НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«АНАЛІЗ СИСТЕМИ ЗАХИЩЕНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ МОБІЛЬНИХ ОПЕРАТОРІВ»

Виконав: здобувач 4 курсу

Рівень бакалавр

Галузь знань 12 «Інформаційні технології»

спеціальність 125 «Кібербезпека»

Хусід Натан Ілліч

Керівник: к.т.н., доцент

Ахмаметьєва Ганна Валеріївна

Рецензент: д.е.н., професор

Горбаченко Станіслав Анатолійович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Хусіду Натану Іллічу

1. Тема роботи: «Аналіз системи захищеного доступу до конфіденційних даних інформаційної системи мобільних операторів»
Керівник роботи: к.т.н, доцент Ахмаметьєва Ганна Валеріївна
затверджені наказом НУ ОЮА № 809-06 від «02» квітня 2024 року
2. Строк подання здобувачем роботи «20» травня 2024 року
3. Дата видачі завдання«15» вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Аналіз системи захищеного доступу до конфіденційних даних інформаційної системи мобільних операторів” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 8 рисунків, 22 літературних джерела за переліком посилань. Робота виконана на 35 сторінках загального тексту і 28 сторінках основного тексту.

Метою роботи є аналіз баз даних, якою володіє мобільний оператор, ризики, які можуть порушити роботу оператора та можуть зашкодити користувачам, та заходи і рішення щодо забезпечення безпеки мобільним оператором і користувачем.

Проведено аналіз баз даних, який має у себе мобільний оператор. Проведено аналіз ризиків, які можуть порушити роботу оператора та можуть зашкодити користувачам, за властивостями інформації. Проведено аналіз заходів та рішень щодо забезпечення безпеки мобільним оператором та користувачем.

Результати роботи можуть бути використані при розробці системи захищеного доступу до конфіденційних даних інформаційної системи мобільним оператором.

Можливими напрямками подальших досліджень є розробка нових заходів або рішень щодо забезпечення захисту.

АНАЛІЗ, ЗАХИСТ, ДОСТУП, ІНФОРМАЦІЙНА СИСТЕМА, БАЗА ДАНИХ, РИЗИКИ, ЗАХОДИ, РІШЕННЯ.

ABSTRACT

Qualification work on the topic "Analysis of the system of secure access to confidential data of the information system of mobile operators" for the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 8 figures, 22 literature sources in the list of references. The work is completed on 35 pages of the general text and 28 pages of the main text.

The purpose of the work is to analysis the databases owned by the mobile operator, the risks that may disrupt the operator's operations and may harm users, and the measures and solutions to ensure security by the mobile operator and the user.

The article analyses the databases owned by a mobile operator. The risks that may disrupt the operator's work and may harm users are analyzed by the properties of information. The analysis of measures and solutions to ensure security by the mobile operator and the user is carried out.

The results of the work can be used to develop a system of secure access to confidential data of the information system by a mobile operator.

Possible areas for further research include the development of new security measures or solutions.

ANALYSIS. PROTECTION, ACCESS. INFORMATION SYSTEM. DATABASE, RISKS, MEASURES. SOLUTIONS.

ЗМІСТ

ВСТУП

На теперішній час таке явище, як мобільний оператор, став частиною нашого життя. Завдяки мобільним операторам, люди можуть подзвонити один одному з різних причин через свої смартфони, дивитися у будь-яких соціальних мережах, проводити будь-які конференції через функцію «мобільний Інтернет». Ще з появою мобільних операторів з'явився і такий термін, як call-центр — це бізнес-відділ або самостійна компанія, яка відповідає за обробку вхідних та вихідних дзвінків між компанією та клієнтами [1].

Але є такі ситуації, що руйнують, збивають або припиняють роботу мобільного оператора. Явним та ясним прикладом є кібератака на мобільного оператора «Київстар», яка була здійснена та за якою відповідальність несуть декілька хакерських російських угрупувань.

Мета цієї роботи є аналіз баз даних, якою володіє мобільний оператор, ризики, які можуть порушити роботу оператора, та заходи і рішення щодо забезпечення безпеки мобільним оператором.

Задачами роботи є:

1) аналіз баз даних, якими володіє мобільний оператор, та персональні дані, які підлягають захисту,

2) аналіз ризиків, які можуть порушити роботу мобільного оператора та можуть зашкодити користувачам,

3) аналіз заходів та рішень щодо забезпечення безпеки мобільним оператором та користувачем,

4) формулювання рекомендацій щодо підвищення рівня захисту конфіденційної інформації мобільним оператором.

Об'єктом роботи є сам мобільний оператор та предмет роботи – процес захисту інформації оператора, його бази даних, модель ризиків та рішення і стандарти.

1 АНАЛІЗ ІНФОРМАЦІЇ МОБІЛЬНИХ ОПЕРАТОРІВ, ЩО ПІДЛЯГАЄ ЗАХИСТУ

У кожній компанії або сервісного центру є декілька блоків інформації щодо баз даних. В цьому розділі буде розглянуто три блоки інформації, які мають мобільні оператори: власна інформація самого оператора; персональні дані користувачів; дзвінки та передача даних. Усе детальніше буде розглянуто нижче.

1.1 Власна інформація мобільного оператора

Першим блоком інформації, яка є у мобільного оператора та яка буде розглянута тут, це власна інформація мобільного оператора. Ця інформація поділяється на дві групи: інформація, що стосується до самого оператора, та міжоператорська інформація. Спочатку треба оголосити, які дані можуть бути власною інформацією оператора: бази даних про співробітників, технічна база даних, фінансова база даних, дані про міжоператорських дзвінках та повідомлень, дані про договори та угоди, дані про статистику, дані про відліки та логи. На рисунку 1.1 наведена структура власної інформації мобільного оператора, що підлягає захисту.

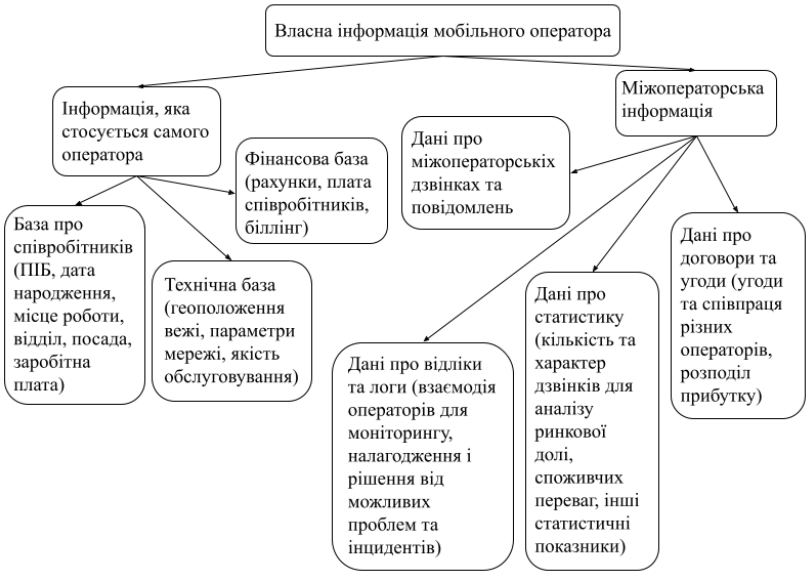

Рисунок 1.1 – Схематичний вигляд власної інформації мобільного оператора

Аналіз починається з бази даних про співробітників. Без співробітників, тобто людського ресурсу, який є одним із важливих стовпів, немає і компанії, і корпорації та інших формувань. Ця база даних є інформацією, що стосується до самого оператора. До неї входить вся інформація, яка пов’язана зі співробітниками, а саме: прізвище ім’я по-батькові співробітника, дата народження, місце роботи (тобто місто та вулиця проживання й вулиця, де працює), відділ, в якому працює, посада та заробітна плата.

Наступна база даних це технічна база. Вона теж є інформацією, яка стосується до самого оператора, та взаємопов’язана з останнім блоком інформації, яка є у мобільного оператора та яка буде розглянута нижче в цьому розділі. До неї входить: географічне положення вежі стільникового зв’язку та інші обладнання, їх стан, параметри мережі та якість обслуговування. В останніх двох пунктів є уточнювальна інформація: у параметрах мережі такою уточнювальною інформацією є пропускна здатність та швидкість передачі; у якості обслуговування – затримки, втрата пакетів інформації та рівень сигналу. Щодо того, що ця база пов’язана з останнім блоком зумовлена таким чином, що вісь блок повністю залежить від вишок зв’язку і технічного обладнання та їх якістю, тобто якщо щось не так з вежею зв’язку – зв’язка як засобу спілкування немає, а якісь бізнесмени запланували дзвінок і таким чином усе даремно.

Далі є фінансова база. Вона теж є інформацією, яка стосується оператора, та другим важливим стовпом для будь-яких формувань. До неї входить інформація такого характеру, як: рахунки, плата співробітникам та біллінг. Біллінг з англійської мови перекладається як виставлення рахунків. У кожного є два параметра, який показує працездатність оператора: в частині «рахунок» такими параметрами є баланс на рахунку користувача або абонента та історія транзакцій (фінансових операцій); в «платі співробітникам» - сума, яку заробив працівник, та була ця сума йому сплачена; в «біллінгу» - дані про виставлені рахунки та сума платежів від абонента. Саме цей рядок є дуже пов’язаним з базою з історією використання послуг, який буде розглянутим нижче.

Наступною базою є дані про міжоператорські дзвінки та повідомлення. Ця база є першою з другої групи щодо власної інформації оператора – міжоператорської. Вона повністю залежна з останнім блоком інформації, яка буде розглянута нижче, тому що ця база даних має теж саму інформацію, як і весь третій блок, але з уточненнями.

Наступною до аналізу базою це дані про договори та угоди. Вона теж відноситься до міжоператорської інформації. В неї є інформація такого характеру, як: угоди та співпраця різних операторів та розподіл прибутку. Ця база даних може допомогти для укладення нових договорів з різними операторами, щоб оператор, з подачею якої цей договір був укладеним, мав шансі на більших прибуток з цього договору.

Далі з групи щодо міжоператорської інформації – дані про статистику. В ньому уточняється інформація щодо кількості та характеру дзвінків для аналізу ринкової долі, споживчих переваг та інших статистичних показників.

Останньою базою, яка є власною інформацією мобільного оператора, це база даних про відліки та логи. Логи з англійської мови перекладаються як файл журналу, тобто це текстові файли, куди автоматично записуються всі події, що відбувалися у комп’ютерній системі 2]. В ній є інформація, яка розповідає про: взаємодію операторів для моніторингу та налагодження і рішення від можливих проблем та інцидентів. Можливо, завдяки таким чином компанія «Київстар» змогла швидко відновити свою роботу в системі.

1.2 Персональні дані користувачів

Другим блоком інформації, яка є у мобільного оператора, це персональні дані користувача або абонента. Треба оголосити, які є дані, що належать до цього блоку інформації, а саме: база про абонента, база з контактною інформацією, база з історією користування послугами, бази зі згодами та вподобання і база зі зверненнями та скаргами. На рисунку 1.2 наведена структура персональної інформації користувача, що теж підлягає захисту.

Рисунок 1.2 - Схематичний вигляд персональних даних абонента

Аналіз даного блоку починається з базою даних, яка оголошена та буде проаналізована, є база про абонентів. Вона є третім стовпом будь-якої компанії, без якої не було б того, що людство має зараз. В цієї бази даних мається така інформація, як: прізвище ім’я по-батькові абонента, дата народження та місце проживання.

Наступним на черзі є база з контактною інформацією. Вона містить в собі таку інформацію, як: виданий абоненту номер телефона; номер телефонів, через які можна подзвонити на випадок можливих проблем або добрих новин, наприклад привітати абонента з днем народженням; фізична або поштова адреса та електронна адреса, завдяки яким абонент може зареєструватися у даного чи іншого мобільного оператора.

Далі на аналіз це база з історією користування послугами. В цій базі даних є інформація, яка всім відома, тобто: тарифний план абонента, додаткові послуги, зміни та історія платежів. Ця база взаємодіє з фінансовою базою через рядок «біллінг», як було обговорено вище.

Наступною на розгляд базою це база зі згодами та уподобаннями. Там описується такий момент, як згода абонента на обробку персональних даних, на

отримання маркетингових комунікацій, а також вподобання абонента відносно використання його даних.

Останньою на розгляд базою є база зі зверненнями та скаргами. Там зберігається інформація, яка пов’язана з записами про запити на обслуговування та скарги на якісь несправності, включаючи текстові описи проблем та результати їх рішення.

1.3 Дзвінки та передача даних

Третім і останнім блоком інформації, який має при собі мобільний оператор, це дзвінки та передача даних. Це важливий блок інформації для будь-якого мобільного оператора. Зараз буде оголошено, які є дані, що належать до цього блоку: база про дзвінки, база про повідомлення та база про мобільний інтернет. Цей блок є повністю залежним до технічної бази даних, що у власної інформації оператора, як це оголошено вище. Що до даних про міжоператорські дзвінки та повідомлення, які були розглянуті вище, то ці дві типу даних, по суті, однакові. Тільки треба уточнити, що вся інформація про міжоператорські операції були оброблені мінімум двома операторами. На рисунку 1.3 наведена структура цього блоку, який потребує захисту.

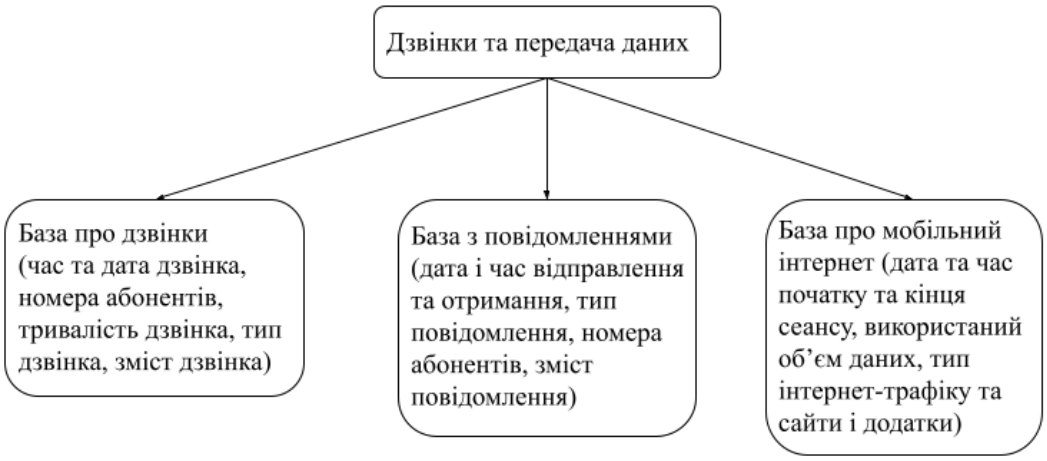

Рисунок 1.3 – Схематичний вигляд «дзвінків та передачі даних»

Аналіз блоку починається з бази про дзвінки. В ньому розглядають інформацію такого типу, як: час та дата дзвінка, номера абонентів, тривалість і тип дзвінка та зміст дзвінка. У «часі та даті» розглядається точний час у годинах, хвилинах, секундах та міллісекундах початку та закінчення дзвінка та його дата в такому параметрі, як число, місяць та рік, або дати, якщо дзвінок було розпочато наприкінці одного дня, а завершився на початку наступного дня. В «номерах абонентів» розглядають вихідний та вхідний номера абонентів, які брали участь у дзвінку. У «тривалості» основним параметром є хвилини та секунди, в яких вимірюють тривалість дзвінка. В «типу дзвінка» розглядають такі параметри, як: вихідний, вхідний або пропущений дзвінок. Тобто вихідний дзвінок описує абонента, який дзвонить комусь; вхідний дзвінок описує, чи прийняв абонент, якому дзвонять та пропущений дзвінок описує, що абонент, до якому дзвонять, не прийняв дзвінок. В «змісту дзвінка» зберігають сам дзвінок в текстовому форматі.

Наступною на черзі це база з повідомленнями. В ньому є інформація таких параметрів, як: дата і час відправлення та отримання, тип повідомлення, номера абонентів, зміст повідомлення. В параметрі «дата і час відправлення та отримання» розглядають точний час в годині, хвилині, секундах та міллісекундах та дату з числом, місяцем та роком відправлення повідомлення та отримання. В параметрі «тип повідомлення» розглядаються дві основні типи повідомлень: SMS та MMS. SMS з англійського перекладається як «служба коротких повідомлень». Довжина SMS-повідомлення складає 160 символів в латиниці [3]. Також є його розширена версія – EMS, що перекладається як «покращена служба повідомлень», який не використовується. MMS з той ж англійської мови перекладається як «служба мультимедійних повідомлень». Такий тип повідомлень дозволяє легко створити мультимедійне повідомлення, зробивши знімок за допомогою камери телефону або використовуючи зображення та звуки, збережені раніше у телефоні [4].

Останньою базою, яка буде розглянутою, це база про мобільний інтернет. В ньому розглядають інформацію такого типу, як: дата та час початку та кінця сеансу, використаний об’єм даних, тип інтернет-трафіку та сайти і додатки. В частині «дата та час початку та кінця сеансу», як і попередніх базах, теж описують дату у вигляді

число, місяць та рік і час у вигляді годин, хвилин, секунд та міллісекунди за той період часу, коли абонент користувався мобільним інтернетом. Наступна частина, «використаний об’єм даних», записується в базі в мега- або гігабайтах. В третій частині, «тип інтернет-трафіку», заповнюється ті запити, які були зроблені абонентом: перегляд веб-сторінки, відправлення або отримання електронної пошти, використання мобільних додатків, використання для мобільної гри та багато чогось. В останній частини, «сайти та додатки», зберігається інформація про відвіданих сайтах або використаних додатків, але це залежить від рівня деталізації даних.

В цьому розділі було проведено аналіз баз даних, які мають мобільні оператори. В наступному розділі буде проведено аналіз ризиків, які впливають на незахищеність системи у мобільного оператора.

2 АНАЛІЗ РИЗИКІВ, ЩО ВПЛИВАЮТЬ НА НЕЗАХИЩЕННІСТЬ СИСТЕМИ МОБІЛЬНОГО ЗВ’ЯКЗУ

Для того, щоб розглядувати, які ризики можуть бути, треба оголосити властивості інформації. Для характеристики основних властивостей інформації як об'єкту захисту часто використовується модель CIA, реалізація якої забезпечує в рамках НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»:

1. Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем.

2. Цілісність – означає неможливість модифікації неавторизованим користувачем.

3. Доступність – властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час [5].

Тепер можна перейти до аналізу ризиків, основуючи на цих властивостях.

2.1 Ризики відносно власної інформації оператора

Почнемо з ризиків відносно власної інформації та одразу з технічної бази, а саме з вішок зв’язку та її обладнання. Ризики щодо цих речей може бути від звичайної крадіжки важливого обладнання до пошкодження або псування вежі або обладнання. Ці ризики ніяк не відносяться до властивостей інформації. Тепер переходимо з уточнень на загальну інформацію.

Першим із властивостей, який буде розглянутим та проаналізованим, є «конфіденційність». Ризики, які можуть порушити цю властивість, це:

1. Хакерські атаки;
2. Недостатній захист інформації;
3. Витоки;
4. Зливи;

5. Віруси, які руйнують конфіденційність;
6. Шпигунство від компаній-конкурентів.

Цей невеликий перелік є одним з прикладів з множини ризиків, які можуть порушити конфіденційність. Перші дві позиції з переліченого будуть декілька раз повторюватися в цьому підрозділі. Тепер буде проведено аналіз кожного ризика.

Аналіз починається з хакерських атак. Для аналізу такого ризику треба з'ясувати, що таке ці атаки. Отож, хакерська атака (вона ж кібератака) — спрямовані дії в кіберпросторі з утручанням у роботу інформаційно-комунікаційних систем з метою порушення конфіденційності, цілісності, доступності, авторства інформації; або контролю, зміни в роботі, вимкнення, знищення обчислювальних механізмів чи інфраструктури [6]. Тобто, ці атаки можуть порушити не тільки конфіденційність інформації, а також її цілісність та доступність.

Як цей ризик відбувається в даному блоку та у властивості «конфіденційність»? Хакер може поширити для всій спільноті всю інформацію, яку має мобільний оператор у себе, а там: вся інформація про співробітників: координати вішок і обладнання та їх стан; різні угоди з іншими операторами; рахунки оператора, тощо. Щодо того, як це реалізовується з іншими блоками, буде інформація нижче.

Наступним на аналіз ризик – недостатній захист інформації. Цей ризик реалізується через то, що спеціалісти не дослідили, або щось не було при їх присутності, або було навмисно не дослідженим. Через цей ризик може відбутися і раніше згадані атаки, і далі описані ризики.

Далі ризик, який є в цьому переліку, це витоки. Витоки бувають технічними каналами та від людського фактора, тобто співробітник забув чи навмисно так зробив утилізувати якісь предмет згідно з нормативними актами та організаційними заходами, а якісь недобросовісна людина забере собі та може продати цей предмет або шантажувати компанію. Витоки через технічні канали відбуваються через те, що деяка людина може дізнатися через деякі технічні засоби, наприклад через радіохвилі, лазери, прослуховуючі апарати та інші засоби,

щоб зняти, прослухати та іншими способами дізнатися про конфіденційну інформацію.

Наступний ризик, який зараз буде розглянутим, це зливи. Зливи реалізуються через співробітника, який має «ключ» та який потенційно може скопіювати або якимось іншим способом зробити, щоб службова інформація в підсумку змогли розглядати несанкціоновані особи, які не мають права оглядати.

Далі ризик, який може витікати з першого пункту даного переліку, це віруси, які руйнують конфіденційність, або віруси-шпигуни. На деяких сайтах цей вірус може називатися як шпигунське програмне забезпечення. Воно записує всі дії, місцезнаходження, IP-адресу тощо [7]. Цей вірус ніяк не помічається без антивірусних засобів, про яких буде йти річь значно нижче. Воно також може бути прихованим в нормальній програмі. Вся інформація, яка була потрібна та повністю викрадена, шпигунське програмне забезпечення може самоліквідуватися завдяки хакерам, які його і «вбудували».

Останній ризик, який буде розглянутим тут, це шпигуни від компаній-конкурентів. Тут просто: шпигун може прикриватися законослухняним співробітником у відділі кібербезпеки, а через деякий час він чи вона звільняється. Потім начальник відділу дізнається, що ця людина була шпигуном для компанії-конкурента. Шпигун пересилав всю конфіденційну інформацію конкуренту для знищення компанії, в якої й працював.

Другим із властивостей, який є таким, це «цілісність». Ризики, які руйнують цю властивість, є:

1. Хакерські атаки;
2. Недостатній захист інформації;
3. Віруси-шифрувальники;
4. Віруси, які можуть знищити інформацію.

Цей перелік є одним з множини ризиків, які можуть порушити цілісність інформації. Тепер кожний пункт буде проаналізованим.

Про хакерські атаки було вище обговорювано. Щодо того, як ця атака може реалізуватися у властивості «цілісність», то там хакер модифікує або знищує весь блок, який має мобільний оператор.

У недостатньому захисту може відбутися така ситуація, що деякий абонент може змінити рядок «біллінг» щодо себе та записати, що його тариф проплачений на мільйони гривень, або співробітник може змінити в рядку «рахунок» та збільшити свою плату таким чином, що компанія зобов'язана платити до смерті цього співробітника.

Наступним ризиком, який буде розглянутим в секції «цілісність», це віруси-шифрувальники. Цим вірусом хакер може зашифрувати весь блок таким чином, що оператору простіше закритися або дати викуп, чим відновлювати весь блок самостійно.

Останній ризик, який буде розглянутим, це ті віруси, які можуть знищити інформацію. Цей ризик реалізується таким чином, що після хакерської атаки деяка інформація може бути знищеною.

Третьою властивістю, яка буде розглянутою та проаналізованою, це «доступність». Ризики, які можуть порушити цю властивість, є:

1. Хакерські атаки;
2. Недостатній захист інформації;
3. Віруси-блокувальники.

Через хакерські атаки доступ до власної інформації мобільний оператор працює не нормально, тобто може бути заблокованим або доступ мають ті, які раніше цього «доступу» не мають права через нормативні акти та організаційні заходи.

Через недостатній захист співробітник може заблокувати через свої пристрої та зробити що-небудь з тою інформацією, яку заблокував. А через віруси-блокувальники доступ до інформації блокується на деякий час, через яку деяка людина може робити що завгодно. На рисунку 2.1 зображено перелік ризиків, які погрожують власної інформації оператора.

Рисунок 2.1 – Перелік ризиків, які погрожують власної інформації оператора

В наступному підрозділі будуть розглянуті ризики, які можуть порушити безпеку у абонента.

2.2 Ризики відносно персональних даних користувачів

Другим на черзі блоком, який має свою сукупність ризиків за всіма властивостями, буде персональні дані користувачів/абонентів. Про хакерські атаки будуть загальні моменти щодо їх реалізації до кожної властивості в цьому блоку.

Перелік ризиків, які можуть руйнувати конфіденційність користувача, це:

1. Фішинг;
2. Телефонне шахрайство;
3. Віруси.

Аналіз даного блоку починається з ризику під назвою фішинг. Фішинг – це вид інтернет-шахрайства, який полягає в крадіжці конфіденційних даних користувачів [8]. Цей ризик частіше виявляється через електронну пошту та дуже маленький відсоток (до п’яти відсотків) здійснюється через шкідливі сайти та через телефон. Тут розглядається останній метод фішингу, решта методів буде розглянута в останньому підрозділу.

Як цей ризик реалізується в даному блоку? Користувачеві насилають повідомлення за типом: «У вас недостатньо коштів на рахунку. Щоб далі розмовляти по телефону, поповніть тариф за цим посиланням». Абонент тисне на посилання та він став жертвою шахраїв через те, що цей абонент вписав своє ім’я, прізвище, номер телефону та номер своєї банківської картки, що є важливим, тому що це є ціллю шахраїв.

Наступним на аналіз буде телефонне шахрайство. Той самий принцип дії, але метод цього шахрайства інший: ці шахраї активно користуються самим номером телефона абонента та роблять через телефон.

Останній ризик, який буде розглянутим в секції «конфіденційність», це будь-які віруси, які руйнують цю властивість. Через них будь-хто може викачати всю персональну інформацію користувача та робити з краденою інформацією будь-що.

Тепер зараз буде оголошено перелік ризиків, які руйнують цілісність персональні дані користувача. До цього переліку входять:

1. Віруси-шифрувальники;
2. Віруси, які можуть знищити інформацію.

Принцип використовування цих вірусів такий самий, як і у ризиків відносно власної інформації: перший тип вірусів можуть зашифрувати так інформацію у мобільного оператора, що буде дуже складно відновлювати; другий тип – знищити усю інформацію.

Перелік ризиків, які можуть руйнувати доступність, представлено одним ризиком: віруси-блокувальники. Як було написано вище, ці віруси можуть заблокувати доступ до інформації, яка мається у мобільного оператора щодо персональних даних користувачів. На рисунку 2.2 зображено перелік ризиків, які погрожують персональним даним користувача.

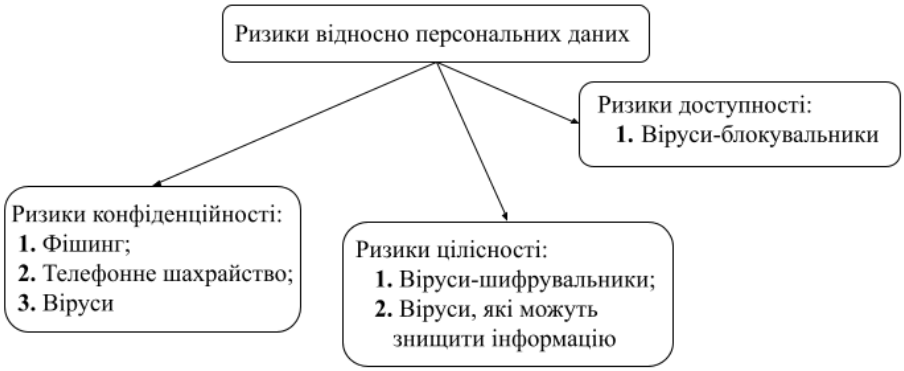

Рисунок 2.2 – Перелік ризиків, які погрожують персональним даним користувача

Всі ці ризики поєднаються одною причиною – хакерська атака на мобільного оператора. Усі ці віруси, фішинги та телефонні шахраї знають номер телефону, яку має абонент, через те, що вони зробили хакерську атаку на мобільного оператора та поширили цю інформацію якісь шахраям або іншим хакерам.

2.3 Ризики відносно дзвінків та передачі даних

Останній блок, який буде розглянутим та проаналізованим, це дзвінки та передача даних. Вище було написано, що пошкодження або псування вішок ніяк не відноситься до властивостей інформації. Там була здійснено помилка: третій блок інформації, який має оператор, дуже залежне від таких нанесених збитків. Через такі збитки погіршується якість зв’язку та є ризики, що правопорушники могли прикріпити на цих вежах.

Отже, тут знову будуть три частини, який розглядає ризики однієї властивості. Першим переліком ризиків, який буде розглянутим та які ризики можуть порушити в цьому блоку, це перелік ризиків конфіденційності, в якій є:

1. Прослуховування та запис дзвінка;
2. Зняття трафіку;
3. Фішинг.

Почати аналіз треба з фішингу, який був згаданим у попередньому підрозділу. Фішинг може реалізовуватися через спам-повідомлення на електронну пошту та через шкідливий сайт. У спам-повідомленнях можуть бути текст такого

плану, що необхідно відправити відповідного листа або зареєструватися на фішинговову сайті, через яку шахраї дізнаються про номер телефону та номер банківської картки.

Наступним ризиком на аналіз буде прослуховування дзвінка. Через якісь додатки, як «Wireshark», можна прослухати дзвінок та дізнатися, про що говорили два абонента. Це може бути і приватний дзвінок, і бізнес-дзвінок тощо. Та особа, яка здійснює прослуховування та записує цей дзвінок на свої носії, може через деякий час скомпрометувати одного з абонентів.

Останній ризик, який є в невеликому переліку, це зняття трафіку. Принцип реалізації такого ризику дуже схожа з попереднім ризиком. В тому же додатку, через якого можна прослухати дзвінок, можна також зняти трафік, тобто цей додаток є одним з основних додатків, через якого можна реалізувати обидва ризика одразу.

Наступний ризик, який треба проаналізувати та який може порушити цілісність дзвінка або передачі даних, перебій зв’язку. На короткий час перебій не є ризиком, рішення від якого треба шукати будь-якими способами, але через те, що немає довгого часу електроенергії, яка підживлює вежі зв’язку, або під час війни, якщо армія ворога знищила точки електроживлення, цей ризик стає великою проблемою.

Останній перелік ризиків, які порушують доступність, це:

1. Втрата номеру;
2. Втрата паролю.

Втрата номеру реалізується, якщо телефон абонент вкрали або пограбували правопорушники та сам абонент не може згадати номер. Втрата паролю реалізується, якщо абонент забув чи втратив пароль для активації номера.

Більша частина ризиків, які були проаналізовані в цьому розділі, можуть порушувати або всі властивості інформації, або тільки конфіденційність, або тільки цілісність. Щодо ризиків, які порушують доступність інформації, то вони не є основними проблемами. На рисунку 2.3 зображено перелік ризиків, які погрожують блоку з дзвінками та передачі даних.

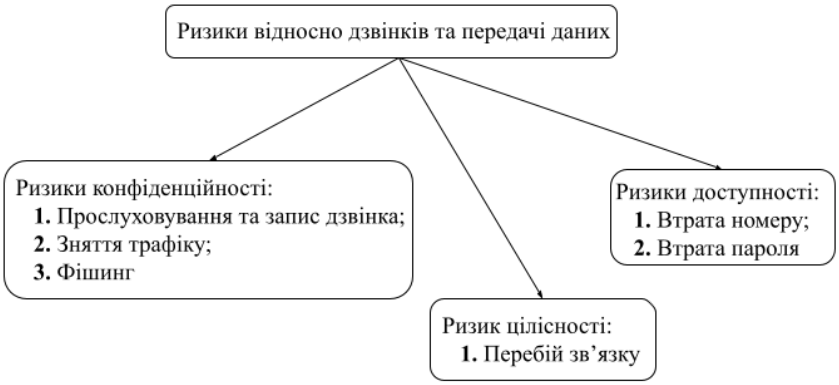

Рисунок 2.3 - Перелік ризиків, які погрожують блоку з дзвінками та передачі даних.

В наступному розділі буде проведено аналіз заходів та рішень, які можуть забезпечити безпеку з боку мобільного оператора та з боку абонента.

3 ЗАХОДИ ТА РІШЕННЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ МОБІЛЬНОГО ЗВЯ'ЗКУ

В цьому розділі будуть розглянуті будь-які стандарти, заходи та рішення для забезпечення безпеки інформації, яку повинен мати мобільний оператор. Наприклад, оператор lifecell відповідає сучасним світовим та національним стандартам безпеки інформації ISO 9000, а також галузевим стандартам захисту як PCI DSS та SOX ITGC [9].

3.1 Реалізація захисту інформації мобільним оператором

Один із стандартів, які є на сьогоднішній день, це ISO 9000. ISO 9000 – мінімальний рівень якості, що дозволяє вийти на світовий ринок. Цей стандарт не гарантує, що товар або послуга буде високої якості, але відповідає мінімально допустимим нормам стандарту [10].

Згідно цього стандарту, під «якістю» визначається здатність задовольняти замовників, а також передбаченим і непередбаченим впливом на відповідні зацікавлені сторони. Також в ньому описується для адекватної роботи в підприємстві система управління якістю (далі СУЯ). СУЯ охоплює дії, за допомогою яких організація ідентифікує свої цілі та визначає процеси й ресурси, які потрібні для досягнення бажаних результатів; керує взаємодійними процесами та ресурсами, які потрібні, щоб створити цінності та здобути результати для відповідних зацікавлених сторін; дає змогу найвищому керівництву оптимізувати використання ресурсів, ураховуючи короткострокові та довгострокові наслідки рішень; забезпечує засоби ідентифікування дій щодо вирішування передбачених і непередбачених наслідків у наданні послуг.

Для підтримання СУЯ з боку найвищого керівництва та задіяність персоналу дають змогу:

- Забезпечувати адекватні людські та інші ресурси;
- Здійснювати моніторинг процесів і результатів;

- Визначати та оцінювати ризики та можливості;
- Запроваджувати відповідні дії [11].

Для дотримання вимог цього стандарту створений ще один стандарт, як ДСТУ ISO 9001 2015 року видання. В тому документі основні терміни посилаються на ДСТУ ISO 9000:2015, тобто в ISO 9000 розглядають терміни та дії, які мають бути дотриманні, ISO 9001 розглядають будь-які вимоги щодо виконання необхідних дій, які перечисленні у попереднього стандарту.

Наступний стандарт, який користується lifecell – це PCI DSS. Воно читається, як Стандарт безпеки даних індустрії платіжних карток або на англійській мові Payment Card Industry Data Security Standard. Це комплексний стандарт безпеки, що включає вимоги до управління безпекою, правил, процедур, мережевої архітектури, розробки програмного забезпечення та інших критично важливих заходів захисту [12].

Описати всі критерії перевірки буде складно – їх 288. Саме процедура досить тривала, тому що торкається перевірки ряду складних технічних моментів. Повністю список критеріїв, розбитий на 12 груп, має такий вигляд:

- Захист обчислюваної мережі;
- Налаштування компонентів інформаційної інфраструктури;
- Захист збережених даних про власників карток;
- Захист переданих даних про власників карток;
- Антивірусний захист інформаційної інфраструктури;
- Розробка та підтримка інформаційних систем;
- Керування доступом до даних про власників карток;
- Механізми автентифікації;
- Фізичний захист інформаційної інфраструктури;
- Протоколювання подій та дій;
- Контроль захищеності інформаційної інфраструктури;
- Управління інформаційною безпекою.

Під словом «перевірка» розуміється буквальна присутність того, хто виконує цю перевірку, в офісі оператора, якого перевіряють. Аудит безпеки виконується двічі. Вперше використовується автоматичний сканер на відомі уразливості, який надає сертифікована організація ASV, тобто «Затверджений постачальник послуг сканування». У разі успішного проходження цього тесту система перевіряється на безпеку вдруге експертами вручну, з винесенням офіційного висновку [13].

Ще одним галузевим стандартом є Закон Сарбенса-Окслі з Загальними засобами контролю за інформаційними технологіями, або SOX ITGC. Перша частина цього стандарту, тобто Закон Сарбенса-Окслі, також відома як «Закон про реформу бухгалтерського обліку державних компаній та захист інвесторів» або «Закон про корпоративну та аудиторську звітність і відповідальність».

Цей закон впливає на те, як компанії реєструють, контролюють і передають інформацію про свої фінансові операції, а керівників та керівництво несе відповідальність за точність їх фінансових звітів. Для того, щоб забезпечити дотримання правил Закону, внутрішні аудитори повинні регулярно проводити перевірки відповідності [14].

Загальні засоби контролю за інформаційними технологіями – це основні засоби контролю, які необхідні для ефективного функціонування ІТ-операцій та безпеки ІТ-систем. Ці засоби є важливими для всіх організацій, які використовують ІТ-системи, і їх необхідно впроваджувати для забезпечення надійності та точності фінансової звітності, дотримання нормативних вимог та захисту конфіденційних даних [15].

Аудит Закону з Загальними засобами контролю має на меті визначити, чи достатньо Загальних засобів, щоб гарантувати точність, повноту та безпомилкову роботу системи фінансової звітності. Ці засоби внутрішнього контролю є способами виявлення та припинення помилок у бізнес-процесах, які можуть вплинути на цілісність або точність фінансових звітів [14].

Цей стандарт потрібен для того, щоб керувати доступом та виправленнями, управляти змінами та робити резервні копії даних [14]. Для впровадження цього стандарту потрібно зануритися в структуру, яка складається з п’яти етапів:

1. Створення середовища контролю. Спочатку треба дізнатися, що таке саме середовище контролю. Середовище контролю – умови, дисципліна, відповідний порядок, які створені власником або керівником для забезпечення всім без винятку рівних можливостей з виконання функцій контролю у відповідності до встановлених положеннями чи інструкціями обов'язками [16].
2. Проведення оцінки ризиків Загальних засобів контролю. Традиційний підхід до управління ризиками в основному зосереджується на потенційних фінансових ризиках. Однак нещодавно фокус управління ризиками підприємства перетворився на стандарт оцінки ризиків, який враховує все, що потенційно впливає на організацію.
3. Здійснення контрольної діяльності. Результатом оцінки ризиків Загальним засобам має стати ретельна структура для впровадження на практиці сурових стандартів, які не залишають нічого на волю випадку. У рамках заходів із контролю, спрямованих на те, щоб залишити тільки чіткий контрольний слід прозорості та підзвітності, усі витрати на проект у компанії чи організації мають підтверджуватися чітким формулюванням мети та цілей.
4. Впровадження інформаційно-комунікаційних систем. Правила Загальних засобів щодо відповідності вимогам Закону Сарбенса-Окслі мають сформуватися до цього етапу. Виходячи із сукупності всіх факторів дуже важливо, щоб Загальні засоби підтримувалися надалі, забезпечуючи підтримку високоякісних даних і розповсюдження ефективного зв'язку, що гарантувати, що стандарти залишатимуться високими та добре підтримуватися.
5. Моніторинг елементів керування Загальними засобами. Цей стандарт потребує постійного моніторингу в підприємствах, в тому числі у мобільного оператора [17].

На рисунку 3.1 зображено схематичний вигляд всіх заходів та рішень, які були оголошені вище та активно використовуються мобільним оператором. Також на рисунку будуть деякі рішення, які будуть оголошені нижче.

Рисунок 3.1 – Схематичний вигляд заходів та рішень, які займається мобільним оператором

Також треба пам’ятати про систему контролю та управління доступом. Ця система має два види: фізична та програмна. Фізична система полягає в тому, що деяким співробітникам дається особовий ключ, за яким той чи інший співробітник доходить до свого робочого місця. Програмна система тим часом полягає в тому, що системний адміністратор дає доступ до інформаційної системи оператора та виконувати якісь дії. Це допоможе мобільному оператору для протидії уникнення витоку інформації з баз даних й інших документів, які є комерційною тайною оператора, та випадкових подій з тим, що співробітник нижчого рангу зайшов до системи, яка є таємною для нього.

Ще є такі стандарти та рекомендації, як ISO/IEC 27005, IEC/ISO 31010, NIST SP 800-39, NIST SP 800-37, NIST SP 800-30 та NIST SP 800-137. Вони є стандартами та рекомендаціями з управління ризиками та є важливими у будь-якому підприємстві.

3.2 Реалізація захисту інформації користувачем

Як абоненти можуть забезпечити безпеку свого номеру на телефоні? Для абонентів є декілька типів порад, які можуть допомогти забезпечити безпеку номеру. На рисунку 3.2 зображено схематичний вигляд, як користувач може реалізувати захист інформації.

Рисунок 3.2 – Схематичний вигляд, як користувач може реалізувати захист інформації

Один із типів порад пов’язана із SIM-картою. Ось невеликий перелік:

1. Заборонити або обмежити можливість віддаленої заміни SIM-карти у мобільного оператора. Це може усунути те, що шахраї можуть скористатися віддаленою заміною SIM-карти для своїй цілей.
2. Зареєструвати номер у оператора за паспортом. Будь-які процедури із SIM-картою можна буде виконувати лише після підтвердження особи за допомогою паспорта.
3. Дбати про безпеку фінансового номеру. Тобто це означає як можна менше викладати його у відкритий доступ в Інтернеті, використовувати для онлайн-шопінгу та не повідомляйте незнайомцям [18].

Наступний тип порад саме про безпеку, тобто:

1. Установити паролі на телефон. Установка пароля для розблокування є першим, що захищає дані на телефоні потраплянні в чужі руки. Для

доступу до інформації потрібно розблокувати екран. На це дається до десяти спроб: зловмисники витрачають всі спроби – телефон буде заблокованим. Вони можуть знести до заводських налаштувань, але це їм не потрібно, бо в чистому телефоні не має ніяких даних. Всього є п’ять способів заблокувати номер:

a. Через PIN-код, в якому вводяться будь-які чотири цифри;
b. Через звичайний пароль, який вводиться більше шести будь-яких цифр, букв та спеціальних символів;
c. Через графічний ключ, де є дев’ять точок та мінімальна кількість якою є чотири потрібно з’єднати, щоб ствердити такий пароль;
d. Через відбиток пальця, з якого спеціальний сенсор сканує будь-який палець користувача та для того, щоб розблокувати телефон або що-небудь ще, потрібно тільки прикласти палець до місця сканування;
e. Через сканування особи, завдяки якому пристрій розблокується через фронтальну камеру.

2. Налаштувати двофакторну авторизацію на сервісах. Користувач після введення основного пароля повинен в такому випадку ввести додатковий пароль. Також двофакторна авторизація стосується на додатки, які люди використовують. Завдяки такої функції, шахраям буде складніше зламати телефон з даними. Звичайно, реалізація цієї функції приходить на:
    a. Електронну пошту в розділі «Повідомлення» або в якісь інших розділах.
    b. SMS-повідомленням або через месенджер на мобільний телефон, якщо номер є підключеним до сервісу.
    c. Повідомленням на інший пристрій, який є підключений до профілю користувача.
3. Створити резервні копії всіх даних на мобільному пристрої. Регулярне копіювання системи повинен стати корисною звичкою для користувача

телефону. Завдяки копіюванню даних, телефон можна буде відкотити до останнього копіювання, якщо пристрій буде зараженим яким-небудь вірусом. Крім цього, тільки через копіювання даних можна швидко перенести всю конфіденційну інформацію.

4. Завантажувати додатки тільки з офіційних джерел. Завантаження додатків зі сторонніх сайтів загрожує потраплянням будь-якого вірусу і подальшим хакерським спробам змінити що-небудь на телефоні.
5. Регулярно оновляти операційну систему телефона. Наявність оновлення для телефона це один з важливих кроків до безпеки даних та є критично важливих для збереження конфіденційності даних користувача. Хакери використовують уразливості системи для злому. Розробники таких систем випереджають їх, закриваючи діри в нові оновлення [19].

Останній тип порад є пов’язаним з сайтами та посиланнями:

1. Не переходити ні за якими сумнівними посиланнями. Ці посилання можуть бути фішинговим шахрайством, або хакери завантажують на пристрій будь-які віруси. Найгірша ситуація, яка може статися, це вербівка в будь-яку кампанію проти якоїсь країни.
2. Не завантажувати на телефон ніякі файли та/або зображення від незнайомих контактів. У цих файлах може бути будь-який зашифрований вірус.
3. Звертати увагу на електрону адресу сторінки. Посилання, які починаються на http:// можуть бути небезпечними. Безпечними сторінками вважаються ті сторінки, що мають протокол https://.
4. Не підключатися до безпарольних мереж Wi-Fi [3520]. Такі мережи легше зламати та користувачу потрібно вимкнути в телефоні функцію «Автопідключення до Wi-Fi».
5. Завантажити антивірусні програми. Вони допоможуть виявити, які є можливі віруси в пристрої користувача та які сайти є проблемними.

3.3 Рішення з забезпеченням безпечного зв’язку при дзвінках та передачі даних

Прослуховування можуть здійснювати лише мобільний оператор та державні органи. Цей процес виконуються завдяки посередника або заліза, через яких і здійснюється дзвінок. Якщо прослуховування проводиться кимось ще, крім вищеописаних юридичних осіб, то користувачу потрібно знати, як виявити та вимкнути незаконне прослуховування.

Для того, щоб хоча б виявити незаконне прослуховування, рекомендується знати їх види та ознаки. В світі є три варіанта прослуховування за інструментом використання: переадресація (номера злочинців приховані), доступ до мікрофонів (через шкідливі програми отримують доступ без запиту) та за допомогою спеціальних технічних засобів (потребує значних фінансових втрат, щоб виявити). Ознаки того, що телефон користувача на деякий час прослуховують: незвичайні звуки під час розмови, батарея нагрівається у вимкненому стані та самостійні вмикання та вимкнення.

Для того, щоб переадресації не було, користувачу не рекомендується давати свій телефон незнайомим людям. Зловмисник може встановити переадресацію за двадцять-тридцять секунд. Якщо користувач дав зловмисникам свій пристрій на час, потрібний для встановлення, то перший може використати спеціальні сервісні коди. Ці коди можуть дати інформацію на наявність переадресації і, якщо в кожному коді пишеться, що переадресація не відбувається, то користувач може користуватися телефоном без проблем. Якщо ситуація протилежна, то користувач може набрати комбінацію ##002#, щоб вимкнути всі переадресації. Набравши даний код, спочатку з’явиться спливаюче повідомлення «MMI-код запущено», а потім «Переадресація дзвінків: видалення виконано успішно».

Для перевірки доступу до мікрофонів можна зробити налаштування, де можна вручну заборонити доступ до «мікрофону». Також слід заборонити доступ до списку дзвінків та параметру «файли та медіа контент» [21].

Трафік, за яким користувач може подзвонити через інтернет, відвідати деякі сайти або прочитати листи в електронній пошті, в даному випадку є потоком інформації, що проходить через бездротові канали зв’язку та обладнання мобільних операторів. Завдяки цьому оператори можуть аналізувати інформацію, яка проходить через них, щодо кожного свого клієнта.

У оператора є свої алгоритми шифрування для забезпечення безпеки своїх абонентів. Це можуть бути симетричні та асиметричні алгоритми шифрування. Також у оператора може бути файли з хеш-шифрами, де зберігаються логіни та паролі користувачів.

Мобільні оператори у багатьох країнах світу зобов’язані передавати інформацію про своїх абонентів державі за запитом спеціальних служб або силових відомств, тобто мобільний оператор змушений передавати всю базу, в якому є вся інформація про мобільний інтернет [22].

ВИСНОВКИ

Було проведено аналіз баз даних, який має у себе мобільний оператор. Ці бази даних розподіленні на три основні блоки: власна інформація, персональні дані абонента та дзвінки й передача даних. Власна інформація поділяється також на ще два під-блока: інформація, яка стосується лише конкретного оператора, та міжоператорська інформація. В кожному блоці або в під-блоці є від трьох до п’яти баз даних, в яких зберігається вся інформація, яка мається у даного оператора.

Також було проведено аналіз ризиків, які можуть порушити роботу оператора, за властивостями інформації. Основною властивістю з більшою кількістю ризиків є конфіденційність. Цілісність та доступність мають меншу кількість ризиків, але теж можуть вплинути на роботу оператора.

Останнє, що було проаналізовано, це заходи та рішення щодо забезпечення безпеки. Деякі оператори використовують стандарти, як ISO 9000 та ISO 9001, а також ISO/IEC 27005, IEC/ISO 31010 та інші стандарти із управлінням ризиками, та різні рішення, як використання алгоритмів шифрування та систему контролю та управління доступом, щоб забезпечити безпеку своїм абонентам. Також в деяких країнах захист інформації будь-якого підприємства є закріпленим на законодавчому рівні, як SOX ITGC.

Також абоненту необхідно знати про заходи з безпеки, щоб він не став жертвою шахрайства та спокійно розмовляти зі своїми знайомими по номерам телефону.

Щодо запобігання атакам та підвищення рівня захисту конфіденційної інформації, мобільний оператор повинен дотримуватися всіх раніше згадані заходи та стандарти та підтримувати своїх співробітників, щоб вони не зливали дані про те, що мається в базах даних.

СПИСОК ВИКОРАСТАННОЇ ЛІТЕРАТУРИ

1. Что такое колл-центр? Огляд [Електронний ресурс]: https://unitalk.cloud/ru/insajty-dlya-biznesa/chto-takoye-koll-tsentr/

2. Лог – что это такое и как с ними работать. Огляд [Електронний ресурс]: https://hostiq.ua/wiki/log/

3. SMS. Огляд [Електронний ресурс]: https://messaggio.com/ru/glossary/sms-short-message-service-3/

4. Правила и условия рассылки - MMS. Огляд [Електронний ресурс]: https://messaggio.com/ru/glossary/mms-3/

5. Необхідність захисту. Огляд [Електронний ресурс]: https://tzi.com.ua/main1ua.html

6. Кібератака – ВУЕ. Огляд [Електронний ресурс]: https://vue.gov.ua/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0

7. Що таке шпигунське програмне забезпечення? Приклади програм-шпигунів | Gridinsoft. Огляд [Електронний ресурс]: https://gridinsoft.ua/spyware

8. Що таке фішинг і фішингова атака | Блог хостера. Огляд [Електронний ресурс]: https://hostiq.ua/blog/ukr/internet-phishing/

9. Мережі мобільних операторів України захищені від злому та зовнішнього втручання. Огляд [Електронний ресурс]: https://interfax.com.ua/news/general/804803.html

10. ISO 9000. Огляд [Електронний ресурс]: https://apix-drive.com/ua/blog/ecommerce/iso-9000

11. ДСТУ ISO 9000:2015. – 2015. – С. 8 [Електронний ресурс]: https://m.tntu.edu.ua/storage/pages/00000651/dstu9000-2015_osnovni_pol.slovnyk.pdf

12. Официальный сайт Совета по стандартам безопасности данных индустрии платежных карт. Огляд [Електронний ресурс]: https://www.pcisecuritystandards.org/minisite/ru-ru/

13. Что такое и как происходит на соответствие стандарту? Огляд [Електронний ресурс]: https://habr.com/ru/companies/payonline/articles/303330/

14. Five most frequently-asked questions about SOX ITGC compliance. Огляд [Електронний ресурс]: https://medium.com/@akitrablog/five-most-frequently-asked-questions-about-sox-itgc-compliance-3324c314234b

15. IT General Controls (ITGC). Огляд [Електронний ресурс]: https://www.controlaudits.com/it-general-controls-itgc/

16. Петренко Н.І., Бутинець Т.А. Середовище контролю: поняття, природа, соціальна цінність. – 2014. – С. 6 [Електронний ресурс]: http://pbo.ztu.edu.ua/article/view/44098/40584

17. How to implement SOX ITGC? Огляд [Електронний ресурс]: https://medium.com/@akitrablog/how-to-implement-sox-itgc-554acd9c86fc

18. Як захистити свій номер телефону від шахраїв? Пояснює Держспецзв'язку. Огляд [Електронний ресурс]: https://life.pravda.com.ua/society/2022/07/15/249561/

19. Як захистити телефон: 7 функцій та ПЗ для захисту смартфона. Огляд [Електронний ресурс]: https://www.moyo.ua/ua/news/kak_zashchitit_telefon_7_funktsiy_i_po_dlya_zashchity_smartfona.html

20. Як захистити телефон від злому і крадіжки даних: поради українцям. Огляд [Електронний ресурс]: https://www.unian.ua/techno/yak-zahistiti-telefon-vid-zlomu-i-kradizhki-danih-pravila-bezpeki-11758804.html

21. Як перевірити телефон на прослуховування? Методи захисту від прослуховування. Огляд [Електронний ресурс]: https://www.itbox.ua/ua/blog/Yak-pereviriti-telefon-na-prosluhovuvannya-Metodi-zahistu-vid-prosluhovuvannya/

22. Як захиститися від «прослушки»: три способи убезпечити розмови. Огляд [Електронний ресурс]: https://ain.ua/2015/11/09/yak-zahystytysya-vid-proslushky-try-sposoby-ubezpechyty-rozmovy/