаючи рівень комірки, рівень бази даних, файли на базі Windows та шифрування рівня передачі. Шифрування SQL Server не може вирішити проблеми інфраструктури та бази даних SQL Server, але навіть якщо інфраструктура SQL Server або конфіденційність бази даних порушена, це також може покращити безпеку даних на рівні бази даних та операційної системи.

Список використаних джерел:

1. Подборка материалов по SQL Injection [Электронный ресурс] – Режим доступа: http://injection.rulezz.ru/

2. Qiu M., Davis S. Database security mechanisms and implementation. IACIS, Issues in Inform. Syst. 2002 vol. 03 pp. 529–534.

3. Потапов А. Е., Манухина Д. В., Соломатина А. С., Бадмаев А. И., Яковлев А. В., Нилова А. С. Безопасность локальных баз данных на примере SQL Server Compact // Укр. Тамбов. ун-та. Серия: Естественные и технические науки. 2014. № 3. С. 915–917.

4. Бортовчук Ю. В., Крылова К. А., Ермолаева Л. В. Информационная безопасность в современных системах управления базами данных // 106 Современные проблемы экономического и социального развития. 2010. № 6. С. 224–225. 31 Горбачевская

5. Ткаченко Н. А. Реализация монитора безопасности СУБД MySQL в dbf / dam системах // ПДМ. Дополнение. 2014. № 7. С. 99–101.

6. Полтавцева М. А. Задача хранения прав доступа к данным в СУБД на примере Microsoft SQL Server // Актуальные направления фундаментальных и прикладных исследований: матер. V Междунар. научно-практич. конф. 2015 С. 118–120.

7. Кузнецов С. Д. Базы данных: учебник для студ. М.: Академия, 2012. 496 с. 42

8. Зегжда Д. П., Калинин М. О. Обеспечение доверенности информационной среды на основе расширения понятия «целостность» и управление безопасностью // Проблемы информ. безопасности. Компьютерные системы. 2009. № 4. С. 7–16.

Ключові слова: шифрування SQL Server, база данних, ключ шифрування, симетричний і асиметоричний ключі.

Ключевые слова: шифрование SQL Server, база данных, ключ шифрования, симметричный и асиметоричний ключи

Keyworbs: encryption SQL Server, database, encryption key, symmetrical and asymmetrical keys.

Науковий керівник: *к.т.н., доцент Соколов А. В.*

Ратушняк Сергій Сергійович
Національний університет «Одеська юридична академія»,
студент студент 3-го курсу факультету кібербезпеки
та інформаційних технологій

МЕТОДИ ЗАХИСТУ ВІД ІНТЕРНЕТ-ФІШИНГУ

Фішинг – являє собою протиправне діяння, що здійснюється з метою змусити ту чи іншу особу поділитися своєю конфіденційною інформацією, наприклад паролем або номером кредитної картки. Сьогодні інформаційні технології розвинені настільки, що фішери можуть оволодіти потрібної їм інформацією практично без участі користувача. Інтерес зловмисників може викликати будь-яка інша конфіденційна інформація. Шахраї «вивуджують» дані користувачів під різними пристойними приводами: перевірка авторизації на сайті, необхідність «відписатися» від спаму в електронній пошті, оплата покупки за низькою ціною або з великою знижкою, необхідність встановити новий додаток.

Як працює інтернет-фішинг?

Специфікою фішингу є те, що жертва шахрайства надає свої конфіденційні дані добровільно. Для цього зловмисники оперують такими інструментами, як фішингові сайти, e-mail розсилка, фішингові landing page, спливаючі вікна, таргетована реклама. Користувач отримує пропозицію зареєструватися для отримання будь-якої вигоди або підтвердити свої персональні дані нібито для банківських або комерційних установ, клієнтом яких він є. Як правило, шахраї маскуються під відомі компанії, додатки соціальних мереж, сервіси електронної пошти. Електронна адреса відправника дійсно схожа на адресу знайомої користувачеві компанії. Наприклад, щоб замаскуватися під інтернет-магазин Aliexpress, шахраї шлють листи з адрес, що містять слово Alliexpress або Aliexxpress. Працює та сама схема, яка змушує людей купувати дешеві китайські кросівки таких «всесвітньо відомих брендів», як Pumma або Abibas.

Зловмисники користуються низьким рівнем обізнаності користувачів, зокрема, незнанням елементарних правил мережевої безпеки. Перш за все, організаторів фішинг-атак цікавлять персональні дані, які дають доступ до грошей, тому жертвами фішингу можуть ставати не тільки окремі люди, а й банки, електронні платіжні системи, аукціони.

Як розпізнати інтернет фішинг:

Фішингові сайти можуть ховатися за спливаючими вікнами. На них може вести таргетована реклама. Бувають ситуації, коли в графі «логін» користувач вже бачить адресу своєї електронної пошти, і йому пропонується всього лише ввести свій пароль в нижній графі.

Пропозиція залишити свої конфіденційні дані може виходити від ресурсу, який схожий на добре знайомий вам сайт, а насправді виявляється фішинговим. Шахраї створюють фішингові сайти з впізнаваним дизайном і схожим адресним рядком. Вони заманюють відвідувачів в фішингові інтернет-магазини шаленими знижками і низькими цінами. Після того, як людина вводить інформацію, необхідну для оплати товару за допомогою кредитної картки, інформація потрапляє до зловмисників.

Велика ймовірність побачити посилання на фішингових сайтів в коментарях на чужих сторінках або групах в соціальній мережі. Її також може надіслати вам друг або знайомий, чий акаунт вже зламали.

Як захиститися від інтернет-фішингу:

Захист від фішингу включає в себе дотримання кількох елементарних правил безпеки в інтернеті.

Перш за все слід пам'ятати що нікому і ні за яких обставин не можна передавати такі конфіденційні дані, як пін-код банківської картки, пароль електронної пошти або акаунтів в соціальних мережах. Ні банк, ні соціальна мережа не стануть запитувати ці дані по електронній пошті.

Установка ліцензійного програмного забезпечення. Захист від вірусів і хакерських атак на домашніх і робочих ПК може забезпечити тільки ліцензійна антивірусна програма, яку

потрібно своєчасно оновлювати. Перед установкою програм з Інтернету або реєстрацією на сервісах з введенням персональних даних слід уважно прочитати угоду користувача, оскільки одним з його умов може бути обробка та використання особистої інформації.

Слід завжди звертати увагу на дизайн сайту. Якщо сайт здається дивним, недопрацьованим, склепати нашвидкуруч або викликає якісь підозри, то дуже може бути, що це фішингових сайтів. Також слід звернути увагу на адресний рядок на засланні переходу. Незначні зміни в електронній адресі можуть привести вас на абсолютно інший сайт (наприклад, замість mail.ru може бути meil.ru).

Використання VPN при роботі з загальнодоступними точками Wi-Fi. Користуючись Інтернетом в готелі, на вокзалі або в кафе через Wi-Fi з'єднання, рекомендується включати VPN сервіс, що перенаправляє трафік на власний ресурс, видаючи «чистий» доступ, недоступний для незаконних маніпуляцій. Оскільки використання пароля не забезпечить повноцінний захист.

Правильно довіряти організацію захисту особистої інформації компаніям, що надають такі послуги. Вони володіють спеціальними методами захисту інформації і допоможуть підібрати індивідуальну систему безпеки в залежності від специфіки роботи компанії-замовника, типових загроз. Такі компанії організують захист відомостей в хмарному сховищі або на фізичному сервері.

Список використаних джерел:

1. Все о фишинге [Електронний ресурс] – Режим доступу до ресурсу: https://ru.malwarebytes.com/phishing/.

2. Острожно, фишинг [Електронний ресурс] – Режим доступу до ресурсу: https://applied-research.ru/ru/article/view?id=9077.

3. Как защититься от фишинга: 10 советов [Електронний ресурс] – Режим доступу до ресурсу: https://www.kaspersky.ru/blog/phishing-ten-tips/9744/.

4. Защита персональных данных в интернете [Електронний ресурс] – Режим доступу до ресурсу: https://searchinform.ru/

resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-internete/.

Ключові слова: фішинг, шахрайство, фішингові сайти.
Ключевые слова: фишинг, мошенничество, фишинговые сайты.
Keywords: phishing, fraud, phishing sites.

Науковій керівник: *к.т.н., Бойко В. Д.*

Ревацкий Александр Алексеевич
Национальный университет «Одесская юридическая академия»,
студент 3-го курсу, факультета кибербезопасности
и информационных технологий

DOS/DDOS-АТАКА

Dos-атака *(Denial of Service* «отказ в обслуживании»*)* – это атака осуществлена хакерами на центральный сервер с целью довести его до отказа. Также существует **DDoS-атака** (*Distributed Denial of Service* «распределенный отказ в обслуживании») – данная атака выполняется посредством нескольких компьютеров, это могут быть сообщники, боты или даже девайсы людей, которые даже не подозревают что они, являются участником данной атаки. Также многие предпочитают этот вид атаки, чтобы было сложнее отследить атаку обратно к её источнику, так как она поступает с нескольких точек. Приведу пример на библиотеке:

Библиотекарь может помочь найти книгу за 5 минут только 1 клиенту, но если к нему обратятся еще 5 клиентов, тогда им придётся ждать. Если обратятся еще около 20 клиентов, то будет давление и он может ошибаться в выдаче книг и недовольные клиенты из-за ожидания, могут просто уйти в другую библиотеку. А библиотекарь потеряет клиентов.

Хакерам проще организовать DDoS-атаку на систему, чем заполучить полный доступ к системе. Существуют множества мотивов для организации такого вида преступления:

1. Личные причины: достаточно часто атаки происходят на государственные организации или корпорации. В конце 20 века хакеры атаковали веб-узлы FBI, произошло данное событие благодаря недавнему рейду FBI на киберпреступников.

2. Конкуренция: тип таких атак обычно делают на заказ недобросовестные конкуренты компании, чтобы их конкурент потерял деньги и клиентов.

3. Развлечение: начинающие хакеры пробуя себя в это ремесле, атакуют любую организацию, а потом смотрят на площади разрушений своей работы.

4. Выкуп или шантаж: довольно часто перед запуском атаки, хакеры связываются с владельцами и требуют выкуп.

5. Политический протест: иногда через эту атаку хакеры показывают свое несогласие с какими-либо политическим решением.

Первые атаки в истории начали фиксироваться в 1999 году, тогда хакеры атаковали крупные торговые площадки Amazon и eBay.

За последние годы частота атак выросла в 2.5 раза, а запредельная мощность выросла до 1 Тбит/сек.

Минимально время такой атаки может составлять несколько минут, а максимальное которое было зафиксировано около 300 часов. Но есть сведения, что была такая атака, что длилась около месяца.

Потенциальные жертвы атаки:

Государственные корпорации и крупные компании;

Медицинские заведения;

Платежные системы;

СМИ;

Интернет-магазины и разные предприятия;

Биржы криптовалюты;

Онлайн-игры.

Механизм работы DDos-атаки

У каждого сервера есть предел запросов, которые он может обслуживать одновременно. Также предусмотрен предел пропускной способности канала, соединяющий сеть и сервер. Для обхода ограничения, преступник создает компьютеру сеть с встроенным вредоносным ПО, называемую «зомби-есть». Для создания такой сети, преступник делает рассылку(закидывает троян) на почту, в разные мессенджеры. Девайсы, пришедшие в данную сеть не имеют никакой связи между собой. Их цель, только выполнять все задания хакера.

Когда хакер начинает атаку, он отправляет команды захвачены вирусом компьютерам, а те оказывают содействие хакеру. Так генерируется колоссальный объем трафика, который способный «положить» сервер.

Признаки атаки

Обнаружить атаку можно только, после того как хакер добьётся своего, это можно понять по некорректной работе сервера или размещенного контента. Также существует пару признаков, благодаря ним можно выявить данное нападение:

ПО и ОС начинают часто тормозить и сбоить, то есть виснуть, некорректно завершать свою работу;

Огромное получение пакетов с одного или нескольких рядов портов;

Постоянно дублирование одного и того же действия;

Резко возросла нагрузка на сервер, которая отличается от обыденных показателей за день.

По каким критериям делятся DDos-атаки

Они делятся на 3 вида: TCP, UDP и другие. Они являются основными протоколами, которые эксплуатируются для передачи информации в сети интернете, благодаря их уязвимостям хакеры делают атаки. В зарубежных компаниях делят на 5 видов: HTTP, TCP, UDP, ICMP, прочие.

Данное деление типов дает возможность обнаружить, какие именно протоколы более уязвимы к таким нападениям, а какие нет. Также дает возможность исправлять баги защиты, а также создавать новые методы защиты.

По классификации на модели OSI(на которые происходит DDoS-атаки):

2-й уровень – канальный;

3-й – сетевой;

4-й – транспортный;

7-й – прикладной.

По механизму действия. Делятся на 3 блока:

1-й блок-является флуд, то есть создается сильный поток запросов, который забивает весь трафик жертве, к данной группе относятся: *DNS амплификация, фрагментированный UDP флуд, ICMP флуд, NTP флуд, Ping флуд, UDP флуд, UDP флуд с помощью ботнета, VoIP флуд, Фрагментированный ICMP флуд, DNS флуд*.

2-й блок-является атака при которой происходит отказ в обслуживании, то есть использующие уязвимости стека сетевых протоколов: *SYN флуд (SYN Flood), IP null атака, TCP null атака, TCP null / IP null атака, Ping смерти, Атака поддельными TCP сессиями, ACK/PUSH ACK флуд, SYN-ACK флуд, RST/FIN флуд, ACK/PUSH ACK флуд, Атаки с модификацией поля TOS, Атака поддельными TCP сессиями с несколькими ACK.*

3-й блок-является атака на прикладной уровень OSI: *HTTP флуд, Атака с целью отказа приложения, HTTP флуд одиночными запросами, Атака фрагментированными HTTP пакетами, HTTP флуд одиночными сессиями, Сессионная атака. Атака медленными сессиями.*

Как избежать такого вида нападения

Чтобы тебя не застала врасплох DDoS-атака, нужно внимательно и тщательно подготовить свои системы, а именно:

Сервера, обладающие непосредственный допуск во внешнюю сеть, обязаны быть готовые к обычному также стремительному удаленному ребуту. Огромным плюсом станет присутствие 2-го сетевого интерфейса, посредством него возможно приобрести допуск к серверу, если главный канал будет недееспособен.

Программное обеспечение, применяемое на сервере, всё время обязано пребывать в дееспособном состоянии.

Абсолютно все дыры обязаны быть пропатчены, а также обязаны быть установлены последние обновления. Это даст возможность сдержать Dos-атаки, эксплуатирующих баги на сервисах.

Все сетевые сервисы, назначенные с целью административного применения, обязаны быть скрыты brandmouer от абсолютно всех недоброжелателей. В таком случае атакующий никак не сумеет применять их с целью выполнения Dos-атаки либо bruteforce.

На подходе к серверу обязана быть система слежения за трафиком, чтобы отследить любую начинающиеся атаку на систему, а также принять меры её предотвращения.

Спиок використаних джерел:

1. Классификация DDoS-атак; краткий обзор современных технологий: Режим доступа: http://surl.li/hhmc
2. Атака сетевых зомби: Режим доступа: http://surl.li/hhme

Ключевые слова: Кибербезопасность, Атака, Взлом, Афера.
Ключові слова: Кібербезпека, Атака, Злом, Афера.
Keywords: Cybersecurity, Attack, Breaking, Scam.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Лоза Илья Олегович
Национальный университет «Одесская юридическая академия»,
студент 2-го курса факультета кибербезопасности
и информационных технологий

КАРДИНГ

С момента появления пластиковых банковских карт жизнь людей стала в разы проще. Больше не нужно ходить за зарплатой к «начальству», думать где хранить свои денежные средства, а также удобное осуществление покупок. Но преступники не дремлют, и они также начали активно использовать эти возможности в своих не совсем законных целях. А именно

зарождение нового вида мошенничества, что получило название «Кардинг».

Кардинг – это вид мошенничества, в котором напрямую задействуются платежные карты пользователей, либо же реквизиты этих карт для дальнейшего их использования. В простонародье можно именовать, как воровство, только в основном это происходит в цифровом виде, но всё же на некоторых этапах мошенник также обращается к так называемой «Социальной инженерии», но где, и как она используется будет описано немного далее.

Для начала ознакомимся с неким словарём «кардера», и далее пойдём по порядку.

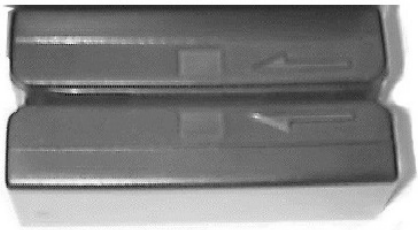
Словарь «кардера»

- **Track(трек)** – информация с магнитной полосы платежной карте.
- **дроп** – человек, который будет заниматься обналичиванием «картона».
- **Credit Card** – собственно сама кредитная карта.
- **White Plastic(белый пластик) –** служит для изготовления банковских карт, в основном тип пластика CR-80.
- **Кард-холдер –** реальный держатель (владелец) карты.
- **Dump –** трек код и пин код карты.
- **Голубь / Глобус –** на каждой кредитке есть голограмма, на Visa – это голубь, на Mastercard – полушарие.
- **Скарженный**- украденный с помощью «кардинга»

Где кардеры берут информацию о картах (CC)

1. Ридеры – устройство выполняет считывание информации с магнитной полосы. Бывают как стационарные, так и портативные на батарейках (прим. Рис 1). В свою очередь у «кардеров» есть специальные агенты, которые устроены кассирами в крупных магазинах, работниками гостиниц, ресторанов. Вкратце, они устроены в тех местах, где есть оплата картой, и с помощью «ридера», они передают информацию непосредственно самому «кардеру». Цена такого труда варьируется от

20$ и до 250$ в зависимости от того, сколько «агент» раздобыл информации.



Mini-Mag Magstripe reader (PMR 102)

Рис. 1. Портативный ридер PMR102

2. Взлом баз данных – этот способ является одним из самых распространенных в наше время, злоумышленнику достаточно сломать процессинговую сеть, через которую проходят физ. платежи (не виртуальные), откуда и берется база данных. Также это работает и с виртуальными магазинами, в которых незащищенное соединение, и имеется способ оплаты картой, здесь же все происходит гораздо проще, нежели в первом варианте, ибо такие магазины в основе своей очень легки на взлом.

3. Покупка дампов – очень актуальный способ, есть достаточно большое количество сервисов «.onion», которые за определенную плату предоставляют вам краденые реквизиты банковских карт. В среднем цена за единицу 1-3, за Американские карты просят до 25$. Они же в свою очередь пользуются одним из вышеперечисленных методов получения этих данных. Способ является самым легким, но также есть БОЛЬШОЙ риск быть обманутым, за счёт того, что сервисы эти расположились под надежной маской TOP.

4. Скимминг – на сегодняшний день почти неосуществимый способ. На приёмник карт банкомата ставится дополнительный пластиковый ридер, который не особо сильно бросается в глаза. А клавиатуру накрывает очень тонкая клавиатура, кото-

рая будет перехватывать ПИН-код держателя карты (кардхолдэра). По итогу выходит банкомат «бабломёт», который полностью перехватит данные вашей карты, и сольет их мошеннику. Неосуществимый этот способ из-за того, что банкоматы периодически обслуживаются работниками банков, и находятся под беспрерывным наблюдением камер.

С помощью всех вышеперечисленных способов мошенник получает дампы карты, далее следует сложный этап кардинга (снятие средств).

Перевод данных на белый пластик

Для дальнейшей работы с дампами мошенниками потребуется «белый пластик» и «энкодер».

1. Используется для этого специальный пластик с маркировкой «**CR-80»**. Раздобывают кардеры такой пластик также на **теневых ресурсах** сети интернет.

2. Далее в ход идёт **Энкодер**.

Энкодер – это специальное устройство, которое из обычной белой карты делает готовую магнитную копию. Для этого достаточно разобраться с несложной программой энкодера, после чего провести белый пластик через устройство. Современные Энкодеры также предоставляют возможность устанавливать на белый пластик магнит для бесконтактной оплаты.

Рис. 2. Энкодер

3. С помощью определенной махинации, мошенник получает ПИН-код карты, либо если дамп куплен, в основном код к нему прилагается. После чего мошенник может снимать деньги с помощью магнитной копии с практически любого банкомата.

Также есть способы получения средств со «скарженных» карт методом нахождения дропа.

Пример: «Дроп» хочет себе новый телефон, который стоит 10к. «Кардер» покупает этот телефон онлайн с помощью оплаты картой на адрес заказчика. Заказчик в свою очередь отправляет 30% суммы мошеннику, по итогу «кардер» обналичил 3к без каких-либо рисков, а заказчик получил новый телефон за 30% от его стоимости. Обе стороны остались довольны, только вот сторона заказчика не учла, что его адрес засветился, и в случае дальнейших разбирательств крайним останется он.

Методы защиты от кардинга

- Быть бдительным при использовании банкоматов, на наличие посторонних устройств.
- Никогда не передавать карты третьим лицам.
- При осуществлении покупок смотреть за тем, чтобы карта использовалась по назначению
- Не сообщать никому трехзначный код, и ПИН-код
- Работники банка не будут у вас спрашивать CVV или PIN, это конфиденциальная информация.

«Корысть дает новые идеи.
Идеи дают новые способы Теневого заработка.
Кардинг не умер.»

Список использованных источников:

1. Рисунок 1 [Источник фотографии]. URL – http://www.e-scan.com/profiles/miniportable.htm

2. Рисунок 2 [Источник фотографии]. URL – https://www.ebay.com/itm/Magnetic-Stripe-Card-Reader-Writer-Encoder-MSR206–606-/310325315390

3. Информация о понятии «Кардинг» [Ссылка на ресурс]. URL – https://xakep.ru/2002/07/02/15687/

4. Словарь кардера [Ссылка на ресурс]. URL – https://rabotadropom.work/chto-takoe-karding/

Ключевые слова: Кардинг, кардер, ридер, взлом, мошенничество.
Ключові слова: Кардинг, кардер, рідер, злом, шахрайство
Key words: Carding, carder, reader, hacking, fraud

***Науковий керівник**: к.т.н., доцент Задерейко О. В.*

Орел Анастасія Олександрівна
Національний університет «Одеська юридична академія»,
студентка 2-го курсу факультету кібербезпеки
та інформаційних технологій

АНАЛІЗ МЕТОДУ ВІОЛИ-ДЖОНСА ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧ

Спроби навчити комп'ютер розпізнавати образи розпочалися ще в 60-тих роках, але тільки 2001 року американські дослідники Поло Віола та Майкл Джонс розробили алгоритм пошуку облич на зображеннях, який згодом став революційним у сфері розпізнавання образів [1; 2]. Нині ця технологія розпізнавання використовується повсюдно. Її застосовують для ідентифікації пішоходів чи автомобілістів на дорозі, людей в аеропортах, у системах безпеки і контролю доступу, при створенні систем комп'ютерного зору в робототехніці, у сенсорних телефонах для ідентифікації власника і розблокування системи захисту, в усіх сучасних фотоапаратах для налаштування автофокусу, у камерах для розпізнавання емоцій та міміки лиця та навіть у дзеркалах з доповненою реальністю, які допомагають у віртуальному виборі окулярів, доборі вдалих відтінків макіяжу тощо.

Розповсюдженість алгоритму Віоли-Джонса з-посеред інших методів розпізнавання облич зумовлена прийнятною швидкістю оброблення і точністю визначення даних, що дало змогу застосовувати цей алгоритм не лише у роботі із зображеннями, а й у відео потоках.

Сам алгоритм складається з двох етапів: навчання та розпізнавання. Спочатку на етапі навчання алгоритм на значній кількості (десятках тисяч) тестових зображень (навчальній вибірці) навчає класифікатор (classifier). Цей процес може тривати від декількох днів до місяців, адже від якості етапу навчання залежить подальша якість і швидкість розпізнавання.

На початку задаються певні значення ознак, на основі яких здійснюватиметься пошук обличчя. Саме зображення динамічно поділяється на невеликі прямокутні ділянки різного розміру, поверх яких накладаються монохромні ділянки – так звані примітиви Хаара, які визначають набори перепадів яскравості й переходів від світлих до темних областей по осі X та Y в задачі розпізнавання обличчя. Так, на всіх обличчях ділянки очей темніші, аніж ділянки щік. Різні пропорції світлих і темних областей, їхні розміри та значення перепадів яскравості формують певну базу об'єктів – наборів ділянок облич, які лежать вище очей і на щоках [3]. Ознаки обчислюються як сумарні значення яскравості світлих і темних частин ділянок.

Саме Віола і Джонс запропонували інтегральне подання зображення [1; 2] у формі двомірної матриці пікселів, колір яких задається однобайтним числовим значенням від 0 до 255 – для монохромних зображень, чи трибайтним значенням від 0 до 2553 – для кольорових (три складові R, G, B). У такій інтегральній матриці сума пікселів прямокутника, яка і формує прямокутні ознаки Хаара, обчислюється дуже швидко, незалежно від його розміру [4]. Саме тому метод Віоли-Джонса має високу швидкість розпізнавання. Математично інтегральне подання є подвійним інтегралом функції, яка описує зображення (спочатку по рядках, а потім по стовпцях) [5].

При розпізнаванні досліджуване зображення сканується так званим вікном пошуку (scanning window) певного розміру, яке послідовно рухається по зображенню. До кожного положення вікна застосовується класифікатор і використовуються ознаки Хаара, за допомогою яких відбувається пошук потрібного об'єкта у базі. При цьому прораховуються різні варіанти

розташування ознак у вікні сканування для різних масштабів, але масштабується не саме зображення, а розмір вікна сканування. Після цього використовується бустінг для вибору найбільш придатних ознак шуканого об'єкта на даній частині зображення [4]. Усі ознаки надходять на вхід класифікатора, який остаточно визначає наявність чи то відсутність обличчя у цьому вікні. Якщо після всіх обчислень певна ознака збігається зі значеннями тестової вибірки, здобутої під час навчання, тоді алгоритм перевіряє наступні ознаки. У разі збігу всіх ознак з тестовою вибіркою, класифікатор виголошує вердикт про те, що на зображенні є обличчя. Вікна без облич виключаються з подальшого розгляду.

Система визначення обличчя на зображенні за допомогою даного методу повністю автоматизована і не вимагає втручання людини, а тому цей підхід працює швидко. Дослідження свідчать [4; 5], що метод Віола-Джонса для розпізнавання осіб на зображенні є одним з кращих за показниками ефективності розпізнавання та швидкості роботи.

Проте, зважаючи на всі переваги методу Віоли-Джонса, слід чітко розуміти і враховувати його недоліки. Одним з них є доволі тривале навчання, адже, перш ніж почати розпізнавати обличчя, алгоритм має проаналізувати тисячі зображень. Крім того, при куті нахилу обличчя понад 30 градусів відсоток їх виявлення засобами цього методу стрімко падає [2], що не дозволяє розпізнавати повернені обличчя під довільним кутом. Ця особливість значно звужує сферу застосування або навіть унеможливлює використання алгоритму до певних категорій зображень. До специфічного недоліку можна віднести наявність декількох близько розташованих один до одного результатів роботи алгоритму через застосування вікна сканування і різних масштабів. Проте всі ці недоліки на практиці розглядаються лише як специфічні аспекти застосування, а сам алгоритм лишається одним із поширеніших при розпізнаванні обличчя.

Список використаних джерел:

1. P. Viola and M. J. Jones, «Rapid Object Detection using a Boosted Cascade of Simple Features», proceedings IEEE Conf. on Computer Vision and Pattern Recognition (CVPR2001), 2001 (Kauai, HI, 2001), pp. 511–518.

2. Viola P., Jones M. J. Robust real-time face detection. *International Journal of Computer Vision.* Vol. 57, no. 2, 2004. P. 137–154

3. Азаров Д. Метод распознавания лиц Виолы-Джонса (Viola-Jones) https://oxozle.com/2015/04/11/metod-raspoznavaniya-lic-violy-dzhonsa-viola-jones/

4. Метод Виолы-Джонса (Viola-Jones) как основа для распознавания лиц https://habr.com/ru/post/133826/

5. Кардаш А. І., Левицька С. М., Дудикевич А. Т. Задача розпізнавання людських облич методами штучного інтелекту. *Інформаційні технології та комп'ютерна інженерія.* 2013, № 1. С. 84–87.

Ключові слова: розпізнавання облич, метод Віоли-Джонса, інтегральне подання зображень, ознаки Хаара.

Key words: face recognition, Viola – Jones method, integral representation of images, Haar features.

Ключевые слова: распознавание лиц, метод Виолы-Джонса, интегральное проедставление изображений, признаки Хаара.

***Науковий керівник**: к.т.н., доц. Трофименко О. Г.*

Павловский Владислав Юрьевич
Национальный университет «Одесская юридическая академия»,
студент 4-го курса факультета кибербезопасности
и информационных технологий

ЗАЩИТА ОТ DDOS-АТАК

Распределенные атаки типа «отказ в обслуживании» (Распределенный отказ в обслуживании или DDoS) сегодня часты, в частности, из-за относительной простоты их реализации и их эффективности против неподготовленной цели.

Эти атаки могут привести к значительным финансовым потерям из-за прерывания обслуживания или даже косвенно через повреждение имиджа цели. По этой причине необходимо предвидеть эту угрозу и принять ряд технических и организационных мер, чтобы противостоять ей.

Атака отказа в обслуживании направлена на то, чтобы сделать одну или несколько служб недоступными. Отказ в обслуживании может заключаться в использовании, например, уязвимости программного или аппаратного обеспечения. Прерывание обслуживания также может быть выполнено путем предотвращения доступа к этой услуге, например, путем насыщения полосы пропускания сети: это называется объемными атаками. Кроме того, атака может запрашивать до исчерпания один или несколько ресурсов службы. Это может быть, например, открытие большого количества новых сеансов TCP за очень короткий промежуток времени или даже слишком большое количество одновременных обработок, выполняемых базой данных [1].

Любая организация, деятельность которой зависит от сетевой инфраструктуры, подключенной к Интернету, может стать целью DDoS-атаки. Мотивы и цели нападавших разнообразны: от идеологических претензий до мести, включая вымогательство. Более того, некоторые атаки, похоже, проводятся для того, чтобы отвлечь внимание и скрыть другие незаконные действия, такие как мошеннические банковские операции. Хотя многие организации подвержены этой угрозе, некоторые виды деятельности более подвержены атакам DDoS. Среди них, в частности, можно упомянуть электронную коммерцию финансовых учреждений, правительства или даже ИТ-хостинговые структуры. В этом контексте тем более важно предоставить соответствующие решения защиты с самого начала проектов по настройке информационных систем и сетевой инфраструктуры.

Существуют различные защитные решения, которые могут быть реализованы для борьбы с DDoS-атаками. Развертывание

фильтрующего оборудования на границе информационной системы объекта обеспечивает защиту от атак, объем которых не превышает пропускную способность сетевых каналов. Когда сетевые каналы организации перегружены, часто необходимо обратиться к транзитному оператору или поставщику Интернет-услуг, чтобы отфильтровать восходящий трафик. Кроме того, поставщики услуг предлагают специальные решения для защиты под названием «в облако», которые размещаются на собственной инфраструктуре. Можно совместить использование выделенного оборудования на границе сети объекта с фильтрацией, выполняемой «в облако». Этот тип гибридной защиты позволяет, в частности, защитить объект от объемных атак, давая ему возможность бороться с атаками с низкой пропускной способностью [4].

Оборудование типа межсетевого экрана. Брандмауэры и балансировщики нагрузки могут помочь отразить некоторые DDoS-атаки, например, с относительно низким трафиком. Таким образом, брандмауэры можно использовать для фильтрации трафика в соответствии с транспортным протоколом и портами источника или назначения или даже для ограничения количества запросов на исходный IP-адрес к серверу. Действительно, некоторые DDoS-атаки специально направлены на исчерпание ресурсов памяти цели. В этом случае брандмауэры и балансировщики нагрузки являются первыми элементами инфраструктуры, которые будут затронуты. Поскольку эти элементы отключены, отказ одного из них достаточен, чтобы отказ в обслуживании стал эффективным. Однако иногда можно изменить конфигурацию этого оборудования, чтобы повысить его устойчивость к атакам этого типа, например, увеличив размер таблиц состояния и сократив время мониторинга соединения.

Использование специального оборудования. Организация может использовать оборудование для фильтрации, специфичное для DDoS-атак. Это оборудование обычно имеет подходящую производительность и предлагает несколько типов

противодействия. Помимо функций фильтрации по белому или черному списку, они позволяют, среди прочего:

– проводить фильтрацию по географическому положению источников;

– определять точные правила фильтрации пакетов по их содержимому (например, используя регулярные выражения);

– ограничить количество запросов в заданном временном интервале для определенных ресурсов (например, для веб-страницы)

– определить пороги обнаружения атак в соответствии с такими параметрами, как пропускная способность или количество пакетов в секунду.

Следует также отметить, что этот тип оборудования может использоваться для фильтрации приложений, когда обмены зашифрованы (например, для трафика HTTPS), позволяя объекту сохранять свой закрытый ключ [5].

Фильтрация на уровне сети транзитного оператора. Транзитный оператор может настроить фильтрацию трафика на основе IP-адресов источника или назначения, используемого транспортного протокола, а также портов источника или назначения. Следует отметить, что фильтрация исходных IP-адресов может быть затруднена, если их очень много. В крайнем случае оператор может исключить весь трафик в заданный пункт назначения. В этом случае трафик к одному или нескольким получателям просто не обрабатывается. Таким образом, оператор создает «черную дыру» для рассматриваемого пункта назначения или пунктов назначения. Этот метод фильтрации обычно называют выражением «черная дыра». Следует отметить, что «черная дыра» трафика на основе пункта назначения вызывает отказ в обслуживании. Однако этот тип фильтрации может оказаться полезным, в частности, когда трафик, предназначенный для цели атаки, влияет на другие службы, которыми последний управляет или от которых он может получить выгоду. Некоторые операторы могут также предлагать аналогичную фильтрацию на основе IP-адресов источника атаки.

Использование сети доставки контента (CDN). Сеть доставки контента (CDN) – это серверная инфраструктура, распределенная в несколько дата-центров, и чья цель состоит в том, чтобы заменить услуги объекта, чтобы обслуживать его контент как можно ближе к пользователям. Таким образом, сети CDN имеют функцию кэширования и, в частности, позволяют повысить доступность ресурсов или даже увеличить скорость, с которой становятся доступными данные, как правило, веб-страницы или мультимедийные потоки. Для этого CDN в основном используют два метода:

– Метод геолокации исходного IP-адреса DNS-запросов, отправленных от клиента. Таким образом, можно направить последний к серверам, наиболее близким к его географическому положению;

– Метод адресации, известный как Anycast, который состоит в том, чтобы делиться одним и тем же IP-адрес между несколькими серверами, также называемыми узлами в контексте любой трансляции. IP-маршрутизация позволяет пользователю быть направленным на «ближайший» сервер или узел.

Распределение вычислительной нагрузки на большое количество серверов может помочь повысить устойчивость к некоторым DDoS-атакам. Например, атака, проводимая из источников, сосредоточенных в одном географическом регионе, затронет только узлы, обслуживающие этот регион. Кроме того, атака, исходящая из источников, распределенных по всему миру, может иметь меньшее воздействие, поскольку атака будет поглощена всеми серверами CDN. [2]

Перенаправление по протоколу DNS. Некоторые службы защиты полагаются на пересылку DNS. Цель – направить трафик в домен, например, example.com, на IP-адрес сервера провайдера защиты. Последний затем занимается фильтрацией трафика, а затем перенаправляет его в исходный пункт назначения. Эта операционная модель часто предлагается сетями CDN для защиты веб-серверов своих клиентов. Когда клиент желает получить доступ к веб-сайту www.example.com,

сначала он запрашивает DNS-сервер, чтобы узнать IP-адрес веб-сервера. Сервер отвечает IP-адресом одного из облачных узлов. Таким образом, трафик между клиентом и веб-сервером будет проходить через CDN, который, таким образом, может фильтровать трафик перед его возможной передачей на защищенный веб-сервер.

Некоторые сети CDN концентрируют трафик, покидающий их сеть и предназначенный для защищенного объекта, на ограниченном количестве четко идентифицированных узлов. Это позволяет защищенному объекту создавать и поддерживать белый список IP-адресов, которые могут связываться с его серверами [1].

Другие технические и организационные меры. Помимо конкретных защитных решений, существуют передовые методы, которые могут помочь повысить устойчивость к атакам типа «отказ в обслуживании». Среди них, в частности, можно отметить:

– сегментация сети объекта для облегчения фильтрации в случае атаки и возможная изоляция определенных подсетей или определенных серверов;

– реализация фильтрации на границе сети объекта для авторизации только тех потоков, которые необходимы последнему для работы.

Эти методы также помогают ограничить риск непреднамеренного участия в атаке отказа в обслуживании. Кроме того, необходимо создание специальной административной сети. Действительно, атака может значительно повлиять на сетевую инфраструктуру объекта и, таким образом, привести к трудностям доступа к оборудованию. Как минимум, административный трафик должен быть отмечен как приоритетный посредством реализации маркировки QoS (Качество обслуживания) [3].

Чтобы справиться с атакой типа «отказ в обслуживании», необходимо определить системы, которые могут стать целью, и знать группы, ответственные за администрирование этих

систем. Кроме того, крайне важно иметь соответствующие контакты внутри компании, с операторами транзита, а также с поставщиками услуг защиты от DDoS-атак.

Список использованных источников:

1. DoS-атака [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0
2. Что такое DDoS-атака [Электронный ресурс]. – URL: https://aws.amazon.com/ru/shield/ddos-attack-protection/
3. Защита от DDoS [Электронный ресурс]. – URL: https://www.xelent.ru/services-additional/zashchita-ddos/
4. DDoS-атака – что это такое? [Электронный ресурс]. – URL: https://ddos-guard.net/ru/terminology/attacks/ddos-ataka
5. Способы защиты от DDoS-атак [Электронный ресурс]. – URL: https://timeweb.com/ru/community/articles/sposoby-zashchity-ot-ddos-ataki-1

Ключові слова: DDoS, DDoS-атака, захист від DDoS-атак.
Ключевые слова: DDoS, DDoS-атака, защита от DDoS-атак.
Keywords: DDoS, DDoS attack, DDoS attack protection.

Научный руководитель: *к.т.н., доцент Соколов А. В.*

Саніцька Інна Валеріївна
Національний університет «Одеська юридична академія»,
студентка 4 курсу факультету кібербезпеки
та інформаційних технологій

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Інформаційна безпека – це такий стан захищеності інформаційної інфраструктури, включаючи також комп'ютери та інформаційно-телекомунікаційну інфраструктуру і інформацію, що в них знаходиться, який також забезпечує сталий розвиток особистості, суспільства і держави.

На сьогодні в Україні немає чітко врегулювання вимог до Інформаційної безпеки на підприємствах. При цьому є вимоги які ставляться до компаній, які працюють з персональними даними громадян Європейського союзу відповідно до вимог General data protection regulation (GDPR), та деяких інших нормативних актів.

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

Не випадково питання інформаційної безпеки вже давно входять до головних пріоритетів практично всіх великих компаній. Останнім часом більше керівників середнього і малого вітчизняного бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією, системами її обробки і співробітниками, що беруть участь у цьому процесі [1].

Інформація може бути будь-якою, як інформація про вашу компанію, вашу особисту інформацію, ваші конфіденційні дані на вашому комп'ютері чи мобільному телефоні тощо.

Але це не єдине пояснення, яке дають нам науковці, адже інформаційна безпека – це порятунок життя організацій по всьому світі. Людей, які працюють у цій галузі, можна вважати та називати лікарями комп'ютерної системи.

Ми не можемо недооцінювати вплив кібератак, які можуть призвести до втрати даних, витоку особистої інформації, втрати часу та розповсюдження вірусів в організаціях.

Безпека – це сфера, яка може створити або в іншому випадку знищити компанію. Дуже важливо в організаціях тримати конфіденційну цифрову інформацію та захищати технічні системи від вірусів та хакерів [2].

Компанії впроваджують інформаційну безпеку з широкого кола причин. Основні цілі, як правило, пов'язані із забезпеченням конфіденційності, цілісності та доступності інформації про саму компанію.

Багато людей досі не мають уявлення про важливість інформаційної безпеки та її реалізації для організації. Багато менеджерів мають хибне уявлення про те, що інформація в їх комп'ютерах повністю захищена і не містить жодних загроз. На жаль, це є зовсім не так. Важливо відмовитись від переконання, що комусь неможливо проникнути у ваші особисті дані, чи дані вашої організації, оскільки компанія вживає заходів для захисту своєї інтелектуальної власності.

З розвитком технологій кібератаки швидко еволюціонують і будь-яка організація, яка має шляхи подолання наслідків кібератак, може не впоратись з хвилею нової атаки [3].

Нехтуючи інформаційною безпекою, вся компанія знаходиться в серйозній небезпеці, оскільки її дані та інформація від клієнтів та ділових партнерів знаходяться під загрозою. Кібератака може спричинити серйозні проблеми та незліченну шкоду бізнесу.

Американський політик Джо Енн Девіс зазначав: «Оскільки країна все більше покладається на електронне зберігання та зв'язок інформації, обов'язково потрібно, щоб уряд вносив відповідні зміни до наших законів про інформаційну безпеку». З цим важко не погодитись, адже через відсутність захисту інформаційних систем багато «успішних» атак були спрямовані на такі компанії.

Втрати у великих компаніях внаслідок кібератак часто викликають більш шокуючі суперечки навіть щодо кількості вкраденої інформації. Невеликі компанії, в такому випадку, чекає закінчення їх бізнесу та фінансових проблем, що призведуть до банкрутства установи.

Для багатьох організацій інформація є їх найважливішим надбанням, тому її захист є надзвичайно важливим.

Питання аналізу загроз і ризиків є визначальним при побудові ефективної системи захисту інформації. Однак, за

оцінками фахівців, лише не більше 5% підприємств використовують власні методики аналізу ризиків, що дозволяють виконувати кількісний аналіз та оптимізацію підсистеми інформаційної безпеки. Водночас дії внутрішніх порушників, такі як недбалість співробітників, крадіжки інформаційних ресурсів та IT-устаткування, фінансові й інші види шахрайства з використанням інформаційних систем і ресурсів тощо, набагато рідше стають предметом уваги при розв'язанні проблем інформаційної безпеки у випадку, якщо вони розглядаються у відриві від загальних завдань забезпечення економічної безпеки.

Впровадження інформаційної безпеки в організації може захистити технологію та інформаційні активи, які вона використовує, запобігаючи, виявляючи та реагуючи на внутрішні та зовнішні загрози.

Для підтримки стратегії інформаційної безпеки організації важливо підвищити обізнаність персоналу з питань інформаційної безпеки за допомогою тренінгів та семінарів. Організаціям також потрібно дотримуватися своїх політик захисту інформації та регулярно їх переглядати, щоб задовольнити вимоги безпеки.

Можливі загрози та вразливості повинні бути оцінені та проаналізовані. Це означає встановлення та впровадження контрольних заходів та процедур для мінімізації ризику та проведення аудиту для оцінки ефективності контролю [4].

Існує три основні цілі, які захищені інформаційною безпекою:

1. Конфіденційність – запобігає доступу несанкціонованих користувачів до інформації для захисту конфіденційності інформаційного вмісту. Порушення конфіденційності можуть відбутись через помилки під людським впливом, навмисне обмін даними або зловмисний вхід.

2. Цілісність –забезпечує достовірність та точність інформації. Втрата цілісності може статися, коли інформація не захищена від умов навколишнього середовища, не передана належним чином цифрова інформація або коли користувачі вносять несхвалені зміни.

3. Доступність – забезпечує авторизованим користувачам надійний доступ до інформації. Доступність забезпечується за допомогою безперервності процедур доступу, резервного копіювання або копіювання інформації, а також технічного обслуговування та мережевих з'єднань.

Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, вірогідність тощо, може призвести до досить негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами; розголошення відомостей, що становлять комерційну й інші види таємниць; порушення вірогідності фінансової документації; несанкціонованого доступу до персональних даних фізичних осіб тощо.

Найбільш зацікавленими сторонами в безпеці організації є клієнти, які не хочуть, щоб їхні дані були виставлені неналежним чином та всезагальний огляд.

Деякі фактори ризику, які можуть залишитися непоміченими, – це застаріле обладнання, незахищені мережі, неправильна конфігурація та навіть відсутність підготовки працівників. Також існує кілька помилок, які можуть підірвати конфіденційність інформації в компаніях.

Наявність ІТ-відділу, підготовленого до захисту інформації, сьогодні є фундаментальним. Уже існують різні засоби інформаційної безпеки, які дозволяють уникнути серйозних проблем та забезпечити цілісність та конфіденційність інформації, що, зрештою, є першим бажанням компаній. Інформація буде безпечною лише тоді, коли користувачі та ІТ-фахівці будуть діяти відповідно, створюючи найкращі способи уникнути майбутніх ризиків [5].

Нарешті, обізнаність щодо інформаційної безпеки організації є дуже важливою практикою для всіх середніх та великих компаній. Це захистить дані компанії, запобігаючи загрозам та будь-яким вразливостям.

Один з найважливіших девізів наукової фантастики говорить «майбутнє зараз», але це майбутнє, яке кожен зобов'язаний будувати.

Це просте повідомлення, але таке, що вимагає відданості підприємців визнанню безпеки як необхідного фактора у винаході майбутнього. Особливої уваги потребує реальне втілення заходів щодо забезпечення інформаційної безпеки, які мають стати основою для формування та реалізації інформаційної політики підприємства, захисту інформації від внутрішніх та зовнішніх загроз.

Список використаних джерел:

1. Сорокін О. Л. Інформаційна безпека та її складові: проблеми визначення кон- цепту. *Держава та право*. 2014. No8. С. 18–22.

2. Ніколаєв В., Остапович Г., Костицька І. та ін. Правове регулювання інформаційної безпеки у сфері підприємницької діяльності. К., 2002. С. 19–25

3. Шубіна О. В. Державна інформаційна безпека: проблеми визначення концепту. *Держава та права*. 2014. No3. С. 26–31.

4. Information Security Requirements: Your Obligations & Considerations, Published by Stephanie Baskerville June 10, 2020 Режим доступу: https://www.proserveit.com/blog/information-security-requirements

5. Караулов О. Н. Захист комп'ютерної інформації з точки зору міжнародного права. *Вісник Української академії державного управління при Президентові України*. 2014. No11. С. 53–63.

Ключові слова: Інформація, інформаційна безпека, кібератака, організація, економіка, компанія

Ключевые слова: Информация, информационная безопасность, кибератака, организация, экономика, компания

Keywords: Information, information security, cyber attack, organization, economy, company

***Науковий керівник**: д. фіз.-мат. н., професор Василенко М. Д.*

Сарокіна Владислава Володимирівна
Національний університет «Одеська юридична академія»
студентка 4-го курсу факультету кібербезпеки
та інформаційних технологій

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЕЛЕКТРОМАГНІТНИМ КАНАЛОМ

Актуальність даної теми полягає у тому, що на сьогоднішній день захист інформації від перехоплення за рахунок побічних електромагнітних випромінювань і наведень є однією з найважливіших задач в загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта технічного захисту інформації. Це пов'язано з тим, що в даний час широко застосовуються різні технічні засоби обробки інформації. Сама по собі інформація, що обробляється за допомогою технічних засобів являє собою найбільшу цінність, так як вона є найбільш простою в обробці, а перехоплення електромагнітних випромінювань дає можливість отримання доступу до оброблюваної інформації без прямого доступу до пристрою користувача. Об'єктами технічного захисту інформації є установи системи державного управління, військові і військово-промислові об'єкти, науково-дослідні установи і т.д.

Сам по собі захист інформації від витоку по електромагнітним каналах являє собою конкретний комплекс розроблених заходів, які виключають зовсім або ж знижують ступінь ймовірного неконтрольованого виходу інформації (як правило, конфіденційної) за межі зони, яка знаходиться під контролем, за рахунок електромагнітних полів побічного характеру [1].

Конструкторсько-технологічні заходи щодо локалізації можливості утворення умов виникнення каналів витоку інформації за рахунок побічних електромагнітних випромінювань і наведень у технічних засобах обробки і передачі інформації зводяться до раціональним конструкторсько-технологічним рішенням, до числа яких відносяться: спеціальні матеріали, що забезпечують зниження рівня паразитних електромагніт-

них випромінювань за межами виділених приміщень (поглинання і екранування); системи активної маскування, що створюють в разведопасних напрямках перешкоди, які знижують ймовірність перехоплення випромінювань; технічні засоби обробки інформації в захищеному виконанні. Для виключення можливості використання технічною розвідкою струмопровідних комунікацій, що виходять за межі зони, що охороняється, застосовуються засоби блокування, екранування і лінійного зашумлення.

Загалом, можна виділити наступні електромагнітні канали витоку інформації: мікрофонний ефект елементів електронних схем; електромагнітне випромінювання низької або високої частоти; виникнення паразитної генерації підсилювачів різного призначення; ланцюги харчування і кола заземлення електронних схем; взаємний вплив проводів і ліній зв'язку; високочастотне нав'язування волоконно-оптичні системи [3].

На сьогоднішній день найбільш відомими методами захисту інформації від витоку по електромагнітним шляхам є активний та пасивний метод захисту.

Суть активного методу захисту інформації полягає в застосуванні спеціальних широкосмугових передавачів перешкод. Його перевагою є те, що скасовується не тільки загроза витоку інформації по каналах електромагнітного випромінювання, але й деякі інші види загроз. Як правило, унеможливлюється прослуховування шляхом застосування закладних пристроїв, також стає неможливою використання випромінювання всіх інших пристроїв, що знаходяться у даному приміщені, з цілю проведення розвідки. Його недоліками можна назвати: наявність приховуваного випромінювання свідчить про те, що в даному приміщенні є інформація, що захищається, а це, саме по собі, привертає до відповідного приміщення підвищений інтерес зловмисників; можлива шкідливість досить потужного джерела випромінювання для здоров'я людини; за певних умов метод не забезпечує гарантований захист комп'ютерної інформації [2].

Пасивний метод передбачає екранування джерела випромінювання технічного засобу, тобто засіб обчислювальної техніки розміщується в екранованій шафі або в цілком екранованому приміщенні. Тобто екранується кожний технічний засіб, що входить до складу наших засобів обчислювальної техніки. Як недолік такого методу можна виділити високу вартість екранованого приміщення, якщо мова йде про декілька засобів обчислювальної техніки [2].

Для того, щоб приховати джерело випромінювання, застосовується сучасна технологія, що базується на нанесенні (наприклад, розпилення) на внутрішню сторону існуючого корпусу и саме тому зовнішній вигляд комп'ютера фактично не зміниться. Навіть за сучасних технологій захист комп'ютера є складним процесом. Отже, захист комп'ютера здійснюється в кілька етапів: 1) спочатку здійснюються спеціальні роботи для зібраного комп'ютера, де визначаються частоти, їх рівні, на яких присутній інформативний сигнал; 2) далі йдуть етапи аналізу конструктивного виконання комп'ютера, розробки технічних вимог, вибору методів захисту, розробки технологічних рішень і розробки конструкторської документації для даного конкретного виробу (або партії однотипних виробів); 3) після проходження перших двох етапів, виріб надходить власне у виробництво, де і виконуються роботи по захисту всіх елементів комп'ютера; 4) після цього повинні бути проведені спеціальні випробування для підтвердження обгрунтованості рішення. У разі успішного проходження випробувань, замовникові буде видано відповідний документ, у якому зазначено, що даний комп'ютер є захищеним від витоку інформації по каналах електромагнітного випромінювання [3].

Отже, на підставі вищевикладеного очевидно, що розробляються засоби захисту від витоку електромагнітними каналами, є необхідними для забезпечення безпеки інформації.

Список використаної літератури:

1. Ярутич А. О. Захист інформації від витоку технічними каналами. *Наука Онлайн*. 2019. № 1.

2. Артем'єва А. В. Захист інформації від витоку по електромагнітним каналам. *Сенергія наук*. 2019. № 33. С. 1006–1012.

3. Кірєєва Н. В. Виток інформації по каналам ПЕМВ та способи її захисту. *Міжнародний журнал прикладних та фундаментальних досліджень*. 2016. № 8. С. 499–504.

Ключові слова: електромагнітні канали, конструкторсько-технологічні рішення, заземлення, екранування.

Ключевые слова: электромагнитные каналы, конструкторско-технологические решения, заземление, экранирование.

Keywords: electromagnetic channels, design and technological solutions, filtration, grounding, shielding.

Науковий керівник: *к.т.н. доц. Кухаренко С. В.*

Сафонов Камиль Муханнадович
Национальный университет «Одесская юридическая академия»,
студент 2 группы факультету кибербезопасности
и информационных технологий

ЗАЩИТА УСТРОЙСТВ КОММУНИКАЦИИ ПОЛЬЗОВАТЕЛЯ ОТ RAT ВИРУСОВ

В современном мире актуализирована проблема вирусного поражения цифровых устройств пользователей. К их числу относятся самые опасные шпионские RAT вирусы (Remote Access Trojan – Троян удаленного доступа) [1].

Алгоритм работы этого вируса позволяет злоумышленнику получить полный удаленный доступ к устройству пользователя жертвы, а следовательно к его файлам, личным данным, видеокамере, геолокации, данным банковских карт и т.д.

Структурно, RAT вирус состоит из двух частей: клиентской и серверной. С помощью клиентской части, которая установлена на устройство злоумышленника, и серверной, которую, ничего не подозревая, запускает пользователь на своем устройстве коммуникации. После запуска серверной части RAT вируса, на устройстве коммуникации пользователя, в клиентской части

на устройстве злоумышленника появляется удаленный хост. В результате злоумышленник получает полный доступ к данным пользователя.

Отличительной особенностью рассматриваемого класса RAT вирусов является криптографическая обработка извлекаемых данных из устройства пользователя. Из-за этого антивирусное программное обеспечение не может определить сам факт передачи извлеченных данных на устройство злоумышленника [2]. Для защиты от последствий внедрения RAT вирусов на устройство пользователя существуют сложные решения, которые являются эффективными, однако в при использовании, обладают рядом недостатков.

Например, к их числу относится создание «виртуальной машины» на своем устройстве. Это позволяет выполнять любые действия в браузере или с файлами в пределах изолированной среды – «виртуальной машины», а не своего устройства [3]. Однако у такого решения есть существенный недостаток «виртуальная машина» потребляет значительное количество вычислительных ресурсов устройства. Следовательно, пользователь в этом случае будет терять время и аппаратные ресурсы из-за использования виртуальной и оперативной памяти «виртуальной машиной», которая, по сути, представляет собой дополнительную операционную систему. Также установка «виртуальной машины» требует много времени и знаний, которые есть не у каждого пользователя. Самым большим недостатком использования «виртуальной машины» является то, что многие вредоносное программное обеспечение, включая RAT вирусы, имеет возможность определить, что программа запущена в виртуальной среде, а не на реальном устройстве и таким образом, даже «виртуальная машина» не всегда предоставит полную безопасность пользователю. Однако, даже полностью подготовленный пользователь, с установленной на своё устройство «виртуальной машиной», всё равно имеет шанс стать жертвой внедрения RAT вируса.

Помимо самого вируса, угрозу несет и злоумышленник, который, прибегая к социальной инженерии, заставляет жертву совершить определенные действия, в том числе и установку вируса на своё устройство коммуникации. Для того чтобы защитить себя от последствий воздействия социальной инженерии достаточно понять основные типы и методы защиты от них [4].

Ведь помимо самого вируса, угрозу несет и злоумышленник, который, прибегая к приемам социальной инженерии, заставляет жертву совершить определенные действия, в том числе и установку вируса на своё устройство. Для того чтобы защитить себя от воздействия социальной инженерии достаточно понять основные ее методы воздействия на человека.

В основном фишинговые атаки выполняются благодаря поддельным сообщениям на почту или через профили в социальных сетях. В самом сообщении содержится форма для ввода персональных данных.

Также возможен и другой вариант развития событий, когда мошенник работает по заранее готовому плану действий, в результате которого он узнает от пользователя, любую нужную ему информацию.

И последний популярный вариант мошенничества с помощью социальной инженерии – «троянский конь». В этом случае мошенник ориентируется на эмоции жертвы, такие как страх, ненависть или жадность, манипулируя или угрожая пользователю, мошенник также с легкостью может получить всю необходимую ему информацию от пользователя.

Таким образом, любые защитные меры, включая антивирус, или «виртуальная машина» не всегда защитят пользователя от потери или утечки данных.

Самым эффективным вариантом решения рассматриваемой проблемы, является применение сетевого экрана. Его суть заключается в организации контроля за абсолютно всеми входящими и исходящими сетевыми соединениями устройства пользователя. Понятно, что в этом случае запросы

RAT клиента с компьютера злоумышленника на RAT сервер пользователя будут зафиксированы и обнаружены пользователем.

Понятно, что в этом случае злоумышленник не сможет удаленно подключиться к устройству пользователя, а значит и не сможет извлечь данные, хоть и сама серверная часть RAT вируса будет установлена и готова к выполнению поставленной задачи.

Таким образом, применение сетевого экрана не может исключить возможность попадания RAT вируса на устройство пользователя, но исключит возможность эксплуатации его серверной части злоумышленником.

Следует отметить, что правильная настройка и эксплуатация сетевого экрана является не самой простой для обычного пользователя задачей. Однако существует большое множество готовых решений с заранее установленными настройками, благодаря которым пользователь сможет легко фильтровать свой трафик, и тем самым обеспечить себе защиту от программ шпионов [5].

Несмотря на наличие этого решения, проблема защиты от RAT вирусов остается актуальной, так как малое число пользователей могут защитить себя от этого типа вирусов.

Именно это обстоятельство обуславливает устойчивую тенденцию массового использования злоумышленниками шпионского программного обеспечения RAT класса.

Список используемых источников:

1. Что такое RAT? Всё про шпионские RAT-трояны. [Електронний документ]. – URL: https://spy-soft.net/chto-takoe-rat/.

2. What is RAT Malware and How to Protect? [Электронный документ]. – URL: https://www.malwarefox.com/rat-malware/.

3. Вишняков В.А., Моздурани Шираз М. Г. Модели и реализация обнаружения вторжений в корпоративной информационной системе предприятия с использованием интеллектуального подхода. *Доклады БГУИР*. 2017. № 8 (110). [Электронный документ]. URL: https://cyberleninka.ru/article/n/modeli-i-realizatsiya-

obnaruzheniya-vtorzheniy-v-korporativnoy-informatsionnoy-sisteme-predpriyatiya-s-ispolzovaniem.

4. Соціальна інженерія в інтернет-просторі. [Електронний документ]. – URL: http://chtei-knteu.cv.ua/herald_ru/content/download/archive/2016/v3–4/NV-2016-v3–4_13.pdf.

5. Мохаммед Ф. О. Межсетевые экраны. *Доклады БГУИР*. 2009. № 5 (43). [Электронный документ]. URL: https://cyberleninka.ru/article/n/mezhsetevye-ekrany.

Ключові слова: RAT вірус, структура RAT вірусу, віртуальна машина, мережевий екран, захист від RAT вірусів.

Ключевые слова: RAT вирус, структура RAT вируса, виртуальная машина, сетевой экран, защита от RAT вирусов.

Keywords: RAT virus, RAT virus structure, virtual machine, firewall, protection against RAT viruses.

***Научный руководитель**: доцент Задерейко А. В.*

Соловйов Артем Сергійович
Національний університет «Одеська юридична академія»,
студент 3 курсу факультету кібербезпеки
та інформаційних технологій

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ

В настоящие время существует проблема кражи персональных данных. В условиях глобализации пользования человека всё больше приобретает связь с глобальной сетью Интернет. За последние десятилетие количество пользователей возросло. Работая в интернете человек получает множество полезной информации, но иногда он может не заметить то как его персональные данные оказываются под большой угрозой. Вопрос о защите персональных данных является очень актуальным, особенно является актуальной информация защита персональных данных, попавшая в интернет. Личные данные – это любые данные, идентифицирующие человека. Ваше имя, адрес электронной почты, местоположение, биометрические данные, логин [1].

В современном мире практически у каждого человека есть электронная почта, профили в различных социальных сетях. В любом случае взлом аккаунтов может привести в потере персональных данных. Отдельным вопросом защиты персональных данных в интернете возникает, если обратить внимание на электронную коммерцию, ведь онлайн покупки стали естественным явление для большинства людей.

При совершении платёжных операций, стоит особо внимательно изучить сайт, на котором будет производиться покупка товара, нежелательно привязывать свою банковскую карту к платёжной системе банка. В повседневной жизни люди оставляют за собой. Цифровую информацию о том: где живут, какую еду предпочитают, что и где покупают и другие данные о личной жизни. По этим элементам жизни человека, можно узнать больше, чем они сами хотели бы о себе рассказать.

Узнав такую информацию о человеке, мошенник может воспользоваться методом социальной инженерии и получить ещё больше персональных данных чем человек мог оставить в интернете.

Угроза потери персональных данных может привести к подмене данных для выполнения входа в социальные сети. Из-за потери персональных данных могут появляться фейковые аккаунты в социальных сетях для проведения мошеннических операций. Получение финансовых данных: номера кредитных карт, электронных кошельков, аккаунтов платных онлайн игр. А также мошенник, получив персональные данные человека может их удалить.

Пользуются персональными данными не только злоумышленники. Личными данными человека также активно интересуются специалисты по таргетинговой рекламе. Главный источник получения сведений для данного вида рекламы – файлы cookie, которые передаются браузером пользователя на сервер таргетингового агентства [2].

Методы самостоятельной защиты персональной информации. Защиту от вирусов, которые могут овладеть личными

данными могут обеспечить только лицензированные антивирусные программы, которую нужно постоянно обновлять. Перед установкой программ из не проверенных источников или регистрацией на сайтах с введение персональных данных, требуется внимательно прочитать пользовательское соглашение, поскольку одним из его условий может быть обработка и использование личной информации.

Пользователи мобильных устройств имеют функцию, разрешения или запрета получения приложением личной информации, например: геолокация, список записной книжки, фотогалерея, камера и внутренние файлы устройства. Важно иногда проверять какие личные файлы вы доверили приложению на своём устройстве. При появление подозрительных действий со стороны приложения рекомендуется отказаться от установки и пользования таки приложением.

Для предоставления лучшей зашиты в социальных сетях или других электронных сервисах, советуется использовать сложные пароли. Для создания паролей можно использовать генератор паролей. Для каждого сервиса рекомендуется использовать отдельный пароль, чтоб они не повторялись. Менять пароли следует менять каждые пару месяцев.

А также для большей защиты своих данных и аккаунтов, требуется использовать двойную аутентификацию. Каждый раз для входа будет требоваться код, который будет случайно генерироваться в стороннем приложении для большей надёжности.

В местах где вы можете подключиться к бесплатным точкам доступа к интернету, часто сидят злоумышленники, которые могут перехватить ваш трафик и получить ваши личные данные. Для этого можно использовать VPN сервисы, которые будут шифровать ваш трафик, и злоумышленнику будет сложней получить ваши данные.

В заключение можно выделить правила для пользования интернетом, которых следует придерживаться, чтобы обеспечить свои персональные данные.

1. Следить за тем что и кому пересылается в сообщениях.

2. Внимательно изучать лицензионное соглашение на наличие пункта об обработке персональных данных.

3. При пользовании электронной коммерции, не привязывать свои банковские карты в непроверенных сервисах.

Таким образом, можно обеспечить достаточную защиту персональных данных. Существует множество способов обезопасить свои данные через генераторы паролей, двух этапная аутентификация и различные приложения для шифровки трафика в интернете, так как защита личной информации в современном мире это большая проблема, много злоумышленников пытаются украсть вашу информацию, прикрываясь поддельными сервисами очень похожими на настоящие.

Список використаних джерел:

1. Юрист и закон [Електронний ресурс] – Режим доступу до ресурсу: https://uz.ligazakon.ua/magazine_article/EA012189.

2. SEARCHINFORM [Електронний ресурс] – Режим доступу до ресурсу: https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-internete/.

Ключові слова: Персональні дані, особиста інформація, інтернет, захист.

Ключевые слова: Персональные данные, личная информация, интернет, защита.

Key words: Personal data, personal information, internet, protection.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Степанов Денис Вікторович
Національний університет «Одеська юридична академія»,
студент 2-го курсу факультету кібербезпеки
та інформаційних технологій

ІНСТРУМЕНТАРІЙ QT ДЛЯ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У наш час існує величезна кількість цікавих технологій і рішень в IT-сфері і початківцям доволі важко обрати шлях, яким

варто розвиватися, щоб досягти успіху. Qt як потужний інструментарій розробки програмного забезпечення (ПЗ) – це один з достойних претендентів для вивчення, позаяк має потужний функціонал і дозволяє запускати написане його засобами ПЗ в більшості сучасних операційних систем шляхом простої компіляції програми для кожної системи без змінення коду.

IDE Qt було випущено 1995 року, хоча Хаарвард Норд і Айрик Чеймб-Інг розпочали роботу над ним ще 1990 року. Працюючи над цим проектом було вирішено розробити об'єктно-орієнтовану систему з візуальним середовищем розробки графічного інтерфейсу. У 1991 Хаарвард написав класи, які і стали першоосновою Qt. До 2005 року середовище розробки Qt версії 4.0 вже мало близько 500 класів і понад 9000 функцій, підтримувало численні платформи як для комерційної розробки, так і для розробки з відкритим кодом [1].

Основною мовою програмування для Qt є C++, але не лише з нею можливе використання бібліотек та модулів. Для Python – це PyQt або PySide (PyQt через використання ліцензії GPL може використовуватися лише для відкритих проектів або за ліцензією, а PySide використовує ліцензію LGPL, що дозволяє використовувати її у закритих проектах), для Java – Qt Jambi, PHP – PHP-Qt.

Найбільш відомим модулем, який може працювати самостійно, є Qt Designer. По суті цей модуль є графічним дизайнером інтерфейсу користувача, який дозволяє створювати та налаштовувати форми без написання коду [2]. Qt Designer має бібліотеку елементів інтерфейсу, кожен з яких має набір властивостей. Qt Designer дозволяє створювати адаптивний інтерфейс не лише для персональних комп'ютерів, а й для мобільних пристроїв. Крім того, Qt має багато інших готових модулів з готовими функціями широкого спектра застосування [3]. Ось деякі з них:

– QtCore – базовий неграфічний модуль Qt, на який зав'язані всі модулі бібліотеки Qt. Саме QtCore спрощує зв'язок класів всередині програми і містить різні ідентифікатори, які використовуються у всьому Qt;

– Qt SQL – це важливий модуль, який забезпечує підтримку баз даних. API Qt SQL поділяються на різні рівні: рівень драйвера, рівень SQL API та рівень інтерфейсу користувача;

– Qt Multimedia – це модуль для роботи з мультимедійним контентом (аудіо композиціями, відеозаписами, плейлистами тощо). Він надає необхідні API для доступу до функцій камер. Вбудований Audio Engine дозволяє керувати та налаштовувати відтворення 3D-аудіо;

– Qt Network – це модуль з різними класами C++, які надають програмні засоби роботи з протоколом TCP/IP, cookie файлами та HTTP-запитами, пропонує класи високого рівня QHttp і QFtp для роботи з відповідними протоколами прикладного рівня і низькорівневі класи, як-от: QTcpSocket, QTcpServer і QUdpSocket. Модуль використовують при програмуванні мережевих застосунків, наприклад, є можливість створювати сервери і клієнти TCP/IP, файлообмінники тощо;

– Qt QML та Qt Quick – є основою для розроблення декларативною мовою програмування QML, заснованій на JavaScript, дивовижних користувацьких інтерфейсів з анімацією, які можна використовувати як самостійні JavaScript-скрипти або інтегрувати у QML-код;

– Qt Charts – модуль для реалізації інтерактивних динамічних двомірних графіків з використанням C++ і/або технології Qt Quick;

– Qt Data Visualization дозволяє за лічені хвилини створювати інтерактивні тривимірні графіки для візуалізації даних;

– Qt Virtual Keyboard – повнофункціональна налаштовувана віртуальна клавіатура, використання якої дозволить реалізувати інтерфейс для пристроїв з сенсорним екраном чи то інші технології введення;

– Qt Quick Enterprise Controls – додаткова бібліотека візуальних елементів для створення інтерфейсів промислового призначення;

– Qt Enterprise Tooling – інструменти для профілювання, локалізації, документування, створення інсталяційного пакету та розгортання застосунків.

І це ще не весь перелік засобів Qt. Інструментарій професійного рівня Qt пропонує розробникам модульну бібліотеку, яка налічує понад 700 C++ класів, технологію Qt Quick для створення UI засобами декларативної мови QML. Важливою перевагою Qt є потужний набір інструментів для швидкої багаторівневої розробки ефективного високопродуктивного ПЗ. Суттєво, що для зручності сотні класів поєднані у модулі, які можна доповнювати та наслідувати. Завдяки підтримці Visual Studio, можна застосовувати Qt Quick безпосередньо в середовищі розробки Qt Creator.

Наявність детальної документації для кожного класу з описом всіх методів і функцій, прикладів застосування, зручної класифікації класів є доволі зручними для користувача, особливо на начальному етапі під час навчання. Крім того, важливою є можливість швидкого старту розробки, завдяки зручним інсталяторам, готовим інструментам і можливості створення прототипів одразу після встановлення.

Фреймворк QT вбудованими засобами автоматично очищує виділену пам’ять і позбавляє програміста від ручного керування пам'яттю, а також має механізм сигналів та слотів для створення подій. Це дає значну гнучкість у програмуванні з високим рівнем абстракції. Разом з тим QT дозволяє використовувати низькорівневі інструменти мови.

Ключовою перевагою Qt є можливість написання кросплатформних програм, тобто можливість застосування одного коду для різних платформ, операційних систем і пристроїв. При чому, підтримуються мобільні платформи (Android, iOS та інші), десктопні (Windows, Linux, Mac), вбудовані (Embedded Linux, Embedded Android, Windows Embedded, QNX, VxWorks тощо).

Недоліком Qt можна вважати доволі великі розміри створюваних застосунків, позаяк долучені використовувані бібліотеки займають понад 15 Мб. А для мобільних платформ велика «вага» ПЗ здебільшого неприпустима. Проте це не применшує популярність технології QT для розробки кросплатформного

ПЗ будь-якого рівня складності для UNIX-подібних систем та Windows.

Список використаних джерел:

1. Краткая история развития Qt. URL: https://www.opennet.ru/docs/RUS/qt3_prog/f71.html (дата звернення: 01.11.2020).
2. Qt Designer Manual. URL: https://doc.qt.io/qt-5/qtdesigner-manual.html (дата звернення: 01.11.2020).
3. Qt Documentation. URL: https://doc.qt.io (дата звернення: 01.11.2020).

Ключові слова: Qt, інструментарій розробки програмного забезпечення, кросплатформне ПЗ, графічний інтерфейс користувача.

Ключевые слова: Qt, инструментарий разработки программного обеспечения, кроссплатформенное ПО, графический интерфейс пользователя.

Keywords: Qt, software development toolkit, cross-platform software, graphic user interface.

***Науковий керівник**: к.т.н., доц. Трофименко О. Г.*

Стаднік Денис Андрійович
Національний університет «Одеська юридична академія», студент 3-го курсу факультету кібербезпеки та інформаційних технологій

ПРОТИДІЯ ЗЛОЧИНЦЯМ В МЕРЕЖІ DARKNET

DarkNet – прихована мережа, з'єднання якої встановлюються тільки між довіреними бенкетами, з використанням нестандартних протоколів і портів. Анонімна мережа являє собою систему не зв'язаних між собою віртуальних тунелів, що надає передачу даних в зашифрованому вигляді. Даркнет відрізняється від інших розподілених тимчасових мереж, так як файлообмін відбувається анонімно, і, отже, користувачі можуть спілкуватися без особливих побоювань і державного втручання.

Зброя, фальшиві гроші, наркотики, крадений кредитки – Це не повний перечнь всього наявного. Це справжнє дно інтернету, де щодня покидьки порушують закон. Вони настільки небезпечні тільки через те, що навчилися використовувати і комунікувати між собою за допомогою Darknet.

Всі адреси, через які вони працюють використовують домен. onion, а такого по суті не існує. ICANN (американська корпорація), без якої не виникне ні один домен першого рівня, нічого подібного не санкціонувала. Однак ці правила не поширюються в DarkNet. Вони не замінюють звичайний інтернет, але створюють поверх публічного Інтернету замасковані, огорожі від зовнішнього світу мережі передачі даних з криптографічним захистом трафіку і своїми методами адресації ресурсів. Використовувати Darknet можна тільки за допомогою технології Tor. Пакет даних, який передається по вузли Tor-мережі, багаторазове шифрується. Ланцюжок з'єднань між двома користувачами будується випадковим чином. Перехоплення даних в одній з ланцюжків не дасть потрібної інформації про користувача або про дані. За допомогою криптографічного захисту всіх даних, це дає можливість сховатися від спостереження.

Як тільки слідчі виявлять активність, пов'язану з наркотиками в реальному світі, вони зацікавляться тим, що робиться онлайн. Спостереження і таємні операції дозволяють визначити ті точки, де зустрічаються реальний і віртуальний світ.

Торговці наркотиками і іншими забороненими засобами використовують свої замасковані сайти тільки як магазини, а шукають клієнтів у відкритому интеренете. Через це торговці забороненим є досить вразливою мішенню. Відповідно до закону, адміністратори сайтів зобов'язані співпрацювати з поліцією і передавати їм необхідну інформацію.

Для боротьби з продажами наркотиків в інтернеті використовується метод знаходження та перевірки інформації про сайтах, на яких можна купити наркотики. Обчислення злочинців в TOR займає багато часу. Спершу за підозрюваним ведуть спостереження, паралельно перевіряючи всіх з ким він

спілкується і його клієнтів. Буває що вже на цьому етапі злочинець робить помилку, за допомогою якої обчислюють його справжній IP-адресу. Після цього його місце розташування стає відомо і його можна успішно затримати. Злочинців в TOR ловлять і за допомогою підставних ресурсів, форумів та посилань. На них розміщують зображення і відео, частина яких розташовується в іншій доменній зоні – наприклад.com або. ru. Картинки відкриваються поза TOR-браузера, і поліцейські відразу дізнаються справжню IP-адресу зловмисника. Часто агенти спец.служб входять в довіру до адмінам заборонених сайтів і уявляють себе в ролі торгашів і споживачів. Боротися з фінансовими шахраями допомагають банківські сервера. Коли злочинець входить в акаунт, який він вкрав або електронний гаманець, що надходить трафік на сервер починає сповільнюватися. Навіть якщо злочинець захищає своє з'єднання, ці затримки будуть у в його зашифрованому трафіку – Таким способом можна довести його провину. Самий вразливий момент для злочинця це висновок грошових коштів, так як для цієї операції потрібно знайти спеціально навченого людини, якими можуть виявитися ті самі агенти спец служб. «Більшість таких випадків разові, і правоохоронці постійно повинні шукати особливий підхід для злочинця».

Зараз в світі задаються питанням, як забезпечити більш ефективний і швидкий спосіб пошуку злочинців. Це війна білого і чорного, і як в будь-якій сучасній війні, щоб її закінчити мало однієї тактики, хитрощів і вивертів. Потрібно мати нову, сучасну зброю, яка зможе поставити крапку в цій війні. Якщо уявити технологію, яка могла б зчитувати дані користувача навіть через Onion посилання, або створити масштабний штучний інтелект, який буде сам відслідковувати незаконні дії користувачів на всіх сайтах і передавати інформацію до відповідних органів, це б змінило все. Однак для створення цих технологій потрібні великі кошти, а так само необхідно щоб люди зрозуміли всю небезпеку даркнета і кинули більше сил для боротьби. Але як можна було помітити, анонімність користувачів в самому даркнета переоцінена. Зловмисники

з DarkNet залишаються безкарними лише до тих пір, поки правоохоронні органи не починають приймати контрзаходи, які найчастіше бувають засновані не на новітніх технологіях машинного навчання, а на класичних методах розслідування.

Список використаних джерел:

1. Что такое Даркнет [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82.

2. Как ловят преступников в DarkNet [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/wirex/blog/400723/

Ключові слова: Даркнет, протидія, злочинці
Ключевые слова: Даркнет, противодействие, преступники
Keywords: Darknet, anti-action, criminals
***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Трєгубов Нікіта Олександрович
Національний університет «Одеська юридична академія»,
студент 3 курсу факультету кібербезпеки
та інформаційних технологій

МЕТОДЫ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ ПОЛЬЗОВАТЕЛЯ

Все мы сталкивались с небольшим оповещением на сайте о том, что надо принять «cookie» файлы, принять условия соглашения конфиденциальности, о сборе данных и так далее, и просто дальше пользовались сетью Интернет. Но задумывались ли вы на что именно соглашаетесь? Были ли у вас мысли что именно за данные вы отдаёте компаниям, чьими услугами вы пользуетесь?

Возьмем, например, компанию Google. Данная компания собирает данные обо всём что вы делаете, когда вы пользуетесь любым из предлагаемых продуктов или асоциированных

с нею. Почти каждый интернет-магазин асоциирован с маркетинговым продуктом Google – AdSense. Когда вы интересуетесь определенным товаром, то он обязательно когда-нибудь появится в рекламных блоках, интеграциях в видеороликах. Но почему так? Потому что вам уже был присвоен определенный рекламный идентефикатор [1]. Действует он ровно как личное дело или как история браузера. В нём накапливается список сайтов или товаров, которыми вы интересуетесь в данный момент либо интересовались. После чего на базе этого идентификатора алгоритм пытается предоставить в рекламе товары, имеющие наибольший шанс вас заинтересовать на определённый интернет-магазин, который выкупил рекламу. Такой технологией пользуется не только Google, но и другие гиганты IT-индустрии, но именно Google начала собирать данные о вашей геолокации и использовать её в маркетинговых целях. Никто вас не заставляет дальше давать информацию о ваших посещениях – вы можете без проблем выключить данную функцию сбора данных в вашем аккаунте Google.

Перейдем к социальным сетям, взяв за основной пример компанию Facebook. Представленная компания тщательно следит за своими пользователями используя огромное количество различных алгоритмов, а также устройства самих пользователей. Так, в 2017 году один из пользователей социальной сети уличил компанию в слежке на повседневной основе, воспользовавшись микрофоном смартфона для подслушивания бытовых разговоров вдали от телефона, обрабатывая полученные данные и выдавая соответствующую контекстную рекламу. Но недавно Facebook была замечена за продажей данных, использования в своих целях, а также в политической рекламе. Также в 2019 году данные сотен миллионов пользователей были опубликованы в открытом доступе, за что Facebook получил штраф в размере 5 миллиардов долларов США [2].

Допустим, мы можем отказаться от социальных сетей и найти альтернативу. Но что если даже ваша операционная система начинает следить за вашими действиями? Недолго

после выхода операционной системы Windows 10, стало известно, что компания Microsoft начала собирать данные о посещённых сайтах, местоположении, голосовой речи, используемых приложениях и даже получает данные о том, что вы печатаете на клавиатуре [3]. С недавними обновлениями данного продукта стало возможно отключить скрытую функцию, но раньше многие не просто не могли это отключить – они даже не знали, что данная функция слежки присутствует в Windows 10.

Может показаться, что от всего можно скрыться задействовав технологию VPN и ни о чем больше не беспокоится. Так можно было действовать 10 лет назад, но не сейчас. На данный момент в скрытом режиме сайт может собирать не просто данные о браузере, но и системе вцелом: какая версия операционной системы используется, какие технологии поддерживает браузер, какие спецификации вашего устройства, какие установлены шрифты, какой ваш публичный и локальный IP адрес и так далее. Это называется «отпечатком» и у каждого он уникальный. Если мы хотим всё это прикрыть и больше никому не выдавать информацию о вашем устройстве, то какие технологии и программы использовать? На данный момент есть несколько систем, позволяющие скрыть ваше присутствие в сети:

– Операционная система Tails. Это действующая в режиме реального времени операционная система Linux, которую можно запускать практически на любом компьютере с DVD, USB-накопителя или SD-карты и не оставлять следов на компьютере, который вы используете. Важной особенностью Tails является то, что все исходящие соединения вынуждены проходить через Tor, а не анонимные соединения блокируются.

– Операционная система Whonix. Операционная система состоит из двух виртуальных машин: один исключительно управляет Tor и действует как шлюз, который называется Whonix-Gateway. Другой, который называется Whonix-Workstation, находится в полностью изолированной

сети. Отличие между ними в том, что Tails это независимая операционная система, которую можно запустить с любого компьютера, и она не оставляет после себя следов, а также не хранит данные. Каждый раз при запуске системы она будет как новая. В свою очередь Whonix устанавливается на уже готовую ОС посредством виртуальной машины, и она сохраняет все данные, одна Whonix невозможно деанонимизировать.

– Програмное обеспечение AntiOS является небольшой программой с открытым исходным кодом на Python и является самым простым способом изменить данные о вашем компьютере. Большую эффективность показывает в работе с другими приложениями.

– Браузер Linken Sphere. Браузер работает в OTR-режиме, что делает его самым безопасным. На компьютере не сохраняется абсолютно никаких следов действий, что не позволит даже случайно попавшим на машину вредоносным программам получить доступ к информации, шифрует всю сохраняемую информацию по стандарту шифрования AES-256, позволяет одновременно работать с различными типами подключений в мультипоточном режиме HTTP, SOCKS, SSH, TOR, TOR + SSH и многие другие функции возможны в данном продукте.

Многие компании хотят знать как можно больше о потенциальных клиентах, собирая как можно больше данных об их действиях и только те люди, которые ценят себя и свою личную жизнь, знают как себя обезопасить от скрытого сбора данных о себе.

Список использованной литературы

1. Политика конфиденциальности и Условия использования Google [Електронний ресурс] – Режим доступу до ресурсу: https://policies.google.com/technologies/partner-sites?hl=ru

2. Как Facebook собирает и продает данные пользователей [Електронний ресурс] – Режим доступу до ресурсу: https://www.tadviser.ru/index.php/Статья:Как_Facebook_собирает_и_продает_данные_пользователей

3. Windows 10 поставляется с кейлоггером [Електронний ресурс] – Режим доступу до ресурсу: https://xakep.ru/2014/10/10/windows-10-keylogger/

Ключові слова: дані, система, Facebook, Google.
Ключевые слова: данные, система, Facebook, Google.
Keywords: data, system, Facebook, Google.
***Науковий керівник**: д. фіз.-мат. н., професор Василенко М. Д.*

Лопаєв Дмитро Валерійович
Національний університет «Одеська юридична академія»,
студент 4 курсу факультет кібербезпеки
та інформаційних технологій

ЗАХИСТ ІНФОРМАЦІЇ В СУЧАСНИХ СИСТЕМАХ РАДІОЗВ'ЯЗКУ ТЕХНОЛОГІЇ LTE

Необхідність захищати технології LTE приманює багато уваги операторів мобільного зв'язку, так і рядових користувачів інтернету.

Бездротові цифрові тенета, яскраво стартувавши, постійно розвиваються і дуже швидко. Це грає на руку в мікроелектроніці, що допускає можливість робити все складніші і також – дешевші – засоби бездротового зв'язку.

Технологія WIMAX (IEEE802.16–2004) не була тепло прийнята, вона уступала по швидкості, конфідеційності і вартості. Але оператори очікують інноваційного прориву від мобільного WIMAX (IEEE802.16e).

Розвиток технології LTE як стандарту офіційно розпочався наприкінці 2004 року. Основною метою початкового дослідження є вибір 84 технологій фізичного рівня, які можуть забезпечити високу швидкість передачі даних. В якості запропонованих запропоновано два основні варіанти: розробка звичайного бездротового інтерфейсу W-CDMA (для HSPA) та створення на основі технології OFDM (ортогональне мультиплексування з частотним поділом) нової добірки.

Результатом цього дослідження є те, що єдиною відповідною технологією став OFDM, таким чином встановив першу специфікацію для еволюціонованого радіоінтерфейсу UMTS Terrestrial Radio Access (E-UTRA).

Порівняно з системами 3G, радіоінтерфейси LTE забезпечують покращені технічні характеристики. Зокрема, в LTE пропускна здатність змінюється з 14 МГц на 20 МГц, що відповідає потребам різних операторів з різною пропускною здатністю. Обладнання LTE одночасно підтримує щонайменше 200 активних з'єднань, або телефонних дзвінків на соту [1].

Мережа LTE також покращує ефективність використання радіочастотного спектру, тобто обсяг даних, що надсилаються в межах заданого діапазону частот, набагато більший.

Це забезпечує підтримку зв'язку для абонентів, які рухаються зі швидкістю до 350 км / год. У звичайному режимі БС може подолати до 30 км, але він може працювати з осередками радіусом більше 100 км. Також є підтримка багатоантенної системи MIMO (кілька входів і кілька виходів).

Принцип побудови бездротового інтерфейсу LTE базується на трьох основних технологіях: мультиплексування з використанням ортогональної OFDM, багатоантенної системи MIMO та еволюційної архітектури системи.

Дуплексний поділ каналу може бути частотним FDD і часовим TDD. Це дозволяє операторам дуже гнучко використовувати частотні ресурси. Це рішення відкриває шлях на ринок для компаній, які не мають спарених частот.

Що стосується використання частотних ресурсів, то ефективність самої системи FDD набагато вища, ніж у TDD – вона має менші накладні витрати (поля обслуговування, інтервали тощо).

Подальший розвиток технології LTE знайшов своє продовження як частина нового стандарту LTE Advanced. Поки що відповідають основним вимогам LTE Advanced: [1]

1. Максимальна швидкість передачі даних бездротового каналу низхідної лінії зв'язку становить до 1 Гбіт/с, а макси-

мальна швидкість передачі даних висхідної лінії зв'язку до 500 Мбіт/с (середня пропускна здатність на користувача втричі перевищує LTE).

2 Пропускна здатність висхідної лінії зв'язку становить 70 МГц, а пропускна здатність висхідної лінії зв'язку становить 40 МГц.

3. Максимальна ефективність використання спектру в бездротовому каналі низхідної лінії зв'язку становить 30 біт/с/ Гц, а висхідна лінія зв'язку становить –15 біт/с/ Гц (втричі вище, ніж LTE).

4. Абсолютна сумісність із LTE та іншими системами.

Як вже згадувалося раніше, LTE використовує модуляцію OFDM, яка була глибоко вивчена у DVB, Wi-Fi та WIMAX.

Технологія OFDM передбачає передачу широкосмугових сигналів шляхом незалежної модуляції вузькосмугових типу $Sk(t)=\sin[2\pi(f0+k\Delta f)]$, які розташовані на певних кроках частоти Δf.

Символ OFDM містить групу модульованих підносійних. У часовій області символ OFDM включає поле даних (корисна інформація) та так званий циклічний префікс, який є сегментом у кінці попереднього символу, який циклічно передається [1].

Для вирішення цих нюансів у випадку частотного дуплекса використовується більш широкий радіоканал (до 100 МГц) та асиметричне розділення смуги пропускання між висхідними та низхідними каналами; вдосконалена система кодування та виправлення помилок; висхідна лінія Гібридні OFDMA та SC-FDMA технології для зв'язку, а також передові рішення в галузі антенних систем MIMO.

Метод встановлення та підвищення ефективності сучасних систем полягає у відборі методів, інструментів та алгоритмів за кількома критеріями на різних етапах аналізу та фактичної реалізації.

Процеси, що виникають в радіосистемах, потребують використовувати складні математичні прилади, і не завжди

вдається отримати необхідні функціональні залежності в аналітичній формі.

Можна зробити висновок, що для дослідження радіосистеми також потрібно використовувати багато математичних моделей, які слід проводити на базі сучасних комп'ютерних систем, а потім розробляти конкретні користувальницькі інтерфейси для кожного функціонального блоку та всієї системи [1].

Список використаних джерел:

1. Застосування технології LTE у системах реального часу – 2009. – URL: http://jrnl.nau.edu.ua/index.php/SBT/article/-view/5242/5784 (дата звернення: 18.11.2020)

Ключові слова: технологія LTE, технологія 3G, радіочастнотний спектр, радіоінтерфейс, антенні системи MIMO, WIMAX, W-CDMA, OFDM, Evolved UMTS Terrestrial Radio Access (E-UTRA), SC-FDMA.

Ключевые слова: технология LTE, технология 3G, радиочастотный спектр, радиоинтерфейс, системы антенн MIMO, WIMAX, W-CDMA, OFDM, наземный радиодоступ Evolved UMTS (E-UTRA), SC-FDMA.

Keywords: LTE technology, 3G technology, radio frequency spectrum, radio interface, MIMO, WIMAX, W-CDMA, OFDM, Evolved UMTS Terrestrial Radio Access (E-UTRA), SC-FDMA.

***Науковий керівник**: д. фіз.-мат. н., професор Василенко М. Д.*

Yurganov Vladislav Yurievich.
National University «Odessa Law Academy»,
4th year student of the Faculty of Cybersecurity
and Information Technologies

DATA PROTECTION IN COMPUTER NETWORKS

It is no coincidence that data protection in computer networks is becoming one of the most pressing problems in modern computer science. To date, three basic principles of information security have been formulated, which should ensure [1].

- data integrity;
- confidentiality;
- availability.

When considering the problems of data protection in the network, first of all, the question arises about the classification of failures and violations of access rights that can lead to the destruction or unwanted modification of data. Among these potential «threats» are:

1. Loss of information due to incorrect software operation:
– failures of servers, workstations, network cards;
– loss or change of data in case of software errors.
2. Unauthorized access losses:
– losses when the system is infected with;
– unauthorized copying, destruction or forgery of information.
3. Hardware failures:
– cable system failures;
– power outages;
– failures of disk systems;
– failures of data archiving systems.
4. Errors of service personnel and users:

– familiarization with confidential information constituting a secret of unauthorized persons or accidental destruction or modification of data.

Depending on the possible types of network disruptions (by disruption, we also mean unauthorized access), numerous types of information protection are combined into three main classes:

– physical protection means, including means of protection of the cable system, power supply systems, archiving means, disk arrays, etc.

– software protection tools, including: anti-virus programs, systems of differentiation of powers, software access control.

– administrative security measures, including control of access to premises, development of a firm's security strategy, contingency plans, etc.

The cable system remains the main problem of most local area networks: according to various studies, it is the cable system that is the cause of more than half of all network failures [2]. In this regard, the cabling system must be given special attention from the very moment of network design.

Improving the reliability and data protection in the network, based on the use of redundant information, is implemented not only at the level of individual network elements, such as disk arrays, but also at the network operating system level. So, over the past ten years, Novell has been implementing fault-tolerant versions of the Netware operating system – SFT (System Fault Tolerance), which provide for three main levels:

– SFT Level I. The first level provides, in particular, the creation of additional copies of FAT and Directory Entries Tables, immediate verification of each newly written data block to the file server, as well as backup on each hard disk about 2% of the disk space. If a failure is detected, the data is redirected to the reserved area of the disk, and the bad block is marked as bad and is not used in the future.

– SFT Level II additionally contained the ability to create «mirrored» drives, as well as duplication of disk controllers, power supplies and interface cables.

– The SFT Level III version allows the use of duplicated servers in the local network, one of which is the master, and the second, containing a copy of all information, comes into operation in the event of a master server failure.

The main and most common method of protecting information and equipment from various natural disasters (fires, earthquakes, floods, etc.) consists in storing archival copies of information or in placing some network devices, for example, database servers, in special protected premises located as a rule, in other buildings or, less often, even in another area of the city or another city.

The problem of protecting information from unauthorized access has become especially acute with the widespread use of local and, especially, global computer networks. It should also be noted that often the damage is caused not because of malicious intent, but because of elementary user errors that accidentally spoil or delete vital data. In this regard, in addition to access control, a necessary element of information protection in computer networks is the differentiation of user rights.

By equipping the server or network workstations, for example, with a smart card reader and special software, you can significantly increase the level of protection against unauthorized access. In this case, to access the computer, the user must insert a smart card into the reader and enter his personal code. The software allows you to set multiple levels of security, which are managed by the system administrator. A combined approach with the introduction of an additional password is also possible, with special measures taken against interception of the password from the keyboard. This approach is much more reliable than using passwords, because if the password is snooped, the user may not know about it, but if the card is missing, you can take action immediately.

Access control smart cards allow you to implement, in particular, functions such as access control, access to personal computer devices, access to programs, files and commands. In addition, it is also possible to carry out control functions, in particular, registration of attempts to violate access to resources, use of prohibited utilities, programs, DOS commands.

It is clearly not enough technical solutions (hardware or software) to organize reliable and safe operation of complex local networks. A single comprehensive plan is required, which includes both a list of daily security measures and urgent data recovery in case of system failures, as well as special action plans in emergency situations (fire, power outages, natural disasters). Most financial institutions in Western countries have specially developed and constantly updated security plans.

List of sources used:

1. Warwick Ford Computer Communications Security. Principles, Standard Protocols and Techniques. PTR Prentice Hall, 1994, 500 p.

2. Regis J. Bates Physical protection. In Disaster Recovery for LANs, 1994, McGraw-Hill, Inc, pp. 44-65

Key words: software, hardware, unauthorized, administrator.

Ключевые слова: программное обеспечение, оборудование, несанкционированный, администратор.

Ключові слова: програмне забезпечення, обладнання, несанкціонований, адміністратор.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

ЗМІСТ

ДЛЯ НОТАТОК

Наукове видання

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ
ІІ Всеукраїнської науково-практичної конференції

20 листопада 2020 року

Верстка – Т.В. Мартиненко

Підписано до друку 01.12.2020 р. Формат 60х84/16.
Папір офсетний. Гарнітура Cambria. Цифровий друк.
Умовно-друк. арк. 14,18. Тираж 150. Замовлення № 1120-300.
Віддруковано з готового оригінал-макета.

Видавництво і друкарня – Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефони: +38 (0552) 39 95 80,
+38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 6424 від 04.10.2018 р.