МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, доцент
_____ С.В. Легомінова
«_____» _____2020 р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, доцент
_____ С.В. Легомінова
«_____» _____2020 р.

ДИПЛОМНА РОБОТА

на тему:

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ВІДПОВІДНО ДО СТАНДАРТУ ISO 27002

СТУДЕНТ: Стегнієнко Андрій Дмитрович _____
(підпис)

КЕРІВНИК: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.т.н., с.н.с. Щебланін Юрій Миколайович _____
(підпис)

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Освітньо-кваліфікаційних рівень – бакалавр
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
(підпис)
«___»_____2020 р.

ЗАВДАННЯ
на дипломну роботу

студенту Стегнієнку Андрію Дмитровичу

1. Тема роботи «Організація інформаційної безпеки підприємства відповідно до стандарту ISO 27002», затверджена наказом по університету від «___» _____ 2020 р. № ____.

2. Термін здачі студентом оформленої роботи «04» червня 2020 р.

3. Об'єктом дослідження: є засади організації інформаційної безпеки підприємства.

4. Предметом дослідження є напрями організації інформаційної безпеки підприємства відповідно до стандарту ISO 27002.

5. Мета дослідження полягає у теоретичному обґрунтуванні основних напрямів організації інформаційної безпеки підприємства відповідно до стандарту ISO 27002 та розробці відповідних рекомендацій.

6. Перелік питань, які мають бути розроблені:

У відповідності до мети дослідження поставлені наступні задачі:

1.Дослідити підходи до управління інформаційною безпекою;

2. Проаналізувати напрями організації інформаційної безпеки підприємства на основі стандарту ISO 27002;

3.Розробити рекомендації щодо організації інформаційної безпеки на підприємстві.

Дата видачі завдання «_02_» __березня_____ 2020 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «___» _____ 2020 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.03.2020	
2.	Збір та аналіз літератури.	30.03.2020	
3.	Дослідження підходів до управління інформаційною безпекою	16.04.2020	
4.	Аналіз напрямів організації інформаційної безпеки підприємства на основі стандарту ISO 27002	30.04.2020	
5.	Розробка рекомендацій щодо організації інформаційної безпеки на підприємстві	15.05.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	22.05.2020	
7.	Оформлення роботи.	29.05.2020	
8.	Оформлення презентації.	05.06.2020	
9.	Отримання рецензії на роботу.	08.06.2020	
10.	Захист в ДЕК.	09.06.2020	

Студент групи: _____ А.Д. Стегнієнко
(підпис)

Науковий керівник: _____ Т.М. Мужанова
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню проблеми впровадження системи менеджменту інформаційної безпеки підприємства відповідно до стандарту ISO 27002. Робота складається зі вступу, трьох розділів, що містять 8 рисунків, висновки та список використаних джерел, що містить 34 найменування. Загальний обсяг роботи становить 75 аркушів, з яких 4 аркуша займають перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження є засади організації інформаційної безпеки підприємства.

Предметом дослідження є напрями організації інформаційної безпеки підприємства відповідно до стандарту ISO 27002.

Мета дослідження полягає у теоретичному обґрунтуванні основних напрямів організації інформаційної безпеки підприємства відповідно до стандарту ISO 27002 та розробці відповідних рекомендацій.

Як результат у роботі досліджено підходи до управління інформаційною безпекою; проаналізовано напрями організації інформаційної безпеки підприємства на основі стандарту ISO 27002; розроблено рекомендації щодо організації інформаційної безпеки на підприємстві.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті вибору напрямів для впровадження організаційних заходів інформаційної безпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СТАНДАРТ ISO 27002, СТАНДАРТ COBIT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

IEC – International Electrotechnical Commission (Міжнародна електротехнічна комісія)

ISACA - Information Systems Audit and Control Association (Асоціація контролю і аудиту систем)

ISO – International Organization for Standardization (Міжнародна організація зі стандартизації)

ITIL - Information Technology Infrastructure Library (Бібліотека інфраструктури інформаційних технологій)

АС – автоматизована система

ЗПТВ – засоби програмно-технічного впливу

ПБ – політика безпеки

ПЗ – програмне забезпечення

СУІБ – система управління інформаційною безпекою

ВСТУП

У наш час організація ефективних заходів захисту інформаційної системи стає критично важливим стратегічним чинником розвитку будь-якої компанії. По суті, інформація є одним з ключових елементів бізнесу. При цьому під інформацією розуміють не тільки статичні інформаційні ресурси (бази даних, поточні налаштування обладнання та інші), а й динамічні інформаційні процеси обробки даних.

Актуальність теми. У міру розширення сфери використання інформаційних систем та їх ускладнення, проблема забезпечення інформаційної безпеки (ІБ) загострюється. Безпеку вже неможливо забезпечити одним лише набором технічних засобів та підтримувати тільки силами підрозділу безпеки. Відсутність регулярної оцінки інформаційних ризиків, недостатня інформованість співробітників про правила роботи з захищеними системами і дотримання режиму ІБ, відсутність формалізованої класифікації інформації за ступенем її критичності і уявлень про те, скільки коштують інформаційні активи, - все це може звести нанівець зусилля компанії щодо забезпечення інформаційної безпеки.

З підвищенням ролі інформаційних систем в підтримці основних бізнес-процесів компанії до цих проблем додаються питання забезпечення безперервності функціонування бізнесу в критичних ситуаціях. Ігнорування проблем ІБ, практика «латання дірок» сьогодні можуть обійтися компанії дуже дорого. Вирішити ці питання можна шляхом побудови ефективної системи управління інформаційною безпекою (СУІБ).

Мета дослідження полягає у теоретичному обґрунтуванні основних напрямів організації інформаційної безпеки підприємства відповідно до стандарту ISO 27002 та розробці відповідних рекомендацій.

Мета дослідження полягає у теоретичному обґрунтуванні та визначенні основних способів захисту конфіденційної інформації.

Мета дослідження передбачає розв’язання таких **завдань**:

1. Дослідити підходи до управління інформаційною безпекою.

2. Проаналізувати напрями організації інформаційної безпеки підприємства на основі стандарту ISO 27002.

3. Розробити рекомендації щодо організації інформаційної безпеки на підприємстві.

Об’єктом дослідження є засади організації інформаційної безпеки підприємства.

Предметом дослідження є напрями організації інформаційної безпеки підприємства відповідно до стандарту ISO 27002.

Методи дослідження. Для розв’язання поставлених завдань використано такі методи досліджень: теоретичний – для визначення основних вимог міжнародного стандарту ISO 27002 до побудови системи управління інформаційною безпекою, та емпіричний – для дослідження основних способів аудиту політик інформаційної безпеки в організації

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації організаційних заходів інформаційної безпеки підприємства.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів при впровадженні СУІБ на підприємстві.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ПІДХОДІВ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1. Міжнародні стандарти з управління інформаційною безпекою серії ISO 27000

Фахівцям у галузі інформаційної безпеки сьогодні майже неможливо обійтися без знань відповідних стандартів і специфікацій.

На це є декілька причин. Необхідність дотримання певних стандартів закріплена законодавчо. Також, є більш переконливі причини: по-перше, стандарти і специфікації – одна з форм накопичення знань (насамперед на процедурному і програмно-технічному рівнях інформаційної безпеки). У них зафіксовані апробовані, високоякісні рішення та методології, розроблені найбільш кваліфікованими фахівцями; по-друге, і ті, і інші є основним засобом забезпечення взаємної сумісності апаратно-програмних систем та їх компонентів. З точки зору України, можна виділити міжнародні та державні стандарти у галузі інформаційної безпеки. Серед міжнародних стандартів варто виділити серію ISO 27k, що присвячена побудові системи управління інформаційною безпекою (СУІБ) [1].

Міжнародні стандарти для систем управління інформаційною безпекою надають модель, якої слід дотримуватися у створенні та експлуатації системи управління. Ця модель включає в себе особливості, за якими експерти в даній галузі досягли консенсусу як міжнародного стану сучасності. ISO 27К підтримує експертний комітет, присвячений розробці міжнародних стандартів систем управління інформаційною безпекою, інакше відомих як сімейство стандартів системи управління інформаційною безпекою (СУІБ).

Завдяки використанню сімейства стандартів СУІБ організації можуть розробити та впровадити систему управління безпекою своїх інформаційних активів, включаючи фінансову інформацію, інтелектуальну власність та реквізити працівника, або інформацію, доручену їм клієнтами чи третіми особами. Ці стандарти також можуть бути використані для підготовки до незалежної оцінки їх СУІБ, що застосовується для захисту інформації [1].

В основі серії стандартів ISO 27000 лежить процесний підхід на основі циклу Шухарта-Демінга.(див. табл.1.).

Таблиця 1.1.

Цикл Шухарта-Демінга

Плануй (розробляй СУІБ)	Розробляй політику, цілі, процеси та процедури щодо управління ризиком та поліпшення інформаційної безпеки, для досягнення результатів, які б відповідали загальній політиці та цілям організації
Виконуй (впроваджуй та забезпечуй функціонування СУІБ)	Впроваджуй та застосовуй політики інформаційної безпеки, заходів управління, процеси та процедури СУІБ
Перевіряй (проводь моніторинг та аналізуй СУІБ)	Оцінюй, зокрема, по можливості, вимірюй результативність процесів щодо вимог політики, цілей і практичного досвіду функціювання СУІБ та інформуй керівництво про результати для подальшого аналізування
Дій (підтримуй та поліпшуй СУІБ)	Проводь коригувальні та запобіжні дії на підставі результатів внутрішнього аудиту СУІБ або іншої важливої інформації та аналізування з боку керівництва для досягнення безперервного поліпшення СУІБ

ISO 27000:2018 складається з політик, процедур, вказівок та пов'язаних з ними ресурсів та діяльності, що спільно керуються організацією, у напрямку захисту своїх інформаційних активів.

Основні вимоги ISO 27000: 2018 це:

Сфера застосування Перший пункт детально визначає сферу застосування стандарту.

Контекст організації. Визнає всі зовнішні та внутрішні питання, що мають відношення до вашої організації, та вашу інформацію чи інформацію, довірену вами третіми сторонами. Потім встановіть усіх зацікавлених сторін, а також наскільки вони стосуються інформації. Необхідно визначити вимоги до зацікавлених сторін, які можуть включати юридичні, нормативні та договірні зобов'язання.

Необхідно визначити сферу вашої СУІБ, яка пов'язана зі стратегічним напрямком вашої організації, основними цілями та вимогами зацікавлених сторін.

Лідерство. Все про роль "топ-менеджменту", що є групою людей, які керують та контролюють вашу організацію на найвищому рівні. Вищому

керівництву необхідно створити СУІБ та політику інформаційної безпеки, забезпечивши сумісність із стратегічним напрямом організації. Необхідно переконатися, що вони стають доступними, повідомляються, підтримуються та розуміються усіма сторонами. Потрібно забезпечити постійне вдосконалення системи СУІБ.

Планування визначає, як організація планує дії щодо подолання ризиків та можливостей інформації. Зосереджується на тому, як організація поводиться з ризиком інформаційної безпеки та має бути пропорційною потенційному впливу. Організації також зобов'язані скласти “Заява про застосовність” (від англ. Statement of applicability (SoA). Планування SoA містить зведення рішень, прийнятих організацією щодо лікування ризиків, цілей контролю та контролю, які ви включили, та тих, які ви виключили, і чому ви вирішили включити та виключити контролі в SOA. Ще одним ключовим напрямком цього пункту є необхідність встановлення цілей інформаційної безпеки, а стандарт визначає властивості, які відповідають цілям інформаційної безпеки.

Підтримка. Все про отримання потрібних ресурсів, потрібних людей та належної інфраструктури для створення, впровадження, підтримки та постійного вдосконалення СУІБ. Він стосується вимог до компетенції, поінформованості та комунікацій для підтримки СУІБ, і це може включати, наприклад, навчання та персонал. Організація також забезпечує належну комунікацію внутрішніх та зовнішніх комунікацій, що мають відношення до інформаційної безпеки та СУІБ. Також весь персонал, який працює під контролем організації, має бути обізнаний про політику безпеки інформації, як вони сприяють її ефективності та наслідки невідповідності. Це включає визначення того, що потрібно повідомляти кому, коли і як це здійснюється.

Експлуатація. Цей пункт стосується виконання планів та процесів, що є предметом попередніх пунктів. Він стосується виконання визначених дій та досягнення цілей інформаційної безпеки. Зважаючи на збільшення використання аутсорсингових функцій у сучасному діловому світі, ці процеси також потрібно визначити та контролювати. Будь-які зміни, будь то заплановані чи непередбачувані, необхідно розглянути тут та наслідки цих наслідків для СУБД. Також стосується виконання оцінок ризику інформаційної безпеки через заплановані інтервали, а також необхідності збереження документальної інформації для фіксації їх результатів. Нарешті, є розділ, який стосується

впровадження плану лікування ризиків, і знову ж таки, необхідність збереження їх результатів у документально підтвердженій інформації[2].

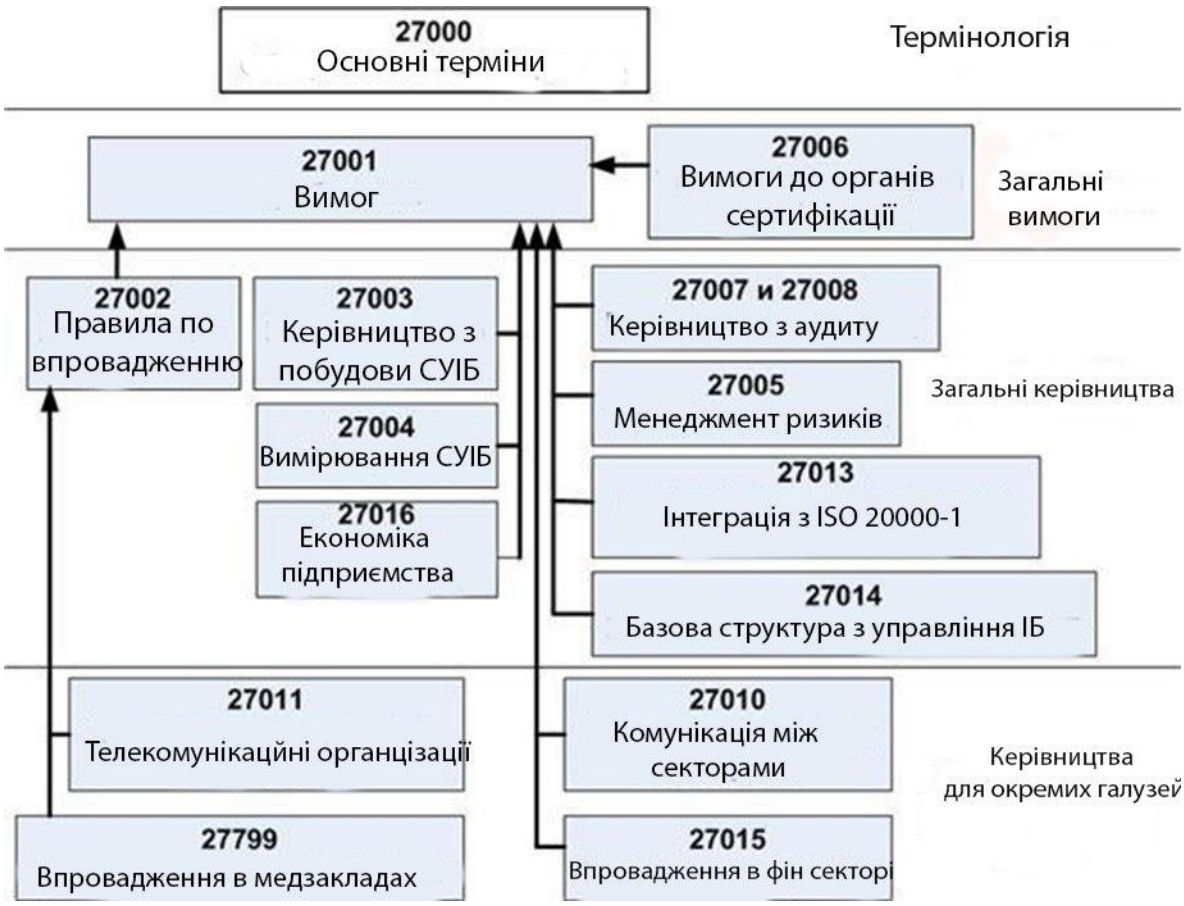

Рис. 1.1. Взаємозв’язок стандартів серії ISO 27000

ISO / IEC 27000 Information technology. Security techniques. Information security management systems. Overview and vocabulary - Визначення та основні принципи.

ISO / IEC 27001 Information technology. Security techniques. Information security management systems. Requirements - Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги.

ISO / IEC 27002 Information technology. Security techniques. Code of practice for information security management - Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою.

ISO / IEC 27003 Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance - Керівництво по впровадженню системи управління інформаційною безпекою.

ISO / IEC 27004 Information technology. Security techniques. Information security management. Measurement - Вимірювання ефективності системи управління інформаційною безпекою.

ISO / IEC 27005: 2011 Information technology. Security techniques. Information security risk management - Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки.

ISO / IEC 27006 Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems - Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою.

ISO / IEC 27007 Information technology. Security techniques. Guidelines for Information Security Management Systems auditing - Керівництво для аудитора СУІБ.

ISO / IEC TR 27008 Information technology. Security techniques. Guidance for auditors on ISMS controls - Керівництво по аудиту механізмів контролю СУІБ. Буде служити доповненням до стандарту ISO 27007.

ISO / IEC 27009 Information technology. Security techniques. Application of ISO / IEC 27001 - Reguirements. - Вимоги щодо застосування ISO / IEC 27001. (в розробці)

ISO / IEC 27010 Information technology. Security techniques. Information security management for inter-sector communications - Управління інформаційною безпекою при комунікаціях між секторами. Стандарт складається з декількох частин, які надають керівництво по спільному використанню інформації про ризики інформаційної безпеки, механізми контролю, проблеми та / або інциденти, що виходить за межі окремих секторів економіки і держав, особливо в частині, що стосується "критичних інфраструктур".

ISO / IEC 27011 Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO / IEC 27002 - Керівництво з управління інформаційною безпекою для телекомунікацій.

ISO / IEC 27013 IT Security. Security techniques. Guideline on the integrated implementation of ISO / IEC 20000-1 and ISO / IEC 27001 - Керівництво щодо інтегрованого впровадження ISO 20000 та ISO 27001.

ISO / IEC 27014 Information technology. Security techniques. Information security governance framework - Базова структура управління інформаційною безпекою.

ISO / IEC TR 27015 Information technology. Security techniques. Information security management systems guidelines for financial and insurance sectors - Керівництво по впровадженню систем управління інформаційною безпекою в фінансовому та страховому секторі.

ISO / IEC TR 27016 Information technology. Security techniques. Information security management. Organizational economics. Економіка підприємства.

ISO / IEC 27017 Information technology. Security techniques. Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002 - Керівництво з управління інформаційною безпекою щодо використання послуг хмарних обчислень.

ISO / IEC 27018 Information technology. Security techniques. Code of practice for PII protection in public clouds acting as PII processors - Звід практичних правил для захисту PII в громадських хмар, які виступають в якості процесорів PII.

ISO / IEC TR 27019 Information technology. Security techniques. Information security management guidelines based on ISO / IEC 27002 for process control systems specific to the energy utility industry. - Керівництво по впровадженню систем управління інформаційною безпекою в секторі енергетики.

ISO / IEC 27031 Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity - Керівництво по забезпеченню готовності інформаційних і комунікаційних технологій до їх використання для управління безперервністю бізнесу.

ISO / IEC 27032 Information technology. Security techniques. Guidelines for cybersecurity - Керівництво по забезпеченню кібербезпеки.

ISO / IEC 27033-1 Information technology. Security techniques. Network security. Overview and concept - Основні концепції управління мережевою безпекою.

ISO / IEC 27033-2 Guidelines for the design and implementation of network security - Керівництво з проектування та впровадження системи забезпечення мережевої безпеки.

ISO / IEC 27033-3 Reference networking scenarios - threats, design techniques and control issues (CD, revised title) - Базові мережеві сценарії - загрози, методи проектування та механізми контролю.

ISO / IEC 27033-4 Securing communications between networks using security gateways - threats, design techniques and control issues (NP, revised title) - Забезпечення безпеки міжмережевих взаємодій за допомогою шлюзів безпеки - загрози, методи проектування та механізми контролю.

ISO / IEC 27033-5 Securing Virtual Private Networks - threats, design techniques and control issues - Забезпечення безпеки Віртуальних Приватних Мереж - загрози, методи проектування та механізми контролю.

ISO / IEC 27033-6 IP convergence - Конвергенція в IP мережах (Визначення загроз, методів проектування і механізмів контролю в IP мережах з конвергенцією даних, голосу і відео).

ISO / IEC 27033-7 Guidelines for securing wireless networking - Risks, design techniques and control issues - Керівництво щодо забезпечення безпеки бездротових мереж - Ризики, методи проектування та механізми контролю (в розробці).

ISO / IEC 27033-8 Guidelines for securing [insert other network security aspects] - Risks, design techniques and control issues Керівництво по забезпеченню [інші аспекти мережевої безпеки] - ризики, методи проектування та управління (можливо будуть розроблені додаткові частини).

ISO / IEC 27042 Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence - Керівні принципи для аналізу та інтерпретації цифрових доказів.

ISO / IEC 27043 Information technology. Security techniques. Incident investigation principles and processes- Принципи і процеси розслідування інцидентів.

ISO / IEC 27789 Health informatics - Audit trails for electronic health records - Журнал аудиту для електронних медичних записів.

ISO 27799 Health informatics. Information security management in health using ISO / IEC 27002 - Управління інформаційною безпекою в сфері охорони здоров'я. Впровадження вимог ISO / IEC 27002 в медичній галузі.

Що стосується власне українських стандартів з управління ІБ, то спочатку були прийняті стандарт ДСТУ ISO/IEC 27001:2015 Інформаційні технології.

Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT. В даний час українська стандартизація в області управління ІБ проходить деяку проміжну стадію свого формування і є ще недостатньо зрілою, проте намічаються позитивні тенденції у розвитку даної галузі.

1.2. Стандарт з управління безпекою інформаційних технологій COBIT

COBIT (Control Objectives for Information and Related Technologies) - підхід до управління інформаційними технологіями, створений Асоціацією контролю і аудиту систем (Information Systems Audit and Control Association - ISACA) та Інститутом керівництва IT (IT Governance Institute - ITGI) в 1992 році. Він надає менеджерам, аудиторам і IT користувачам набір затверджених метрик, процесів і кращих практик з метою допомогти їм в отриманні максимальної вигоди від використання інформаційних технологій і для розробки відповідного керівництва і контролю IT в компанії.

COBIT 5 є новим поколінням рекомендацій ISACA по керівництву підприємством і менеджменту IT.

COBIT 5 заснований на більш ніж 15-річному досвіді практичного використання і застосування COBIT багатьма підприємствами та спільнотами фахівців в області бізнесу, IT, управління ризиками та безпекою, а також контролю якості. Головними рушійними силами розвитку COBIT 5 є потреби рекомендаціях з наступних питань:

• Отримання інформації від більш широкого кола зацікавлених сторін про їхні очікування від інформаційних і пов'язаних технологій (вигоди, прийнятний рівень ризику і ціни) і про їх пріоритети в забезпеченні впевненості в отриманні очікуваної цінності. Одні зацікавлені особи хочуть отримати віддачу в короткостроковому періоді, іншим цікава довгострокова стабільність. Одні готові до високого ступеня ризику, а інші ні. Цими сподіваннями, які відрізняються і, можливо, конфліктуючими, потрібно ефективно управляти. Більш того, зацікавлені сторони не тільки хочуть брати участь в ухваленні рішень, а й вимагають прозорості - як виконуваних робіт, так і результатів.

Управління зростаючої залежністю успішності підприємств від зовнішніх контрагентів бізнесу та IT, таких як аутсорсингові компанії, постачальники, консультанти, клієнти, постачальники хмарних і інших послуг, а також від різноманітності внутрішніх способів і механізмів формування очікуваної цінності. Управління істотно збільшеним об'ємом інформації. Інформацією слід результативно управляти, а цьому сприятиме результативна інформаційна модель. Управління всепроникливі інформаційними технологіями, які стають все більш інтегрованими в бізнес. Уже недостатньо незалежного управління IT, хай навіть скоординованого з бізнесом. Необхідно, щоб IT стали невід'ємною частиною бізнес-проектів, організаційних структур, управління ризиками, політик, навичок, процесів і так далі.

Роль CIO (Chief Information Officer) і роль IT функції розвиваються. IT та бізнес мають все більше інтегруватися. Подальший розвиток технологій і інновацій. Це питання, пов'язані з творчістю, винахідництвом, розробкою нових продуктів - всім, що робить існуючі пропозиції більш привабливими для клієнтів і допомагає залучати нові категорії клієнтів. Інновації також припускають раціоналізацію і прискорення процесів розробки, виробництва і ланцюжки поставок з тим, щоб доставляти продукти на ринок більш ефективно, швидко і якісно[3].

Повні і наскрізні описи функціональних обов'язків бізнесу та IT і опис всіх аспектів результативного керівництва та управління IT підприємства, таких як організаційні структури, політики, культура і, звичайно, процеси.

Удосконалення контролю над зростаючим числом IT-рішень, що створюються і керованих користувачами. Забезпечення на рівні підприємства:

- формування цінності шляхом результативного та інноваційного використання IT на підприємстві;
- задоволеності бізнес-користувачів послугами та роботою IT;
- відповідності IT законодавству, правилам, контрактними зобов'язаннями і внутрішнім політикам;
- вдосконалення зв'язків між потребами бізнесу і цілями IT.

Розуміння і, в разі потреби, застосування рекомендацій найбільших методологій і стандартів індустрії, таких як Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Framework (TOGAF®), Project Management Body of Knowledge (PMBOK®), PRojects IN Controlled Environments

2 (PRINCE2®), Committee of Sponsoring Organizations of the Treadway Commission (COSO), а також стандартів International Organization for Standardization (ISO). Це допоможе зацікавленим сторонам зрозуміти зв'язку між методологіями і можливості їх спільного використання.

Рис. 1.2. Взаємозв'язок COBIT 5 та інших стандартів ІБ

Інтеграція всіх основних методологій (рис 1.2.) і наборів рекомендацій ISACA, головними з яких є COBIT, Val IT і Risk IT, а крім того Business Model for Information Security (BMIS), IT Assurance Framework (ITAF), Board Briefing on IT Governance і ініціативи Taking Governance Forward (TGF). Методологія COBIT 5 створює основу для інтеграції інших методологій, стандартів і практик.

На основі бази знань COBIT 5 будуть створюватися керівництва і інші продукти, орієнтовані на потреби різних зацікавлених сторін. Очікується, що архітектура продуктів COBIT 5 з часом розвиватиметься [4].

Домени співвідносяться з традиційними сферами відповідальності IT: планування, впровадження, експлуатація та моніторинг. Така структура охоплює всі аспекти управління і використання IT. Виконання всіх 34 високорівневих процесів дозволяє гарантувати власнику бізнес-процесу, що система управління IT є адекватною завданням бізнесу.

У стандарті COBIT детально описано цілі і принципи управління, об'єкти управління, чітко визначені всі IT процеси (для кожного процесу визначені входи

і виходи, виконавці та відповідальні, а також об'єкти контролю та метрики) і вимоги до них, описаний можливий інструментарій (практики) для їх реалізації. В описі IT процесів також наведені практичні рекомендації з управління IT безпекою. COBIT застосовується для контролю і аудиту існуючої системи управління інформаційними технологіями, організації оперативного і стратегічного управління IT, аналізу витрат на IT проекти та підтримку відповідної інфраструктури, відповідності вимогам стандартів і регулюючим організаціям, таких як SOX і COSO.

За допомогою використання стандарту COBIT керівники IT підрозділів перетворять завдання бізнесу в чіткі і зрозумілі плани розвитку IT. Основною перевагою стандарту COBIT є його повнота і виразні практичні рекомендації та інструменти, за допомогою яких можна побудувати систему управління інформаційними технологіями корпорації і, в тому числі, ефективну систему управління ризиками в IT. Таким чином, при використанні методології COBIT інформаційна система будується виходячи з вимог бізнесу і умов жорсткої економії ресурсів, а також ефективного використання цих ресурсів. Іншими словами, стандарт COBIT описує бізнес-орієнтований підхід до створення інформаційного середовища: IT розглядаються в вигляді інструменту бізнесу, а стандарт визначає принципи побудови та організації роботи IT департаменту.

1.3. Підхід до управління інформаційною безпекою ITIL

Згідно з цим підходом пряме використання моделей і стандартів ISO / IEC 27001 та ISO / IEC 17799: 2005 для побудови СУІБ важке. Вони або занадто конкретизовані, а в будь-якій організації, як правило, вже існує певна система процесів, ролей, організаційно-розпорядчих документів інформаційної безпеки, які необхідно інтегрувати в систему управління ІБ.

При цьому не визначаються пріоритети, т.зв. «ваги директив», які зазвичай застосовуються в стандартах аудиту, або навпаки, рекомендації носять занадто загальний характер. Наприклад, стандарти містять або набір контрольних директив, або загальний підхід до систем менеджменту, тобто визначають, що потрібно зробити, але не визначають, як це зробити[5].

Практичний підхід до побудови систем управління ІБ, включає розробку процесів забезпечення ІБ, базується на наступних методичних рекомендаціях і директивах:

• рекомендації ITIL (Information Technology Infrastructure Library, кращий світовий досвід в області організації роботи IT-служби), а також моделі управління IT-ресурсами та IT-сервісами Microsoft Operations Framework (MOF);

• рекомендації Microsoft Service Management Function (SMF);

• стандарт ISO 27001.

Доцільність використання рекомендацій з управління IT-ресурсами та IT-послугами (і в першу чергу процесів управління інцидентами, змінами) при побудові СУІБ обумовлена тим, що процеси забезпечення інформаційної безпеки нерозривно пов'язані з процесами захисту, а значить, і управління інформаційними системами і мають бути тісно інтегровані з процесами управління IT.

Бібліотека ITIL містить комплекс необхідних для побудови СУІБ рекомендацій. По-перше, в ITIL з певним ступенем деталізації описаний процес управління безпекою (Security Management). По-друге, надання IT-послуг, включаючи послуги інформаційної безпеки, відноситься до відповідальності служб інформаційних технологій та інформаційної безпеки. Методи ефективної організації діяльності IT-служб узагальнені в бібліотеці ITIL і багаторазово апробовані. Крім того, компанії пред'являють сьогодні жорсткі вимоги щодо якості IT-послуг (в тому числі і з інформаційної безпеки), що забезпечують підтримку базових бізнес-процесів. Забезпечення гарантованої якості IT-послуг - одна з основних задач процесів ITIL.

Важливо, що для організації ефективної системи управління ІБ, аналогічно управлінню IT-послуг, необхідна чітко діюча система оперативного управління змінами. У ITIL ці завдання вирішені шляхом організації процесів управління змінами. (Change Management).

У даний час бібліотека ITIL стала фактично стандартом в галузі управління IT послугами та увібрала в себе кращі підходи і методики, узагальнюючі накопичений світовий досвід. На рис 3. представлені процеси еталонної моделі ITIL. Згідно з методологією ITIL в забезпеченні інформаційної безпеки беруть участь практично всі процеси еталонної моделі ITIL. Зв'язки процесу управління безпекою з іншими процесами ITIL наведені на рис 1.3.

Інтеграція процесу управління безпекою в систему процесів управління IT-ресурсами та IT-послугами і застосування сервісно-ресурсного підходу при побудові СУІБ (коли забезпечення ІБ розглядається як сервіс з певним рівнем якості, надання якого забезпечується певними фінансовими, технічними, людськими ресурсами) дає цілий ряд переваг. Зокрема, з'являється можливість правильної розстановки пріоритетів для вирішуваних завдань ІБ, підвищення ефективності витрачання ресурсів і коштів, що виділяються на управління безпекою, і як наслідок - підвищення керованості системи ІБ в цілому.

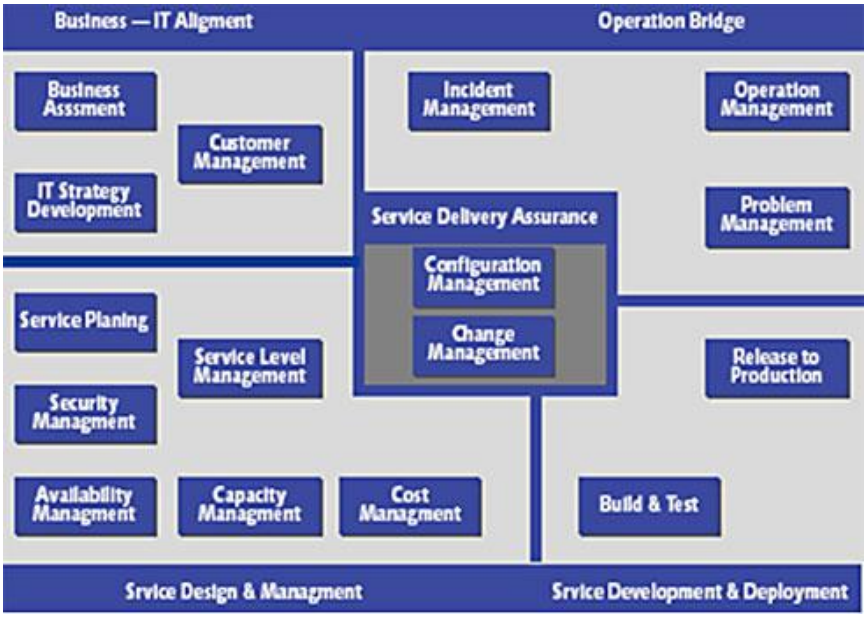

Рис. 1.3. Процеси еталонної моделі ITIL

Рис. 1.4. Зв'язки процесу управління безпекою з іншими процесами ITIL

Разом з тим, одних рекомендацій ITIL для побудови повнофункціональної СУІБ недостатньо. По-перше, необхідна підтримка життєздатності СУІБ в часі, забезпечити її життєвий цикл. Необхідні для цього компоненти і властивості СУІБ («контрольні точки») наведені в використовуваному нами стандарті ISO 27001.

По-друге, в ITIL не містяться деякі важливі складові СУІБ, наприклад, планування забезпечення безперервності ведення бізнесу. Крім того, необхідно більш глибоке визначення процесів забезпечення ІБ і їх взаємозв'язків. Наприклад, для виявлення інцидентів необхідно вести моніторинг підсистем ІБ, який пов'язаний з процесом моніторингу IT-систем, системами Asset Management тощо. Для усунення інцидентів необхідна організація процесу управління інцидентами. Для підтримки життєздатності системи ІБ необхідні регулярні внутрішні аудити системи ІБ, що вимагає певного навчання співробітників і, природно, певного фінансування. Важливими складовими забезпечення інформаційної безпеки є також процеси управління інформаційними ризиками, інформування співробітників про політику ІБ, правила роботи з конфіденційною інформацією тощо [5].

Крім того, необхідно накладення на модель процесів рольової моделі СУІБ, тобто визначення власників процесів, ролей співробітників, які експлуатують підсистеми ІБ і відповідають за відповідні сегменти системи. Тоді в разі інциденту ІБ, наприклад, порушення мережевого захисту, можна буде простежити його вплив на інші процеси і підсистеми ІБ, визначити відповідальних за усунення таких інцидентів, оцінити економічні параметри (яких збитків завдано, які кошти знадобляться для запобігання такого роду інцидентів і т. д.). Певні рекомендації з побудови рольової моделі містяться в документах Microsoft Service Management Function (SMF).

Тому при побудові СУІБ ми використовуємо наведені вище рекомендації та стандарти і на їх основі будуємо процесну модель СУІБ компанії-замовника, що містить три рівні процесів.

• Процеси стратегічного рівня - управління ризиками, управління безперервністю ведення бізнесу, розробка та розвиток політики ІБ верхнього рівня.

• Тактичні процеси - розробка і розвиток процедур ІБ, технічної архітектури системи ІБ, класифікація ІТ-ресурсів, моніторинг і управління інцидентами і інші.

• Процеси операційного рівня - управління доступом, управління мережевою безпекою, перевірка відповідності та ін.

Визначаються взаємозв'язку процесів. В результаті ми отримуємо трирівневу процесно-сервісну модель системи управління ІБ, що відповідає вимогам стандарту ISO 27001, на яку накладається рольова модель.

Модель СУІБ формалізується в єдиному комплексі нормативних документів. У цей комплекс входять наступні основні документи.

1. Концепція забезпечення ІБ.

2. Політика інформаційної безпеки.

3. Положення про інформаційну безпеку компанії.

4. План забезпечення безперервної роботи та відновлення працездатності інформаційної системи в кризових ситуаціях.

5. Правила роботи з захищається.

6. Журнал обліку позаштатних ситуацій.

7. План захисту інформаційних систем компанії.

8. Положення про права доступу до інформації.

9. Інструкція по внесенню змін до списків користувачів і наділення їх повноваженнями доступу до інформаційних ресурсів компанії.

10. Інструкція по внесенню змін до складу та конфігурацію технічних і програмних засобів інформаційних систем.

11. Інструкція по роботі співробітників в мережі Інтернет.

12. Інструкція з організації парольного захисту.

13. Інструкція з організації антивірусного захисту.

14. Інструкція користувачеві інформаційних систем по дотриманню режиму інформаційної безпеки.

15. Інструкція адміністратора безпеки мережі.

16. Аналітичний звіт про проведену перевірку системи інформаційної безпеки.

17. Вимоги до процесу розробки програмного продукту.

18. Положення про розподіл прав доступу користувачів інформаційних систем.

19. Положення з обліку, зберігання і використання носіїв ключової інформації.

20. План забезпечення безперервності ведення бізнесу.

21. Положення щодо створення резервної копії інформації.

22. Методика проведення повного аналізу та управління ризиками, пов'язаними з порушеннями інформаційної безпеки.

Перший крок в побудові процесно-рольової моделі управління системи ІБ - це складання і / або аналіз CMDB (Configuration Management Database) - бази елементарних одиниць, що містить активи системи ІБ (ПО, апаратне забезпечення, співробітники і процедури). Як правило, якісь процеси управління IT у компанії вже є. На жаль, вони часто недостатньо організовані, не формалізовані і погано відповідають вимогам ITIL. Тому для початку потрібно зрозуміти, що є в компанії, потім проаналізувати ключові процеси, які необхідно покращувати. Вибрати один-два процеси, найбільш важливих і вимагають модернізації. Як правило, більшість компаній починають з організації служби Help Desk (сучасна назва-це Service Desk) і впровадження процесу управління інцидентами. У деяких компаніях система Help Desk вже існує і працює, а більш актуальним залишається питання створення процесу управління змінами. У будь-якому випадку, потрібно розставити пріоритети впровадження процесів і співвіднести їх з планами створення СУІБ.

Всі послуги (поточні, знову розроблені і заплановані) мають дотримуватися строгих корпоративних стандартів, що стосуються безпеки інформації [6].

Висновки до розділу 1

У першому розділі розглянуто найбільш відомі міжнародні стандарти в галузі інформаційної безпеки.

У стандарті ISO 27001 міститься опис кроків зі створення, супроводу і вдосконалення СУІБ. Стандарт декларує ризик-орієнтований підхід, який дозволяє вибрати необхідні заходи і засоби захисту, найкращим чином відповідають потребам і інтересам бізнесу. За результатами впровадження стандарту ISO / IEC 27001 компанія може пройти сертифікацію.

Стандарт COBIT 2019 «Впровадження і оптимізація рішення по керівництву інформацією і технологіями» охоплює всю діяльність компанії і дозволяє

широко поглянути на управління ІТ та ІБ. Стандарт носить високорівневий характер, тобто говорить, що має бути досягнуто, але не пояснює, як. За допомогою принципів COBIT 2019 можна мінімізувати ризики і контролювати повернення інвестицій в ІТ і засоби інформаційного захисту.

Рекомендації ITIL визначають кроки на рівні процесів. Крім того, бібліотека містить рекомендації з вибудовування суміжних процесів, наприклад, з управління інцидентами, що дозволяє комплексно поглянути на вибудовування процесів і їх інтеграцію в ІТ-середовище. Бібліотека ITIL корисна фахівцям, в завдання яких входить вибудовування процесу управління ІТ-послугами і інтеграція ІБ в цей підхід.

Зроблено висновок, що для якісної побудови системи інформаційної безпеки потрібно агрегувати знання і поєднувати підходи, отримані з різних джерел, оскільки кожна система поглядів містить плюси і мінуси і вимагає адаптації до умов конкретної компанії. Фахівцям з інформаційної безпеки необхідно постійно вдосконалюватися, розширювати набір компетенцій і професійних знань, і прийняті за кордоном стандарти істотно допомагають в цьому.

РОЗДІЛ 2
НАПРЯМИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДПОВІДНО ДО СТАНДАРТУ ISO 27002

ISO/IEC 27002 було підготовлено Об'єднаним технічним комітетом ISO/IEC JTC 1. Інформаційні технології. Підкомітет SC 27. Безпека інформаційних технології [7].

Цей міжнародний стандарт призначено для застосування організаціями як посилання для вибору елементів управління в процесі реалізації системи управління інформаційною безпекою (СУІБ) на основі ISO/IEC 27001 або як керівний документ для організацій, що виконує загальноприйняті заходи управління інформаційною безпекою. Цей стандарт також призначено для використання як настанови в галузях, що розвиваються для специфічних підприємств та організацій щодо управління інформаційною безпекою, беручи до уваги ризик(и) специфічного навколишнього середовища.

Структура стандарту представлена на Рис. 2.1.

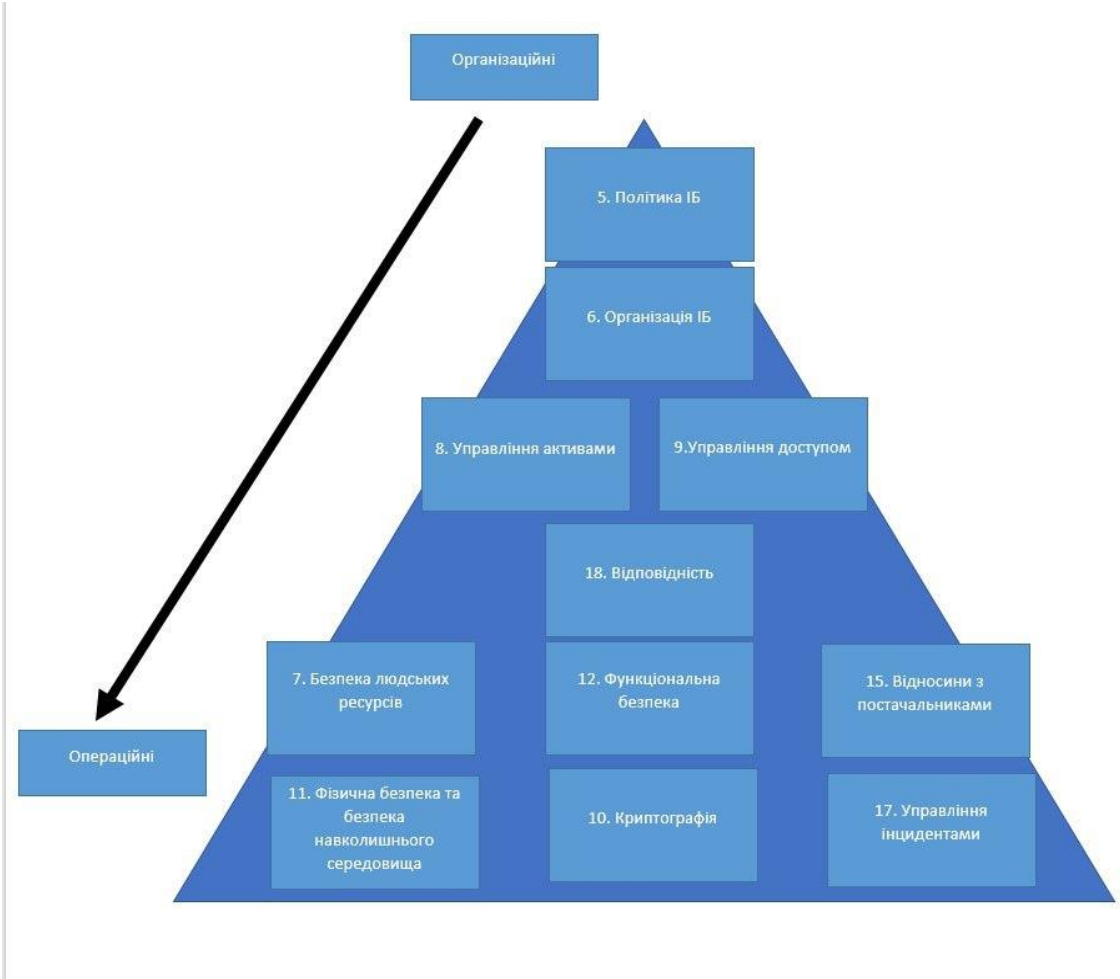

Рис. 2.1. Структура стандарту ISO 27002

Організації всіх типів і розмірів (у тому числі державного і приватного сектора, комерційних і некомерційних) збирають, обробляють, зберігають та передають інформацію в різних формах, охоплюючи електронну, фізичну та словесну (наприклад, розмови і презентації).

Значення інформації виходить за рамки написаних слів, цифр та зображень: знання, концепції, ідеї і бренди є прикладами нематеріальних форм інформації. У взаємопов'язаному світі інформація та процеси, системи, мережі і персонал, який бере участь в її роботі, обробці та захисті, пов'язані, це активи, які, як і інші важливі бізнес-активи, є цінними для бізнесу підприємства і, отже, заслуговують або потребують захисту від різних небезпек.

Активи це суб'єкти як умисних, так і випадкових загроз, в той час як, пов'язані з ними процеси, системи, мережі і люди мають притаманні вразливості. Зміни в бізнес-процесах і системах або інші зовнішні зміни (наприклад, нові закони і правила) можуть створювати нові ризики інформаційної безпеки. Тому, враховуючи безліч способів, в яких загрози можуть скористатися вразливістю, щоб нашкодити підприємству, ризик інформаційної безпеки завжди є наявним. Ефективна інформаційна безпека знижує ці ризики, захищаючи підприємство від загроз і вразливостей, а потім зменшує вплив на його активи.

У більш загальному сенсі ефективна інформаційна безпека також запевняє управління та інші зацікавлені сторони, що активи підприємства є досить безпечними і захищеними від шкоди, тим самим виступаючи як бізнес-виконавець.

2.1. Нормативно-організаційні аспекти управління інформаційною безпекою

Розробка політики інформаційної безпеки

Створення політики інформаційної безпеки має на меті забезпечити спрямування управління і підтримку інформаційної безпеки відповідно до бізнес вимог та відповідних законів і нормативно-правових актів.

Набір політик інформаційної безпеки має бути визначений, схвалений керівництвом, виданим і повідомленими співробітникам і відповідним третім сторонам.

На найвищому рівні підприємства потрібно визначити "Політику інформаційної безпеки", яка схвалена керівництвом і яка викладає підхід організації до управління його цілями інформаційної безпеки.

Політики інформаційної безпеки мають задовольняти вимоги, створених:

a) бізнес-стратегією;

b) нормативно-правовими актами, законодавством і контрактами;

c) поточними і спроектованими умовами загроз інформаційній безпеці навколишнього середовища.

Політика інформаційної безпеки має містити положення щодо:

a) визначення інформаційної безпеки, цілей і принципів для ведення будь-яких дій, що стосуються інформаційної безпеки;

b) призначення загальних і приватних обов'язків, що визначають ролі з управління інформаційною безпекою;

c) процеси для обробки вручну відхилень і винятків.

На нижчому рівні політика інформаційної безпеки має бути підтримана специфічними вузько направленими політиками, які передають управління впровадженням заходів контролю інформаційної безпеки, і вона, як правило, структурована під відповідні потреби певних цільових груп в рамках підприємства або зачіпає деякі цілеспрямовані теми.

Прикладами таких політик можуть бути:

a) управління доступом;

b) класифікація інформації (і обробка вручну);

c) фізична безпека і безпека навколишнього середовища;

d) кінцевий користувач, орієнтований на такі теми, як:

1) прийнятне використання активів;

2) «чистий» стіл і «чистий» екран;

3) інформаційна передача;

4) мобільні пристрої і віддалена робота;

5) обмеження на встановлення програмного забезпечення та його використання;

e) резервна копія;

f) інформаційна передача;

g) захист від шкідливого програмного забезпечення;

h) управління технічно слабкими місцями;

i) управління криптографічними засобами захисту;

j) безпеку комунікаційних засобів;

k) приватне життя і захист персональних даних;

l) відносини з постачальниками [7].

Ці політики мають бути повідомлені співробітникам і відповідним третім сторонам у формі, яка є доступною і зрозумілою читачеві її, наприклад, в контексті "обізнаності в питаннях інформаційної безпеки, освітня програма і програма навчання".

Потреби підприємства у внутрішніх політиках для інформаційної безпеки можуть варіюватися. Внутрішні політики особливо корисні в більших і складніших організаціях, де вони визначають і забезпечують очікувані рівні заходів контролю, знаходяться окремо від тих, які здійснюють заходи контролю, або в ситуаціях, де політика може бути застосована до багатьох різних людей або функціонує на підприємстві. Політики інформаційної безпеки можуть бути випущені в єдиному документі "політика інформаційної безпеки" або як набір окремих, але пов'язаних між собою, документів.

Якщо будь-які політики інформаційної безпеки винесені за межі підприємства, то потрібно забезпечити нерозголошення конфіденційної інформації.

Деякі підприємства використовують інші терміни для цих програмних документів, такі як: "Стандарти", "Директиви" або "Правила".

Політики інформаційної безпеки необхідно розглянути в запланованих інтервалах або при наявності істотних змін, щоб гарантувати її придатність, відповідність та ефективність.

У кожної політики має бути власник, який схвалив відповідальність керівництва за розвиток, огляд і оцінку політики. Огляд має включати можливості оцінки для покращення політики підприємства і підходу в керівництві інформаційної безпеки у відповідь на зміни навколишнього середовища підприємства, бізнес обставин, юридичних чи технічних умов.

Огляд політики для інформаційної безпеки має взяти до уваги результати оглядів щодо управління.

Має бути отримано схвалення керівництва для переглянутої політики.

Організація інформаційної безпеки

Метою організації інформаційної безпеки підприємства є встановити основні рамки управління, що починають та контролюють впровадження та функціонування інформаційної безпеки в межах підприємства.

Усі зобов'язання щодо інформаційної безпеки має бути визначено та розділено.

Розподіл зобов'язань у сфері інформаційної безпеки має бути зроблено відповідно до політик інформаційної безпеки [7]. Зобов'язання щодо захисту окремих активів та відповідних визначених процесів інформаційної безпеки мають бути визначені. Відповідальність за управління ризиками інформаційної безпеки та, зокрема, для прийняття остаточних ризиків мають бути визначені. Ці відповідальності мають бути доповнені, за необхідності, більш детальною настановою для конкретних приміщень та засобів обробки інформації. Конкретні обов'язки щодо захисту активів і для відповідних визначених процесів інформаційної безпеки мають бути визначені.

Особи, які відповідають за інформаційну безпеку, можуть делегувати завдання щодо забезпечення безпеки іншим. Проте вони залишаються підзвітними і мають повідомляти, що будь-які делеговані завдання були виконані правильно.

Багато організацій призначають менеджера з інформаційної безпеки, який бере на себе відповідальність за розробку та впровадження інформаційної безпеки та підтримки встановлених заходів контролю.

Тим не менше, відповідальність за виділення ресурсів та впровадження заходів контролю, часто залишають за окремими керівниками. Практикують призначення власника для кожного активу, який відповідає за нього увесь час.

Розподіл обов'язків — це метод зниження ризику від випадкового або навмисного неправильного використання активів підприємства.

Суперечливі обов'язки та сфери відповідальності мають бути відокремлені, щоб зменшити можливості для несанкціонованої або випадкової зміни, або неправильного використання активів підприємства.

Слід проявляти обережність, щоб жодна людина не може отримати доступ, змінювати чи використовувати активи без авторизації. Початок події має бути відокремлено від його авторизації. Слід враховувати можливість змови під час проектування заходів контролю.

На невеликих підприємствах важко досягти розподілу обов'язків, але

принцип має застосовуватись, наскільки це можливо і доцільно. Кожного разу, коли важко відокремити, інші заходи управління, такі як: моніторинг діяльності, аудит та управління - необхідно розглянути.

Інформаційна безпека в управлінні проектами. Інформаційну безпеку слід розглядати в управлінні проектами, незалежно від типу проекту.

Інформаційну безпеку має бути інтегровано в метод(-и) управління проектами підприємства, щоб забезпечити інформаційну безпеку, якщо є ризик(-и), які виявляють і, які є частиною проекту. Це стосується, як правило будь-якого проекту, незалежно від його характеру, наприклад, проект для бізнес-процесу, ІТ, управління будівлями та інші підтримувальні процеси.

Залучення інформаційної безпеки мають бути спрямовано і регулярно переглядатись у всіх проектах. Відповідальності за інформаційну безпеку має бути визначена для визначених осіб, визначених у методах управління проектами.

Дистанційна робота має бути впроваджено політику та підтримувальні заходи безпеки щодо захисту інформації, допуску, функціонування та збереження місць дистанційної роботи.

Підприємства мають лише тоді дозволяти дистанційну роботу, якщо вони впевнені, що належні заходи безпеки та заходи контролю наявні і що вони задовольняють політику безпеки підприємства.

Робота з персоналом

Стандарт встановляє три основні аспекти роботи з персоналом у сфері інформаційної безпеки [7] (Рис.2.2.).

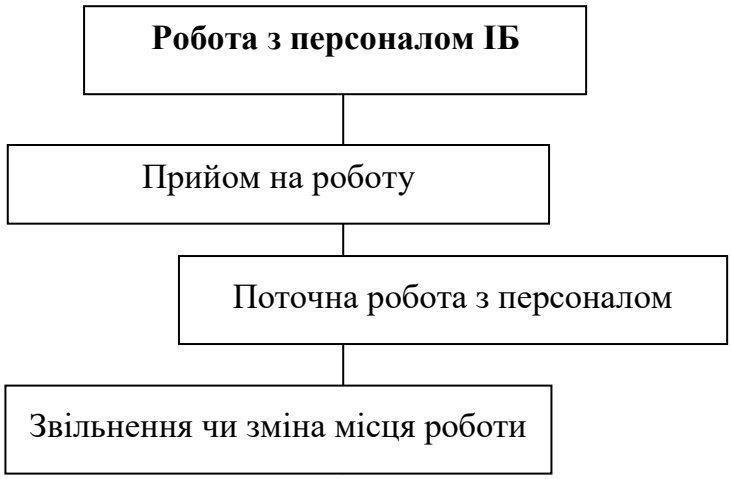

Рис. 2.2. Робота з персоналом у сфері інформаційної безпеки

Перед прийомом на роботу забезпечити, щоб працівники, наймані на постійній основі та працівники за договором розуміли свої обов’язки і чи підходять вони для ролі, на які їх розглядають.

Детальні перевірки всіх кандидатів при прийомі на роботу мають виконуватись згідно з відповідними законами, правилами й етичними нормами, та мають відповідати бізнес-вимогам, класифікації інформації, що буде їм доступна і передбачуваних ризиків.

Процедури мають визначити критерії та обмеження для оглядів перевірки, наприклад, хто має право сортувати людей і як, коли і чому огляди перевірки здійснюються.

Процедуру відбору має бути також застосовано до підрядників. У цих випадках угода між підприємством і підрядником має конкретизувати відповідальності для проведення відбору та процедур повідомлення, за якими потрібно слідувати, якщо відбір не було завершено або якщо результати дають привід для сумніву або занепокоєння.

Інформацію відносно всіх кандидатів, що розглядаються для позицій в межах підприємства, потрібно зібрати і використовувати відповідно до будь-якого відповідного законодавства, наявного в доречній юрисдикції. Залежно від відповідного законодавства, кандидатів має бути завчасно проінформовано про відібрання.

Договори за контрактом з працівниками і підрядниками мають встановлювати їх відповідальності та відповідальності підприємства за інформаційну безпеку.

Договірні зобов’язання для працівників або підрядників мають відображатись політиками інформаційної безпеки підприємства на додаток до уточнення та констатації:

a) що всі співробітники та підрядники, яким надається доступ до конфіденційної інформації, мають підписати угоду про конфіденційність або угоду про нерозголошення до того, як надається можливість доступ до засобів обробки інформації;

b) законні обов’язки та права працівників або підрядників, наприклад відносно законів про авторське право або законодавства про захист даних;

c) зобов’язання щодо класифікації інформації та управління активами підприємства, пов’язані з інформацією, засобами обробки інформації та інформаційних послуг, оброблених працівником або підрядником;

d) зобов’язання працівника чи підрядника за обробку інформації, отриманої від інших компаній або організацій ззовні;

e) дії, які мають бути прийняті, якщо працівник чи підрядник ігнорує вимоги безпеки підприємства [5].

Ролі інформаційної безпеки та зобов’язання мають доводитися до відома кандидатів на роботу під час процедури приймання на роботу.

Підприємство має забезпечити, що працівники та підрядники, що погоджуються з термінами та умовами стосовно інформаційної безпеки, відповідно до природи та розміру доступу, який вони будуть мати до активів підприємства, пов’язаних з використанням інформаційних систем і послуг.

Де відповідно, зобов’язання, що містяться в межах термінів і умов зайнятості, мають продовжуватись певний період після кінця зайнятості.

Кодекс поведінки можна використовувати для співробітників або підрядників щодо зобов’язань з інформаційної безпеки, що стосується конфіденційності, захисту даних, етичних питань, належного використання обладнання та об’єктів підприємства, а також авторитетні практики, поширювані на підприємство. Може бути потрібним, щоб організація ззовні, з якою підрядник є пов’язаний, вступила в договірні відносини від імені особи договору.

Керівництво має вимагати, щоб усі працівники і підрядники застосовували інформаційну безпеку відповідно до встановлених політик і процедур підприємства.

Зобов’язання керівництва мають стосуватись гарантування, що працівники і підрядники:

a) були належним чином поінформовані про свої ролі з інформаційної безпеки та відповідальності перед тим, як отримати доступ до конфіденційної інформації або інформаційних систем;

b) були забезпечені настановами з встановлення інформаційної безпеки про їх ролі в межах підприємства;

c) були мотивовані, щоб виконувати політики інформаційної безпеки підприємства;

d) досягнули рівня інформованості щодо інформаційної безпеки відповідно

до їх ролей та обов’язків на підприємстві;

e) відповідність термінів та умов найму, що охоплює політику інформаційної безпеки підприємства і відповідні методи роботи;

f) продовжували мати відповідні навички та кваліфікацію і регулярно навчатись;

g) були забезпечені анонімним каналом для повідомлень про порушення інформаційної безпеки політики або процедур.

Керівництво має продемонструвати підтримку політики, процедури та заходи контролю інформаційної безпеки, а також виступати як модель ролі.

Якщо співробітники і підрядники не поінформовані про свої обов’язки щодо забезпечення інформаційної безпеки, то вони можуть завдати значної шкоди підприємства. Мотивований персонал, ймовірно, буде більш надійними і буде спричиняти менше інцидентів інформаційної безпеки.

Неефективне управління може призвести до відчуття неоціненності персоналу, в результаті чого буде негативний вплив на інформаційну безпеку підприємства.

Усі співробітники підприємства та, у відповідних випадках, підрядники мають отримати відповідну обізнаність, навчання та професійна підготовка та регулярне оновлення інформації в політиках та процедурах підприємства, відповідно для їх функціональних обов’язків.

Програма обізнаності щодо інформаційної безпеки направлена на допомогу співробітникам та, за необхідності, підрядникам, усвідомлення своїх обов’язків щодо інформаційної безпеки та засоби, за допомогою яких ці обов’язки виконують.

Програма обізнаності щодо інформаційної безпеки встановлюється відповідно до політик інформаційної безпеки підприємства і відповідних процедур, беручи до уваги розгляд підприємством інформації, яку захищено та заходи контролю, які були впроваджені, щоб захистити інформацію. Програма обізнаності має охоплювати низку інформаційно-просвітницьких заходів, таких, як кампанії (наприклад "день інформаційної безпеки") та випуск буклетів або інформаційних бюлетенів.

Програму обізнаності планують, беручи до уваги ролі працівників в організації, і, де доречно, очікування підприємства про обізнаність підрядчиків. Діяльність в рамках програми обізнаності має відбуватись за розкладом

протягом тривалого часу, переважно регулярно, так, щоб діяльність повторювалася і охоплювала нових співробітників і підрядників. Програма обізнаності також має регулярно оновлюватись, так щоб залишалась відповідною політикам і процедурам підприємства, а також має бути побудована на досвіді, отриманому з інцидентів інформаційної безпеки.

Професійна підготовка щодо обізнаності виконується відповідно до програми обізнаності інформаційної безпеки підприємства. Професійна підготовка щодо обізнаності може використовувати різні способи подання, зокрема, використання аудиторних занять, дистанційне навчання, навчання на основі інтернету, індивідуальні та інші [7].

Навчання інформаційній безпеці та професійна підготовка має відбуватись періодично. Початкова освіта і підготовка стосується тих, хто переходить на нові посади чи ролі з істотно різними вимогами щодо інформаційної безпеки, не лише стажерів і має мати місце перед тим, як роль стане активною.

Підприємство розробляє програму навчання та професійної підготовки для ефективного управління навчанням та професійною підготовкою. Програма має бути відповідною політикам інформаційної безпеки підприємства і процедурам, беручи до розгляду інформацію підприємства, яка захищена і заходи контролю, які були впроваджені, щоб захистити інформацію. Програма розглядає різні форми навчання та професійної підготовки, наприклад, лекції або самостійне вивчення.

Під час складання програми обізнаності, важливо не лише зосередитися на «що» та «як», але і «чому». Важливо, щоб співробітники розуміли мету інформаційної безпеки та потенційні наслідки, позитивні і негативні, на підприємство, через їх поведінку.

Обізнаність, навчання та професійна підготовка можуть бути частиною, або провадиться у співпраці з іншими навчальними заходами, наприклад, звичайні ІТ або загальна підготовка в галузі безпеки. Діяльність щодо обізнаності, навчання та професійної підготовки мають бути придатними і відповідними для ролей, обов’язків і навичок кожного співробітника.

Оцінка розуміння співробітників буде провадитися наприкінці навчального курсу щодо обізнаності, навчання та професійної підготовки, щоб перевірити передачу знання.

Має бути формалізовано і повідомлено про дисциплінарний процес на місці,

щоб вжити дії проти працівників, які скоїли прорив інформаційної безпеки.

Дисциплінарний процес розпочинають без попереднього підтвердження того, що стався інцидент інформаційної безпеки.

Формальний дисциплінарний процес має забезпечити правильне і справедливе ставлення до працівників, підозрюваних у скоєнні проривів інформаційної безпеки, а також градуйовану реакцію, яка бере до уваги такі чинники, як природу та вагу прориву, та його вплив на бізнес, чи це вперше або повторне порушення, чи порушник був належним чином навчений або ні, відповідне законодавство, ділові контракти й інші чинники, якщо це необхідно.

Дисциплінарний процес може також бути використано як стримувальний засіб, щоб перешкоджати працівникам порушити політики та процедури інформаційної безпеки підприємства і будь-які інші прориви інформаційної безпеки. Навмисні прориви можуть потребувати негайних дій.

2.2. Управління безпекою фізичних активів

Управління активами

Управління активами має на меті ідентифікувати активи підприємства і визначити відповідні відповідальності з безпеки.

Управління активами включає три етапи [7] (Рис.2.3.).

Рис. 2.3. Управління активами

Активи, пов’язані з інформацією і засобами обробки інформації, мають бути ідентифіковані та інвентаризаційний опис цих активів має бути складений і підтриманий.

Підприємство має ідентифікувати активи, відповідно до життєвого циклу інформації, і мати документ щодо важливості. Життєвий цикл інформації охоплює створення, обробку, зберігання, передачу, видалення та руйнування. Документування підтримується в спеціалізованих або поточних інвентаризаційних описах.

Інвентаризаційний опис активу має бути точним, сучасним, послідовним і вирівняний до інших описів.

Для кожного з ідентифікованих активів має бути призначено володіння активом, і класифікація має бути ідентифікована.

Інвентаризаційний опис активів допомагають гарантувати, що ефективний захист має місце і може також бути потрібним для інших цілей, такі як: здоров'я і безпека, страхові або фінансові (управління активами) причини.

ISO/IEC 27005 забезпечує приклади активів, які, можливо, потрібно було розглянути підприємством, ідентифікуючи активи. Процес складання інвентаризаційного опису активів є важливою передумовою управління ризиками [8].

Активи, що містяться в інвентаризаційному описі, мають бути у володінні.

Окремі співробітники, так само як інші юридичні особи, що мають схвалену керівництвом відповідальність для життєвого циклу активу визначені, будуть призначені як власники активу.

Процес гарантує своєчасне призначення володіння активом як звичайне впровадження. Володіння має бути визначено, коли активи створено або коли активи передано до підприємства. Власник активу має бути відповідальним за належне управління активом протягом усього життєвого циклу активу.

Власник активу має:

a) гарантувати, що активи інвентаризовані;

b) гарантувати, що активи відповідно класифіковано та захищено;

c) визначити і періодично переглядати обмеження доступу та класифікацію, зважаючи на важливість активів, беручи до уваги застосовні політики управління доступом;

d) гарантувати правильне поводження, коли актив буде видалено або зруйновано.

Ідентифікований власник може бути або окремо узятим працівником, або юридичною особою, хто підтвердив і готовий нести відповідальність за

управління протягом життєвого циклу активу. Ідентифікований власник не обов’язково має які-небудь права власності на актив.

Звичайні завдання можуть бути делеговані, наприклад, розпоряднику, який піклується про активи щодня, але відповідальність залишається за власником.

У складних інформаційних системах може бути корисно визначати групи активів, які діють разом, надаючи окрему послугу. У цьому разі власник цієї послуги є відповідальним за надання послуги, що охоплює функціонування цих активів.

Правила для прийнятного використання інформації та активів, пов’язаних з інформацією та пристроями обробки інформації мають бути ідентифіковані, задокументовані та впроваджені.

Співробітники та зовнішні користувачі, що використовують активи або мають доступ до активів підприємства, мають бути проінструктовані на предмет знання про вимоги інформаційної безпеки щодо актив

ів підприємства, пов’язаних з інформацією і засобами обробки інформації та ресурсів. Вони мають бути відповідальними за своє використання будь-яких ресурсів оброблення інформації і будь-якого іншого використання проведених під їх відповідальністю.

Усі співробітники та зовнішні користувачі мають повернути всі активи підприємства їх власнику на завершення їх використання, договору чи угоди.

Процес звільнення має бути формалізовано, щоб охоплювати повернення всіх раніше виданих фізичних та електронних активів, що належали підприємству або їх було доручено.

У разі, якщо співробітник або зовнішній користувач купує обладнання для підприємства або використовує власне приватне обладнання, то процедур слід дотримуватись, щоб гарантувати, що вся відповідна інформація передана підприємству, надійно стерта з устаткування.

У разі, коли у співробітника або зовнішнього користувача є знання, що є важливим для виконання операцій, то ця інформація має бути задокументована і передана підприємству.

Протягом періоду повідомлення щодо процесу звільнення підприємство має управляти несанкціонованим копіюванням відповідної інформації (наприклад, інтелектуальна власність) звільненими співробітниками і підрядниками [7].

Власники інформаційних активів мають бути відповідальними за їх

класифікацію.

Система класифікації має містити угоди щодо класифікації та критерії для перегляду класифікації протягом довгого часу. Рівень захисту системи має бути оцінено, аналізуючи конфіденційність, цілісність і доступність і будь-які інші вимоги щодо інформації має бути розглянуто. Система має ураховувати політику управління доступом.

Кожному рівню потрібно дати ім’я, яке матиме сенс в контексті розуміння системи класифікації.

Система має бути сумісною з усією організацією так, щоб усі могли класифікували інформацію і пов’язані з нею активи у такий спосіб, щоб мати однозначне розуміння захисних вимог і застосовували відповідній засіб захисту.

Класифікація має бути включена в процеси підприємства, і бути послідовною і взаємопов’язаною. Результати класифікації мають вказувати на вартість активів залежно від їх уразливості і важливості для підприємства, наприклад, з точки зору конфіденційності, цілісності та доступності. Результати класифікації мають оновлюватися відповідно до змінення їх вартості, уразливості та важливості протягом їх життєвого циклу.

Класифікація надає людям, які мають справу з інформацією короткі вказівки щодо того, як поводитися і захистити її. Створення груп інформації з подібними потребами захисту і зазначенням процедур безпеки інформації, що застосовні до усієї інформації у кожній групі, полегшують це. Такий підхід скорочує потреби в індивідуальній оцінці ризику та у звичайній розробці заходів контролю.

Інформація може припинити бути чутливою або важливою після певного періоду часу, наприклад, після того, як інформацію було оприлюднено. Ці аспекти мають бути прийняті до уваги, як така надкласифікація може привести до використання непотрібних заходів контролю, що призводить до додаткової витрати або навпаки недокласифікація може піддати небезпеці досягнення бізнес-цілей.

Процедури з маркування інформації мають охоплювати інформацію та пов’язані з нею активи в фізичному та електронному форматі. Маркування має відобразити систему класифікації. Маркування має бути легко пізнаваним. Процедури мають дати вказівки, де і як маркувати, викладені з урахуванням того, як отримують доступ до інформації, або як управляють активами, залежно від використовуваного типу медіа. Процедури можуть визначити випадки, де

маркування упущено, наприклад, маркування неконфіденційної інформації, щоб скоротити навантаження на робітників. Співробітники та підрядники мають зробити правильне маркування процедур.

Результат від систем, що містять інформацію, яку класифіковано як уразливу або важливу, має нести відповідне маркування класифікації.

Маркування інформації з обмеженим доступом – ключова вимога для заходів спільного користування інформацією. Фізичне маркування та метадані – стандартна форма маркування.

У маркування інформації та пов'язаних з нею активів можуть іноді бути негативні ефекти. Класифіковані активи легше ідентифікувати і відповідно можуть бути вкраденими інсайдерами або зовнішніми нападниками.

Процедури щодо обробки активів має бути розроблені і впроваджені відповідно до системи класифікації інформації, схваленої підприємством.

Процедури мають бути складені для того, щоб до них звертатись, обробляти, зберігати і повідомляти інформацію, сумісну з її класифікацією.

Наступні позиції потрібно розглянути:

a) обмеження доступу, що підтримують вимоги безпеки для кожного рівня класифікації;

b) обслуговування формального запису уповноважених одержувачів активів;

c) захист тимчасових або постійних копій інформації до рівня, сумісного із захистом з первісної інформації;

d) зберігання ІТ активів відповідно до специфікацій виробників;

e) чітке маркування всіх копій медіа з повідомленням уповноваженого одержувача [7].

Система класифікації, яка використовується в межах підприємства, може не бути еквівалентною схемами, використовуваним іншими організаціями, навіть якщо назви рівнів подібні; крім того, інформація, що переміщається між організаціями може змінитись за класифікацією залежно від його контексту в кожній організації, навіть якщо їх системи класифікації ідентичні.

Угоди з іншими організаціями, які охоплюють спільне користування інформацією, містять процедури ідентифікації та класифікації тієї інформації і інтерпретування маркування класифікації від іншої організації.

Процедури мають бути впроваджені для управління знімними медіа

відповідно до системи класифікації, прийнятої підприємством.

Формальні процедури з безпечного позбавленню від медіа мають бути встановлені, щоб мінімізувати ризик витоку конфіденційної інформації несанкціонованим особам. Процедури щодо безпечного позбавленню від медіа, що містять конфіденційну інформацію, мають бути пропорційними уразливості цієї інформації.

Фізична безпека та безпека інфраструктури

Фізична безпека та безпека інфраструктури має на меті запобігти неавторизованому фізичному доступу, ушкодженню та вторгненню до службових приміщень підприємства, та втручанню в її інформацію.

Для захисту зон, що містять інформацію чи засоби оброблення інформації, треба використовувати периметри безпеки.

Щодо периметрів фізичної безпеки розглядають та впровадити там, де належно, такі настанови:

a) периметри безпеки мають бути чітко визначені, а розміщення та міцність кожного з периметрів мають залежати від вимог безпеки щодо активів в межах цього периметра та результатів оцінки ризику;

b) периметри будівлі або приміщень, які містять засоби оброблення інформації, мають бути фізично надійними (тобто там не має бути проміжків у периметрі або зон, де легко може статись зламування);

b) зовнішні стіни приміщень мають бути міцної конструкції і всі зовнішні двері мають бути відповідним чином захищені від неавторизованого доступу контрольними механізмами, наприклад, засувами, тривожною сигналізацією, замками тощо; двері та вікна мають бути замкнені, коли залишаються без нагляду, також треба передбачити зовнішній захист для вікон, особливо на рівні землі;

c) мають бути наявною зона чергування або інші засоби контролю фізичного доступу до приміщень або будівлі; доступ до приміщень або будівель має дозволятися лише авторизованому персоналу;

d) щоб запобігти неавторизованому фізичному доступу та псуванню інфраструктури там, де це потрібно, мають бути побудовані фізичні бар'єри;

e) усі пожежні двері у периметрі безпеки мають бути обладнані тривожною сигналізацією, треба здійснювати їх моніторинг та тестувати разом зі стінами, щоб встановити потрібний рівень опору згідно з відповідними регіональними,

національними та міжнародними стандартами; вони мають безвідмовно функціонувати згідно з місцевими правилами пожежної безпеки;

f) згідно з національними, регіональними або міжнародними стандартами мають бути встановлені придатні системи виявлення порушників, їх треба регулярно тестувати щодо охоплення цими системами всіх зовнішніх дверей та доступних вікон; незайняті зони мають постійно бути під охороною тривожної сигналізації; також необхідно забезпечувати наданий захист для інших зон, наприклад, кімнат з комп'ютерами та засобами комунікацій;

g) засоби оброблення інформації, якими управляє підприємство, мають бути фізично відокремлені від засобів, якими управляють треті сторони [5].

Фізичної захищеності можна досягти створенням одного чи більше фізичних бар'єрів навколо службових приміщень та засобів оброблення інформації підприємства. Використання численних бар'єрів надає додатковий захист, за якого відмова одного бар'єра не означає негайної компрометації безпеки.

Зоною безпеки може бути офіс, що замикається, або декілька кімнат, оточених суцільним внутрішнім бар'єром фізичної безпеки. Для контролю фізичного доступу між зонами з різними вимогами безпеки всередині периметру безпеки можуть бути потрібні додаткові бар'єри та периметри.

Особливої уваги щодо безпеки фізичного доступу потребують будівлі, де розташовані різні організації.

Додаток фізичного контролю, особливо для зон безпеки, може бути адаптований щодо технічної чи економічної обстановки підприємства, що зазначено в оцінці ризиків.

Зони безпеки мають бути захищені належними контролями прибуття, щоб забезпечити, що доступ дозволений тільки авторизованому персоналу

Щоб уникнути неавторизованого доступу, точки доступу, наприклад, зони доставки та відвантаження, а також інші точки, через які особи, доступ яких не авторизовано, можуть увійти до службових приміщень, мають бути контрольовані і, за можливості, ізольовані від засобів оброблення інформації.

Розглядають наведені нижче рекомендації:

a) доступ до зон постачання та завантаження із-зовні будинку має бути обмежений ідентифікованим і авторизованим персоналом;

b) зони постачання та завантаження мають бути спроектовані таким чином,

щоб поставки могли бути розвантажені без отримання персоналом доставляння доступу до інших частин будівлі;

c) зовнішні двері зони постачання та завантаження мають бути замкнені, коли відчинені внутрішні двері;

d) матеріали, що надходять, мають обстежуватися на наявність вибухових, хімічних або інших небезпечних речовин до того, як вони будуть переміщені з зони постачання та завантаження;

e) матеріали, що надходять, мають реєструватися згідно з процедурою управління активом на вході до приміщення [6];

f) партії товару, що надходять і відсилаються, мають бути, за можливості, фізично розподілені.

g) матеріали, що надходять, мають бути перевірені на наявність підробки в дорозі. Якщо підробка виявлена, то про це потрібно негайно доповісти персоналу з безпеки.

Безпека обладнання має на меті запобігти втратам, ушкодженню, крадіжці або компрометації активів та перериванню діяльності підприємства.

Обладнання має бути розміщене чи захищене таким чином, щоб зменшити ризики загроз, пов’язаних з інфраструктурою і небезпек та можливого неавторизованого доступу.

2.3. Управління безпекою інформаційно-телекомунікаційних систем

Управління взаємодією та функціонуванням

Управління взаємодією та функціонуванням має на меті забезпечити правильну та безпечну роботу систем обробки інформації.

Основними напрямами управління процедурами та функціонуванням є:

– Розробка операційних процедур і обов'язків, які мають забезпечити належне і безпечне функціонування засобів обробки інформації.

– Менеджмент надання послуг третьою стороною з метою реалізації і підтримки належного рівня інформаційної безпеки та надання послуг третіми сторонами згідно з положеннями угод про надання послуг.

– Планування та приймання систем, які забезпечують мінімізацію ризику збоїв у роботі систем.

– Захист від шкідливого коду, спрямований на захист цілісності інформаційних активів і програмного забезпечення.

– Створення резервних копій інформаційних активів з метою підтримки цілісності і доступності інформації та засобів їх обробки.

– Управління безпекою мережі забезпечує захист інформації в мережах та підтримуючої інфраструктури.

– Забезпечення належного поводження з носіями інформації, щоб запобігти неавторизованому розкриттю, модифікації або знищенню активів.

– Безпечний обмін інформацією з використанням надійного програмного забезпечення в межах підприємства і з зовнішніми суб'єктами.

– Послуги електронної торгівлі за умови їх безпечного використання.

– Здійснення моніторингу функціонування систем і мереж з метою виявлення неавторизованих дій, пов'язаних з обробкою інформації [5].

Рис.2.4. Напрями управління взаємодією та функціонуванням

Операційні процедури мають бути задокументовані і доступні всім користувачам.

Документовані процедури мають бути готові до оперативної діяльності, пов’язаної з інформацією обробкою і засобами зв’язку, таких як комп’ютер запуску і закриття процедур, резервне копіювання, технічне обслуговування обладнання, роботи з матеріалами, комп’ютерний зал та обробка кореспонденції

управління і безпеки.

Операційні процедури мають вказати в експлуатаційних інструкціях, зокрема:

a) встановлення та налаштування систем;

b) обробки та обробки інформації як автоматичного, так і ручного;

c) резервні;

d) встановлення вимог, у тому числі і взаємозалежності з іншими системами, ранні роботи початку і останнім часом завершення роботи;

e) інструкції по обробці помилок чи інших виключних умов, які можуть виникнути в процесі роботи виконання, у тому числі обмеження на використання системних утиліт;

f) підтримка та ескалації зовнішніх контактів, включаючи контакти у разі непередбаченого експлуатаційних і технічних труднощів;

г) спеціальні вихідні та ЗМІ інструкції з експлуатації, такі, як використання спеціального канцелярського або управління конфіденційного виробництва, в тому числі процедури для їх безпечної утилізації продукції неробочих місць;

c) перезапуск системи і процедури відновлення у разі збою системи;

я) управління аудиту і системного журналу;

в) процедури контролю.

Чинні інструкції і документовані процедури системи діяльності, розглядають як офіційні документи і зміни, затверджені керівництвом. Це технічне здійснення інформаційні системи має здійснюватися послідовно, з використанням тих самих процедур, інструментів і утиліт. Зони безпеки необхідно захищати належними контролями прибуття, щоб забезпечити, що доступ дозволений тільки авторизованому персоналу

Контроль доступу

Контроль доступу має на меті обмежувати доступ до інформації та засобів оброблення інформації

Політика контролю доступу має бути визначена, задокументована та переглядатися на основі вимог бізнесу та інформаційної безпеки.

Власник активів має визначити відповідні правила контролю доступу, права доступу та обмеження для конкретних ролей користувачів по відношенню до їх активів, разом з відповідною кількістю деталей та точними заходами контролю, що пов’язані з ризиками інформаційної безпеки.

Заходи контролю щодо доступу є як логічними, так і фізичними і їх треба розглядати разом. Користувачам та постачальникам послуг треба надати чітке положення щодо бізнес-вимог, які мають задовольняти заходи контролю щодо доступу.

Правила контролю доступу мають підтримуватись формальними процедурами та чітко визначеними обов'язками.

Роль, основана на контролі доступу є тим підходом, використовуваним успішно багатьма організаціями, що пов'язує права доступу з бізнес ролями.

Два основних принципи керівництва політики контролю доступу:

a) Потрібно знати: вам надається доступ тільки до інформації, щоб ви змогли виконати поставлені вам завдання (мається на увазі різні завдання/ролі які потрібно знати та різні профілі доступу);

b) Необхідно використовувати: Вам надається доступ тільки до об'єктів обробки інформації (IT обладнання, процедур, кімнат) необхідних вам для виконання завдання/роботи/ролей.

Користувачам має надаватися доступ тільки до мережі та мережевих послуг, на використання яких їх було авторизовано.

Має бути сформульована політика стосовно використання мереж і мережевих послуг. Ця політика має стосуватись:

a) мереж і мережевих послуг, до яких дозволено доступ;

b) процедур авторизації для визначення, кому дозволено доступ і до яких мереж та мережевих послуг;

c) управління заходом контролю та процедурами захисту доступу до мережевих підключень та мережевих послуг;

d) засоби, що використовують доступ до мереж і мережевих послуг (наприклад застосування VPN або бездротової мережі);

e) вимоги до автентифікації користувачів для доступу до різних мережевих послуг;

f) моніторинг використання мережевих послуг [5].

Політика користування мережевими послугами має бути послідовною згідно з політикою організації контролю доступу.

Неавторизовані та незахищені підключення до мережевих послуг можуть зашкодити всьому підприємству. Такий контроль є особливо важливим для мережевих підключень до чутливих або важливий бізнес-додатків або до

користувачів, розташованих у місцях високого ризику, наприклад загальнодоступних чи зовнішніх зонах, що знаходяться поза межами управління та контролю інформаційною безпекою підприємства.

Управління доступом користувача має на меті забезпечити авторизований доступ користувача і запобігти неавторизованому доступу до систем та послуг.

Процес офіційної реєстрації та зняття з реєстрації користувача має бути впроваджений, щоб відобразити призначення прав доступу.

Процес надання доступу офіційним користувачам має бути реалізовано призначанням та скасовуванням права доступу всім користувачам до всіх систем та послуг.

Розподіл та використання привілейованих прав доступу має бути обмеженим та контрольованим.

Розподіл привілейованих прав доступу має контролюватися за офіційно оформленим процесом авторизації відповідно до політики контролю доступу. Розглядають наведені нижче кроки:

a) мають бути ототожнені привілейовані права доступу, пов’язані з кожною системою або процесом, наприклад, операційною системою, системою управління базою даних та кожною прикладною програмою, і користувачі, для яких вони мають бути призначені;

b) призначення привілейованих прав доступу користувачам має бути основана на: потребо-використовуй та від-події-до-події згідно з політикою контролю доступу, тобто призначаються на рівні мінімальних вимог, яких потребує їх функціональна роль;

c) має підтримувати процес авторизації та реєструвати всі призначені привілеї. Привілейовані права доступу не мають надаватися до завершення процесу авторизації;

d) мають бути визначені вимоги щодо закінчення привілейованих прав доступу;

e) привілейовані права доступу мають призначатись користувачу ID, які відрізняються від тих, що використовують зазвичай у бізнесовій діяльності. Звичайна бізнес діяльність не має проводитись з привілеями ID;

f) компетенції користувача з привілейованими правами доступу мають регулярно переглядатися з метою перевірки на відповідність їх своїм службовим обов’язкам;

g) конкретні процедури мають бути встановлені і підтримуватися для того, щоб уникнути несанкціонованого використання користувачів IDs загального адміністрування, відповідно до можливостей конфігурації систем [7].

Розподіл привілейованих прав доступу має контролюватися за офіційно оформленим процесом авторизації відповідно до політики контролю доступу. Розглядають наведені нижче кроки:

a) мають бути ототожнені привілейовані права доступу, пов’язані з кожною системою або процесом, наприклад, операційною системою, системою управління базою даних та кожною прикладною програмою, і користувачі, для яких вони мають бути призначені;

b) призначення привілейованих прав доступу користувачам має бути основана на принципах: використовуй за потреби та від події до події згідно з політикою контролю доступу тобто призначаються на рівні мінімальних вимог, яких потребує їх функціональна роль;

c) має підтримувати процес авторизації та реєструвати всі призначені привілеї. Привілейовані права доступу не мають надаватися до завершення процесу авторизації;

d) мають бути визначені вимоги щодо закінчення привілейованих прав доступу;

e) привілейовані права доступу мають призначатись користувачу ID, які відрізняються від тих, що використовують зазвичай у бізнесовій діяльності. Звичайна бізнес діяльність не має проводитись з привілеями ID;

f) компетенції користувача з привілейованими правами доступу мають регулярно переглядатися з метою перевірки на відповідність їх своїм службовим обов’язкам;

h) конкретні процедури мають бути встановлені і підтримуватися для того, щоб уникнути несанкціонованого використання користувачів IDs загального адміністрування, відповідно до можливостей конфігурації систем;

Розподіл привілейованих прав доступу має контролюватися за офіційно оформленим процесом авторизації відповідно до політики контролю доступу. Розглядають наведені нижче кроки:

a) мають бути ототожнені привілейовані права доступу, пов’язані з кожною системою або процесом, наприклад, операційною системою, системою управління базою даних та кожною прикладною програмою, і користувачі, для

яких вони мають бути призначені;

b) призначення привілейованих прав доступу користувачам має бути основана на: потребо-використовуй та від-події-до-події згідно з політикою контролю доступу, тобто призначаються на рівні мінімальних вимог, яких потребує їх функціональна роль;

c) має підтримувати процес авторизації та реєструвати всі призначені привілеї. Привілейовані права доступу не мають надаватися до завершення процесу авторизації;

d) мають бути визначені вимоги щодо закінчення привілейованих прав доступу;

e) привілейовані права доступу мають призначатись користувачу ID, які відрізняються від тих, що використовують зазвичай у бізнесовій діяльності. Звичайна бізнес діяльність не має проводитись з привілеями ID;

f) компетенції користувача з привілейованими правами доступу мають регулярно переглядатися з метою перевірки на відповідність їх своїм службовим обов'язкам;

i) конкретні процедури мають бути встановлені і підтримуватися для того, щоб уникнути несанкціонованого використання користувачів IDs загального адміністрування, відповідно до можливостей конфігурації систем;

Придбання, розробка і супровід системи

Вимоги інформаційної безпеки для пом'якшення ризиків, пов'язаних з доступом постачальника до активів підприємства узгоджують з постачальником та документують.

Підприємство визначає та доручає управління інформаційною безпекою, конкретно розглянувши доступ постачальника щодо інформації підприємства в політиці. Ці елементи управління мають враховувати процеси і процедури мають бути реалізовані в підприємства, а також тих процесів і процедур, які підприємства має вимагати від постачальника в реалізації, зокрема:

a) виявлення та документування типів постачальників, наприклад, IT-послуги, логістика, комунальні послуги, фінансові послуги, компоненти IT-інфраструктури, яким підприємство дозволить отримати доступ до його інформації;

b) звичайним процесом і життєвим циклом для управління відносинами з постачальниками;

c) визначення типів доступу до інформації, що різним типам постачальників буде дозволено, а також моніторинг та контроль доступу;

d) мінімальні вимоги інформаційної безпеки для кожного типу інформації і типу доступу в якості основи для індивідуальних угод з постачальниками на основі бізнес-потреб підприємства і вимоги його ризиків;

e) процеси та процедури контролю дотримання вимог, встановлених в області інформаційної безпеки для кожного типу постачальника і типу доступу, включаючи огляд третьою стороною та перевірки продукції;

f) достовірність і повнота контролю з метою забезпечення цілісності інформації або інформації, обробка однією із сторін, за наявністю відповідної вимоги;

g) види зобов'язань, застосовних до постачальників захисту інформації підприємства;

h) обробка інцидентів і ситуацій, пов'язаних з доступом, у тому числі обов'язків підприємства та постачальників;

i) стійкість і, за необхідності, відновлення та резервні механізми для забезпечення доступності інформація;

j) підготовку з підвищення інформованості персоналу підприємства ведуть щодо застосованої політики, процесів та процедур;

k) проведення інструктажу для персоналу підприємства, щодо взаємодії з персоналом постачальника відносно відповідних правил участі та поведінки в залежності від типу постачальника і рівня доступу постачальника до систем підприємства та інформації;

l) умови, за яких вимоги інформаційної безпеки та управління будуть задокументовані в угоді, що підписана обома сторонами;

m) управління необхідними переходами інформації, засобами обробки інформації, що мають бути переміщені, забезпечивши інформаційну безпеку, що зберігається протягом перехідного періоду [7].

Інформація може бути поставлена під загрозу постачальниками з недостатнім рівнем управління інформаційною безпекою. Управління має бути визначеним і застосовуватися для управління доступом постачальника для обробки інформації. Наприклад, якщо є особлива необхідність в конфіденційності інформації, то угода про нерозголошення може бути використана. Іншим прикладом є захист даних ризиків при угоді з

постачальником, включає в себе передачу або доступ до такої інформації через інших. Підприємство має на увазі, що юридична або договірна відповідальність за захист інформації залишається за нею.

Договори з постачальниками включають вимоги до усунення ризиків інформаційної безпеки пов’язані з інформаційними та комунікаційними технологіями послуг і поставок продукції.

Конкретне управління інформаційно-комунікаційними технологіями, практика побудови ризиків на основі загальної інформаційної безпеки, якості управління проектами та практики системного проектування, але не замінюючи їх.

Підприємствам рекомендується працювати з постачальниками, щоб зрозуміти інформацію та комунікацію технологій ланцюга постачань, а також будь-які питання, які мають великий вплив на продукти і послуги, що надаються. Підприємства можуть впливати на інформаційні і комунікаційні технології ланцюжка поставок, але чітко як прописано в угодах з постачальниками.

Підприємства регулярно проводять моніторинг, огляд і аудит наданих постачальником послуг. Моніторинг та огляд послуг постачальника має гарантувати, що умови інформаційної безпеки та умови угод будуть дотримувалися і що інциденти інформаційної безпеки та проблем будуть вирішені належним чином [15].

Потрібно включати процес управління службових відносин між підприємством і постачальником:

a) рівень продуктивності сервісного моніторингу, щоб перевірити дотримання угод;

b) розглядати товари, послуги, надані постачальником і організувати регулярні зустрічі з обговоренням продуктивності в міру необхідності визначені угодами;

c) проводити перевірки постачальників, звертати увагу на перевірки незалежних аудиторів, якщо такі є, та надалі діяти відповідно до результатів;

d) надавати інформацію про інформаційні інциденти безпеки і розглянути цю інформацію в міру необхідності договорами, залучивши будь-які допоміжні керівні принципи та процедури;

e) провадити аудити та робити записи подій інформаційної безпеки, експлуатаційних проблем, відстежувати помилки і збої, пов’язані з наданням послуг;

f) знаходити рішення і управляти виявленими проблемами;

g) враховувати аспект інформаційної безпеки у взаєминах постачальника з власними постачальниками;

h) забезпечити, щоб постачальник мав достатню здатність роботи у планах визначених для того, щоб рівень роботи не був порушений, крім деяких описаних випадків, або таких подій як стихійні лиха.

Відповідальність за управління відносинами з постачальниками мають бути віднесені до призначених співробітниками або служби управління командою. Крім того, підприємство має забезпечити, щоб постачальники призначили відповідальність за розгляд дотримання та виконання вимог угоди. Достатній технічні навички та ресурси мають бути доступні для контролю, що вимоги Угода, зокрема, вимоги до інформаційної безпеки, виконуються. Відповідні дії мають бути прийняті при виявленні недоліків у наданні послуг не спостерігається. Підприємство має зберігати достатню загальний контроль і видимість у всіх аспектах безпеки для чутливі або важлива інформація або обробки інформації засобами, наданими, обробляються або керованого постачальником. Підприємство має зберігати видимість в діяльності щодо забезпечення безпеки, такі як управління змінами, виявлення вразливостей і події інформаційної безпеки звітності та реагування допомогою Певний процес звітності.

Зміни у наданні послуг постачальниками, в тому числі підтримку і поліпшення існуючих політик, процедури і засобів контролю інформаційної безпеки, має здійснюватися з урахуванням критичності ділової інформації, систем і процесів, пов’язаних з переоцінкою ризиків.

Висновки до розділу 2

В даному розділі розглянуто основні положення міжнародного стандарту ISO 27002 та визначено три основні напрями організації інформаційної безпеки: нормативно-організаційний напрям, управління фізичними активами й управління безпекою інформаційно-телекомунікаційних систем.

Визначено що, політика інформаційної безпеки має на меті забезпечити спрямування управління і підтримку інформаційної безпеки відповідно до вимог бізнесу та нормативно-правової бази. Метою організації інформаційної безпеки підприємства є встановити основні рамки управління, що починають та контролюють впровадження та функціонування інформаційної безпеки в межах підприємства.

Управління активами забезпечує ідентифікацію активів підприємства і визначити відповідні відповідальності з безпеки. Заходи забезпечення фізичної безпеки та безпека інфраструктури спрямовані запобігти неавторизованому фізичному доступу, ушкодженню та вторгненню до службових приміщень підприємства, та втручанню в її інформацію.

Управління взаємодією та функціонуванням має на меті забезпечити правильну та безпечну роботу систем обробки інформації. Контроль доступу забезпечує обмеження доступу до інформації та засобів їх обробки. Придбання, розробка і супровід системи має на меті гарантувати, щоб інформаційна безпека була невід’ємною частиною інформаційних систем в рамках усього життєвого циклу.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1. Рекомендації до політики безпеки та плану захисту інформації підприємства

Протидія соціальній інженерії схожа на внутрішню боротьбу з людською суттю. Коли мова йде про контрзаходи, часто згадуються три основні сфери [21].

Перший рівень захисту, звичайно, технічний. Важливим є правильно налаштувати робочі і антивірусні програми. Вони мають мати змогу зупинити більшість спаму та фішингових листів, а більшість браузерів мають вбудовану функцію виявлення фішингу та шкідливого програмного забезпечення, яка певною мірою також допоможе в протидії. Ще одним простим захистом буде чорний список відправників з доменом підприємства, щоб хто-небудь не зміг підмінити адреси когось з підприємства. Інший підхід полягає у використанні електронних листів із цифровим підписом, як це пропонується у книзі «Соціальний фішинг» [26].

Важливо мати політику, спрямовану на різноманітні сфери ризиків [27]. Не тільки важливо мати правила, що стосуються того, що робити, а чого не робити, що також може звільнити працівників від необхідності думати про те, що є правильним та неправильним, тоді замість посилання на політику, визначені певні обмеження [21].

Співробітники потребують тренінгів щодо того, як безпечно зберігати конфіденційну інформацію. Одним з важливих факторів є те, щоб усі зрозуміли, що вони захищають і чому, і включити це в перегляд політики [28].

Одним із найважливіших факторів успіху при роботі з інформаційною безпекою є видима підтримка та відповідність усіх рівнів управління, як описано в [29]. Отже, важливо реалізувати всі ці контрзаходи. Почнемо з того, що ви мають висвітлити проблему, провести певний тест в рамках аудиту або тест на проникнення. Один з поширених способів полягає в тому, щоб перевірити персонал на рівень їх обізнаності в галузі інформаційної безпеки, але це може бути не настільки ефективним, як проведення фактичних тестів на проникнення, які імітують вірогідний вектор атаки.

Важливою проблемою є визначитись, що саме ви тестуєте. Якщо не існує жодних правил чи політик, персонал має вгадувати, що правильно і неправильно. Можливо, це не очевидно, що захист бездротової мережі важливий. Політика має важливе значення, і, принаймні, мають бути правила для:

-Паролів;

-Бездротової мережі;

-Зовнішніх носіїв інформації;

-Передачі конфіденційної інформації;

-Встановлення програм;

-Пристроїв;

-Соціальної інженерії.

Політика протидії соціальній інженерії також враховує відповідальність працівників щодо прийняття судових по відношенню до зловмисників [30]. Незважаючи на всі політики, термін "соціальна інженерія" ніколи не згадується. Однак працівники потребують належного рівня обізнаності, освіти та підготовки в процедурах безпеки. Окрім політики кінцевих користувачів, адекватна технічна захищеність, безумовно, є важливою і потребує управління людьми, які добре розуміють власні функції і призначення.

Всі люди можуть бути жертвами соціальної інженерії. У людини є слабкі місця, які можуть бути використані, і єдиним способом зменшення ризику є усвідомлення ризиків та на-явність здорової дози параної. Існує очевидна потреба у спеціальній підготовці кадрів для кожної посади. Грагг розповідає про багаторівневий захист від соціальної інженерії [8] і перераховує 5 рівнів захисту для мінімізації ризиків впливу атаки з використанням соціальної інженерії.

-Політика безпеки, що стосується соціальної інженерії;

-Підвищення рівня обізнаності про безпеку для всіх користувачів;

-Навчання для ключових співробітників;

-Поточні нагадування;

-Social Engineering Land Mines (SELM).

SELM означає, що ви можете встановити пастки для запобігання атаці. Якщо хтось закликає надати інформацію, ви маєте політику компанії, щоб надавати її, ви можете зателефонувати безпосередньо до керівника, якщо людина може трохи зачекати, даючи вам час для обговорення з колегою, і, швидше за все, атакуючий відступить, щоб запобігти виявленню. Під час перевірки

спроможності людей потрапити під вплив соціальної інженерії може бути цікавіше перевірити відповідність політики замість людських якостей. Міхаель Сімовітс стверджує: "Єдине, що можна перевірити на захищеність від соціальної інженерії, - це люди, які слідкують за процесом чи не слідкують за ним"[32].

Ще одне важливе питання, яке люди часто забувають: "Що ми захищаємо?". Дуже важливо зрозуміти, що захищає підприємство і чому. Багато компаній зберігають забагато даних, створюючи проблеми, з якими вони не можуть працювати, оскільки це підвищує зацікавленість поганих хлопців у вторгненні. Деякі хмарні сервіси не усвідомлюють, що їх велика кількість інформації створює набагато більший ризик.

Не менш важливим є рівень обізнаності користувачів у компанії, люди, що працюють з інформаційними технологіями та безпекою, мають добре розуміти, як працівники використовують свої комп'ютери та інформаційну систему для виконання своєї роботи. Часто впроваджується політика, без розуміння того, що ніхто не прийме і не дотримуватиметься її. Це було показано в опитуванні, проведеному Manpower Sweden, де 43% із 6362 респондентів заявили, що не виконують політику на своєму робочому місці, в основному тому, що це занадто застаріло або вони не знають як це все виконати, ще. 26% відповіли, що не зможуть виконувати свою роботу, якщо вони дотримуватимуться політики [33].

Є декілька правил, які допоможуть не попадатись на гачки шахраїв:

Звертайте увагу на написання адрес сайтів

Якщо Вам пропонують переглянути сайт/фото/відео, зазиваючи емоційними закликами – не переходьте одразу. По-рахуйте до 10-ти та згадайте, що це можливо приклад соціальної інженерії.

Вводячи логін/пароль в акаунтах на сайтах, звертайте увагу на незвичайні зміни зовнішнього вигляду сторінок. Якщо щось викликає підозру – краще перевірити оригінальність ресурсу ще раз.

Критично ставтесь до електронних листів, а особливо до посилань за якими пропонують перейти незнайомі відправники повідомлень.

Ці чотири правила не є вичерпними, але тримаючи їх у пам’яті та використовуючи як фільтр під час користування Інтернет, Ви зможете суттєво покращити свій інформаційний за-хист та стати менш вразливим до методів соціальної інженерії.

Фішинг. Основою захисту від фішинг-атак є «навчання» користувачів. Своєчасне і повне інформування співробітників про дану загрозу і про необхідність ретельної перевірки джерела запиту конфіденційних або персональних даних усуне основну умову існування фішинг-атак. Тобто виховання у співробітників компанії скептичного ставлення до будь-яких несподіваних вхідних листів. З цією метою в компаніях вводиться спеціальна політика, яка регламентує дії користувачів, які отримують подібні листи і використовують конкретні принципи користування електронної пошти з обов'язковими прикладами атак, що використовують ці принципи:

вкладення в документи;

гіперпосилання в документах;

запит особистої або корпоративної інформації, які виходять із середини компанії;

запит особистої або корпоративної інформації, які виходять із-за меж компанії.

При виникненні нових різновидів фішингу необхідно допрацьовувати документ і з доробками знайомити користувачів

Шкідливі програми. Політика безпеки є необхідним атри-бутом будь-якої продуманої стратегії захисту від черв'яків. Проста заборона на відкриття вкладених файлів з електронних листів знижує ризик зараження поштовими черв'яками практично до нуля.

Спливаючі діалогові вікна і додатки. В першу чергу, в політиці ІБ має бути записано правило, яке по кроках описує дії користувача в разі появи діалогових вікон, дуже властиві операційній системі (наприклад Windows). Про якісь неполадки і системні помилки негайно повідомляти в службу підтримки про проблему. Самому нічого не робити і не натискати жодних кнопок.

З точки зору політики, краще відразу відключати для користувача різні вбудовані рекламні смуги на сторінках, встановити заборону на скачування файлів з веб-сторінок і FTP-серверів (можна як усіх, так і з набором розширень як службових, так мультимедійних та архівів).

Спам. У політиці ІБ необхідно чітко прописати дії користувачів, якщо до них приходить електронне повідомлення від невідомого адресата. Тут підходить все, що зазначено в за-грозі «фішинг». Проте потрібно вказати механізм і

порядок дії для користувача, зробити приклади для наочності. У самих правилах жорстко вказати наступні моменти:

якщо назва теми говорить сама за себе, адресат не відомий – навіть не відкриваючи визначати в кошик;

якщо адресат відомий, але тема не відноситься до робочого процесу і викликає підозру, тим більше якщо видно, що лист прибув із вкладеннями – видалити лист або довести до відома служби підтримки;

ніколи не відкривати вкладення в листі від невідомого адресата, незалежно від розширення вкладення (офісні документи, архіви, програми, фотографії);

ніколи не натискати на посилання в тілі листа і клацати на картинки, навіть якщо адресат відомий;

уважно придивлятися до назви вкладення і розширення від відомого адресата;

ні в якій мірі не висилати ніякі свої паролі і облікові записи, ні за яку вимогу, будь-то безпосередній керівник або директор компанії, або співробітник служби ІБ і адміністратор;

якщо запитувана інформація від «легального» користувача викликає недовіру, що це потрібно написати або переслати – краще передзвонити і повідомити про це безпосереднього керівника, а також до служби ІБ або ІТ (при відсутності служ-би ІБ)

Загроза судового переслідування. У політиці ІБ має бути заборонено обмін/скачування будь-якого контенту, що є по-рушенням авторських прав (мультимедійний, програмні розробки, видавнича та інша література).

Online-ігри. Прописати в політиці ІБ категоричну заборону на даний вид розваг. Аргументовано привести графічні приклади і включити їх в програму навчання співробітників.

Інтернет-пейджери. Необхідно передбачити в корпоративних політиках безпеки механізми захисту від ймовірних загроз цим каналом. Для отримання надійного контролю над миттєвим обміном повідомленнями в корпоративному середовищі виконайте п'ять таких вимог.

Виберіть одну платформу для миттєвого обміну повідомленнями. Це полегшить роботу служби підтримки і зменшить ймовірність того, що співробітники будуть користуватися аналогічними службами інших постачальників. Якщо потрібно надійніше обмежити наявний у користувачів

вибір, можна за-блокувати порти, використовувані популярними службами миттєвого обміну повідомленнями

Визначте параметри захисту, що задаються при розгортанні служби миттєвого обміну повідомленнями. Обов'язково закрити можливість передачі і прийому файлів.

Визначте принципи встановлення нових контактів. Запропонувати користувачам не приймати за замовчуванням будь-які запрошення до спілкування.

Поставте стандарти вибору паролів. Вимагайте від співробітників, щоб їх паролі до служби обміну повідомленнями відповідали стандартам вибору надійних паролів, які прийняті для паролів, службовців для входу в систему.

Складіть рекомендації по використанню служби миттєвого обміну повідомленнями. Сформулюйте для користувачів служ-би миттєвого обміну повідомленнями оптимальні принципи роботи з нею, підкріпивши рекомендації обґрунтованими до-водами.

Телефонія. У разі корпоративної телефонії.

Необхідно, щоб користувачі крім фізичного телефону нічого не знали про пристрій телефонної мережі і використовуване обладнання.

У політиці ІБ необхідно жорстко прописати:

щоб ніяких перемикань і переадресацій дзвінків на інших співробітників компанії ніхто не здійснював, якщо кінцевий користувач сам не чекає на дзвінок (можна завжди запитати, чи чекає конкретний користувач дзвінка від такої-то особи або компанії в даний момент);

заборонити називати прямі міські корпоративні і мобільні номери і внутрішні номери як конкретних осіб, так і підрозділів;

заборонити фразу «Мені з Вашими айтішниками потрібно поговорити» або «Мені б головного бухгалтера почути» здійснювати переадресацію дзвінка. Завжди уточняти питання і, після безпосередньої розмови з даним співробітником або відділом, відмовити або переадресувати дзвінок, якщо він очікуваний;

заборонити називати прізвищ співробітників, особливо керівників і відповідальних за ту чи іншу ділянку роботи;

жорстко прописати, що тільки наші спеціалісти можуть надавати допомогу по телефону.

Крім того, політика безпеки має містити:

Чітке визначення посадовою особою графіку, а також глибину аналізу програмного забезпечення, встановленого на веб-серверах систем, а також клієнтських частин систем, встановлених у клієнтів. Також періодичності оновлення програм-ного забезпечення і встановлення оновлень безпеки та щодо усунення вразливостей програмного забезпечення, операцій-них систем, іншого програмного забезпечення, яке використовується під час підготовки та обміну документами.

Обов'язковість багатофакторної автентифікації.

Розробити порядок дій працівників та клієнтів підприємства у випадках виявлення несанкціонованого доступу (чи підозри в спробі доступу) до рахунку.

Визначити уповноважених осіб, які відповідатимуть за взаємодію з правоохоронними органами, та порядок такої взаємодії у разі виявлення несанкціонованих операцій, здійснених із використанням систем. Під час здійснення за-ходів щодо оперативного обміну інформацією, розслідувань фактів шахрайства, протидії/попередження злочинам, поданні інформації, заяв за вказаними фактами до правоохоронних органів, організаціям слід дотримуватись вимог законодавства з питань захисту даних та інших правил безпеки.

Постійно проводити роз'яснювальну роботу серед співробітників та клієнтів щодо обов'язкового дотримання вимог з питань захисту інформації на робочих місцях, де встановлено систему, а також щодо належного поводження з носіями ключової інформації системи (розроблення та доведення до клієнтів типових рекомендацій/інструкцій для роботи на комп'ютерах, де встановлюються клієнтські частини системи, правил використання та зберігання носіїв ключової інформації тощо).

Щомісячно проводити навчальні фішинг-атаки для перевірки виконання персоналом усіх вимог керівництва, також розробити систему штрафів та інших стягнень для працівників. Якщо були виявлено порушення вимог, то на порушника накладається штраф.

Розробити пам'ятку для клієнтів з такими застереженнями:

- Унеможливлюйте відвідування Інтернету з персонально-го комп'ютера, на якому здійснюється підготовка та відправка документів. Не відвідуйте сайтів сумнівного змісту та будь-яких інших інтернет-ресурсів невиробничого

характеру (соціальні мережі, конференції та чати, телефонні сервіси т.п.). Не читайте пошту та не відкривайте поштових вкладень до електронних листів, які надійшли від невідомих або підозрілих адресатів. Не слід здійснювати установку та оновлення будь-якого програмного забезпечення не з офіційних сайтів виробників.

- Налаштовуйте окремо мережеве обладнання корпоративних і персональних комп'ютерів. Доступ до мережі Інтернет обмежуйте "білим списком" сайтів з усіх робочих місць, на яких здійснюється підготовка, підписання та відправлення платіжних документів. У "білий список" мають включатися виключно перевірені сайти самого підприємства, банків, податкової служби, інших державних органів, доступ до яких необхідний у виробничому процесі, сервери оновлень системного та антивірусного програмного забезпечення.

- Мінімізуйте кількість користувачів комп'ютерів, на яких здійснюється підготовка та відправка документів. Доцільно обмежити фізичний доступ до персональних комп'ютерів, на яких здійснюється підготовка та відправка документів (надавати доступ виключно відповідальним працівникам, які безпосередньо уповноважені та мають право проводити роботи з програмним забезпеченням системи).

- Використовуйте сучасне антивірусне забезпечення, оновлюйте та проводьте антивірусну перевірку на комп'ютерах. Наголошуємо, що шкідливе програмне забезпечення здатне перехоплювати будь-які дані з банків, персональних комп'ютерів клієнтів та/або особистих даних держателів та зберігати/поширювати таку інформацію для подальшого не-санкціонованого використання сторонніми особами злочинним шляхом.

- Забезпечуйте своєчасне встановлення оновлень безпеки операційної системи, браузерів та програмного забезпечення комп'ютерів. Необхідно встановити надійні паролі доступу на вхід до персонального комп'ютера, забезпечити періодичну зміну цих паролів.

- Не допускайте несанкціонованого використання ключів кваліфікованого електронного підпису, зберігайте ключові носії у спосіб, що виключає несанкціонований доступ до них. Генерацію секретних ключів слід виконувати тільки самостійно. Нікому не повідомляти та не передавати паролі до особистих секретних ключів. Не записувати і не зберігати па-ролі разом з носієм ключа."

Працівникам потрібні постійні нагадування про важливість дотримуватися правил, щоб захистити інформаційні активи компанії. Одночасно ті, хто розробляє правила, мають реагувати на відгуки працівників. Робота ніколи не закінчується. Як зазначає Microsoft: "безпека - це подорож, це не та проблема, яку можна раз і назавжди вирішити" [34].

3.2. Рекомендації по роботі з персоналом

Поряд з основними вимогами існує ряд усталених рекомендацій, які будуть корисні, тим хто впроваджує систему інформаційної безпеки:

- найголовніше це навчання персоналу, адже якщо персонал не буде навчений основам інформаційної безпеки, то систему менеджменту інформаційної безпеки буде вкрай не ефективна.

- засоби захисту мають бути прості для технічного обслуговування і «прозорі» для користувачів;

- кожен користувач має мати мінімальний набір привілеїв, необхідних для роботи;

- можливість відключення захисту в особливих випадках, наприклад коли механізми захисту реально заважають виконанню робіт;

- незалежність системи захисту від суб'єктів захисту

- розробники мають припускати, що користувачі мають найгірші наміри (ворожість оточення), що вони будуть робити серйозні помилки і шукати до шляху обходу механізмів захисту;

- відсутність на підприємстві засобів інформації про існування механізмів захисту [22].

Заходи, що вживаються захисту мають бути адекватні ймовірності здійснення даного типу загрози і потенційному збитку, який може бути нанесений в тому випадку, якщо за-гроза здійсниться (включаючи витрати на захист від неї).

Вибираючи захисні заходи, доводитися враховувати не тільки прямі витрати на закупівлю обладнання і програм, але і витрати на їх впровадження, зокрема - на навчання та пере-підготовку персоналу. Важливою обставиною є сумісність нового засобу зі сформованою апаратно-програмної структурою об'єкта.

На думку фахівців, організаційні заходи відіграють вели-ку роль в створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей в значній мірі обумовлені не технічними аспектами, а зловмисними діями, недбальством, недбалістю і халатністю користувачів або персоналу захисту.

Сформована сукупність правових, організаційних та інженерно - технічних заходів виливається в відповідну політику безпеки, відображену в концепції інформаційної безпеки підприємства.

Концепція розробляється на основі аналізу сучасного стану інформаційної безпеки, джерел, видів загроз і динаміки їх розвитку. Концепція системи захисту є систематизований виклад цілей, завдань, принципів і способів досягнення інформаційної безпеки.

Концепція інформаційної безпеки має містити:

- загальну характеристику об'єкта захисту (опис складу, функцій і існуючої технології обробки інформації);

- формулювання цілей створення системи захисту, основ-них завдань забезпечення інформаційної безпеки і шляхів досягнення цілей;

- основні класи загроз інформаційній безпеці, які беруть-ся до уваги при розробці підсистеми захисту;

- основні принципи та підходи до побудови системи забезпечення інформаційної безпеки, заходи, методи і засоби досягнення цілей захисту.

Концепція являє собою офіційну прийняту систему по-глядів на проблему інформаційної безпеки та шляхи її вирішення з урахуванням сучасних тенденцій розвитку інформатизації медичної установи. Вона є методологічною основою політики в розробці практичних заходів щодо її реалізації.

Концепції соціальної інженерії, в основі підходів лежить системність, підкріплена методологією і аналізом, яка і дозволяє поєднувати технологічну інноваційність, інженерну точність розрахунків з соціально-психологічним моделюванням. Майстерне володіння цими інструментами є запорукою успішного вибудовування поведінкової моделі людей, «добровільно» і «самостійно» діючих в потрібному соціальному інженеру напрямку. Інтелектуальним тренажером для майстрів цього жанру може стати практично будь-яка предметна область, що припускає використання людського фактора і формування морального клімату, який спонукає людей до запланованих дій. Тут

і політичне лобіювання, і консалтинг, і рекрутмент, і управління проектами, і особистісне/організаційне проектування, і вибудовування «зовнішньо-політичних» відносин.

У визначеннях соціальній інженерії ми говоримо про експлуатацію людського фактора, впливом на який і займається соціальний інженер для отримання необхідної йому інформації. Охарактеризуємо людський фактор, що є основою моделі загроз пов’язаної з роботою персоналу.

Людський фактор (англ. Humanfactor) – історично сформована в суспільстві сукупність основних соціальних якостей людей:

- ціннісні орієнтири;
- моральні принципи;
- норми поведінки в сфері праці, дозвілля, споживання;
- життєві плани;
- рівень знань та інформованості;
- характер трудових і соціальних навичок;
- установки і уявлення про особистісно-значущі елементи соціального життя: про соціальну справедливість, про права і свободи людини, про громадянський обов'язок тощо.

Інше, часто застосовуване визначення людського факто-ра свідчить, що це стійкий вираз, яким позначають психічні здібності людини як потенційне і актуальне джерело (причину) інформаційних проблем (колізій) при використанні цією людиною сучасних технологій.

Далі, говорячи про соціальну інженерію, ми маємо на увазі маніпулювання людиною або групою людей з метою злому систем безпеки і викрадення важливої інформації. В та-кому випадку соціальний інженер – це зловмисник (шахрай), що здійснює атаку на людину, яка є частиною системи «люди-на-комп'ютер».

Відповідно до викладеного, розглянемо наступні загрози, які загрожують інформаційній безпеці.

Найбільш частими та небезпечними є ненавмисні помилки користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи. Іноді такі помилки є загрозами (невірно введені дані, помилка в програмі, котра викликає колапс системи), іноді вони створюють

ситуації, якими не лише можуть скористатися зловмисники, а які самі по собі становлять безпосередню небезпеку об'єкта.

У цілому ж, за результатами проведених фахівцями з інформаційної безпеки досліджень, понад 65 % шкоди, яка зав-дається інформаційним ресурсам, є наслідком ненавмисних помилок. Пожежі та землетруси, тобто загрози природного характеру, трапляються набагато рідше. Саме тому, доцільним є акцентування уваги на більшому впровадженні комп'ютерних систем для забезпечення безпеки.

Наступними, за розміром шкоди, можна виділити крадіжки. У більшості випадків, суб'єктами вчинення даних дій були штатні працівники підприємства, які є добре обізнаними у роботі інформаційної системи, а також заходів безпеки.

У найбільш загальному плані діями ображених співробітників керує намагання нанести шкоду підприємству, в якій вони працювали, і яка, на їхню думку, їх образила. Така образа може знайти відображення у вчиненні наступних дій:

- пошкодження обладнання;
- вбудовування логічної бомби, яка з часом руйнує програми і дані;
- введення невірних даних;
- знищення даних;
- зміна даних;
- модифікація даних;
- надання доступу до даних із обмеженим доступом тощо.

Ображені співробітники обізнані з порядками на підприємстві і здатні нашкодити вельми ефективно. Необхідно слідкувати за тим, щоб при звільненні співробітника його права доступу до інформаційних ресурсів були повністю обмежені, а після його звільнення змінені всі паролі доступу до внутрішньої мережі. Більш того, слід обмежити його спілкування із особами, які мають доступ до важливої інформації.

До антропогенних джерел загроз відносять суб'єктів, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Тільки в цьому випадку можна говорити про заподіяння збитку. Ця група джерел загроз найбільш численна та представляє найбільший інтерес із точки зору організації захисту, так як дії суб'єкта завжди можна оцінити, спрогнозувати та прийняти адекватні заходи.

Методи протидії у цьому випадку керовані й напряму залежать від волі організаторів захисту інформації.

Антропогенним джерелом загроз можна вважати суб'єкта, що має доступ (санкціонований або несанкціонований) до ро-боти зі штатними засобами об'єкта, що підлягає захисту. Суб'єкти (джерела), дії яких можуть привести до порушення безпеки інформації, можуть бути як зовнішніми, так і внутрішніми. Зовнішні джерела можуть бути випадковими або навмисними та мати різний рівень кваліфікації.

Внутрішні суб'єкти (джерела), як правило, представляють собою висококваліфікованих спеціалістів у галузі розробки та експлуатації програмного забезпечення та технічних засобів, знайомі зі специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання та технічних засобів мережі.

Необхідно враховувати також, що особливу групу внутрішніх антропогенних джерел складають особи з порушеною психікою та спеціально впроваджені та завербовані агенти, які можуть бути з числа основного, допоміжного та технічного персоналу, а також представників служби захисту інформації. Дана група розглядається у складі перелічених вище джерел загроз, але методи протидії загрозам для цієї групи джерел можуть мати свої відмінності.

Виділяють кілька основних правил, якими користуються соціальні інженери, які не дуже сильно змінюються з часом і завжди ефективні:

• дуже багато людей дивляться на зовнішню атрибути-ку не звертаючи уваги на суть, тобто манера поведінки, зовнішній вигляд, як себе позиціонує людина і т.д. Необхідно в собі розвивати навички хорошого актора, що гарантує 50% успіху будь-якої задумки, а якщо сюди додати навички психології, тоді це 100% соціальний зломщик;

• більшість людей негативно залежні від свого почуття власної значущості. Такі люди вразливі для атак. Досить трохи потішити, щоб вони виконали всі побажання. Заздрість взагалі – це корінь усіх інтриг. Олександр Розенбаум каже, що заздрість таке відчуття, яке «з дуже хороших людей робить дуже великих скотів і за дуже короткий час». На підприємстві нескладно розпізнати співробітника схильного до негативної заздрості від почуття власної

значущості. Дуже часто, зробивши такому співробітникові справедливе зауваження по роботі, можна побачити реакцію, що властива такому суб'єкту, який не знає, як швидко вирішити ситуацію, а починає наводити аргументи і порівняння. Не варто сподіватися на лояльність до організації з боку такого типу співробітників.

• багато людей хочуть, щоб все хороше, що тільки може з ними в житті статися, сталося якомога швидше і бажано з мінімальними зусиллями з їх боку (наприклад, маси ошуканих вкладників МММ, бажаючих за невеликі гроші отримати значний добробут).

• багато людей – це істоти, жадібні до грошей. Приклад – «листи щастя», в яких йдеться про те, що, перерахувавши 30-50 гривень на цей рахунок, можливо отримати через тиждень в 10 разів більше.

Слід відзначити, що кваліфікація антропогенних джерел загроз безпеці інформації відіграє важливу роль для оцінки їхнього впливу та враховується при ранжируванні джерел за-гроз. Розгляд даних загроз здійснювався з метою продемонструвати, що знання загроз і уразливих місць дозволить організувати адекватну систему управління інформаційною безпекою.

Висновки до розділу 3

У даному розділі розроблено рекомендації до політики безпеки та по роботі з персоналом.

Встановлено, що найбільшу шкоду для підприємства призводить діяльність в Інтернеті. З огляду на це у політиці ІБ необхідно чітко прописати дії користувачів у випадках: отримання електронного повідомлення від невідомого адресата; появи діалогових вікон, які дуже властиві операційній системі. Має бути встановлено категоричну заборону на Online-ігри, обмін/скачування будь-якого контенту, що може бути порушенням авторських прав. Також мають бути прописані чіткі правила по роботі з документами і магнітними накопичувачами, які з тих чи інших причин вже не потрібні. Обов’язковим є інформування користувачів про те, що при виникненні проблем вони можуть робити запити про допомогу тільки у фахівців служби підтримки.

Зазначено, що людський фактор – історично сформована в суспільстві сукупність основних соціальних якостей людей: ціннісні орієнтири, моральні

принципи, норми поведінки в сфері праці, дозвілля, споживання, життєві плани, рівень знань та інформованості, характер трудових і соціальних навичок, установки і уявлення про особистісно-значущі елементи соціального життя: про соціальну справедливість, про права і свободи людини, про громадянський обов'язок тощо.

Розглянуто основні загрози антропогенного характеру, на основі яких запропоновано рекомендації до політики інформаційної безпеки для попередження виникнення таких загроз та відповідних їх наслідків.

ВИСНОВКИ

У результаті аналізу міжнародних стандартів з управління інформаційною безпекою та безпекою інформаційних технологій зроблено такі висновки.

Встановлено, що в стандарті ISO 27001 міститься опис кроків зі створення, супроводу і вдосконалення СУІБ. Стандарт декларує ризик-орієнтований підхід, який дозволяє вибрати необхідні заходи і засоби захисту, які найкращим чином відповідають потребам і інтересам бізнесу. За результатами впровадження стандарту ISO / IEC 27001 компанія може пройти сертифікацію.

Стандарт COBIT 2019 «Впровадження і оптимізація рішення по керівництву інформацією і технологіями» охоплює всю діяльність компанії і дозволяє широко поглянути на управління IT та ІБ. Стандарт носить високорівневий характер, тобто говорить, що має бути досягнуто, але не пояснює, як. За допомогою принципів COBIT 2019 можна мінімізувати ризики і контролювати повернення інвестицій в IT і засоби інформаційного захисту.

Рекомендації ITIL визначають кроки для забезпечення безпеки IT на рівні процесів. Крім того, бібліотека містить рекомендації з вибудовування суміжних процесів, наприклад, з управління інцидентами, що дозволяє комплексно поглянути на вибудовування процесів і їх інтеграцію в IT-середовище. Бібліотека ITIL корисна фахівцям, в завдання яких входить вибудовування процесу управління IT-послугами і інтеграція ІБ в цей підхід.

Зроблено висновок, що для якісної побудови системи ІБ потрібно агрегувати знання і поєднувати підходи, отримані з різних джерел, оскільки кожна система поглядів містить плюси і мінуси і вимагає адаптації до умов конкретної компанії. Фахівцям з інформаційної безпеки необхідно постійно вдосконалюватися, розширювати набір компетенцій і професійних знань, і прийняті за кордоном стандарти істотно допомагають в цьому.

З’ясовано, що стандарт ISO 27002 визначає організаційні аспекти менеджменту інформаційної безпеки і містить кращі практики впровадження процесів для підвищення ефективності організації інформаційної безпеки підприємства. Метою організації інформаційної безпеки підприємства є встановити основні рамки управління, що контролюють впровадження та функціонування інформаційної безпеки.

Проаналізовано напрями організації інформаційної безпеки відповідно до зазначеного стандарту: нормативно-організаційний, управління фізичними активами й управління безпекою інформаційно-телекомунікаційних систем.

Встановлено, що політика інформаційної безпеки має на меті забезпечити спрямування управління і підтримку інформаційної безпеки відповідно до вимог бізнесу та положень нормативно-правової бази.

У рамках діяльності з управління активами ідентифікують і класифікують активи підприємства, визначають відповідальності за їх безпеку. Заходи забезпечення фізичної безпеки та безпеки інфраструктури спрямовані на запобігання неавторизованому фізичному доступу, ушкодженню та вторгненню до службових приміщень підприємства, та втручанню в його інформацію.

Управління взаємодією та функціонуванням має на меті забезпечити правильну та безпечну роботу систем обробки та передачі інформації. Заходи з контролю доступу обмежують доступ неавторизованих користувачів до інформації та засобів її обробки. У рамках діяльності з придбання, розробки і супроводу систем гарантується, що заходи інформаційної безпеки є невід’ємною частиною інформаційних систем упродовж усього їхнього життєвого циклу.

За результатами дослідження та на основі аналізу найбільш поширених загроз інформаційній безпеці розроблено рекомендації до політики інформаційної безпеки щодо запобігання виникненню загроз внаслідок небезпечної діяльності в мережі Інтернет і негативного впливу людського фактору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001, Information technology— Security techniques— Information security management systems — Requirements [Online]. Available: https://www.iso.org/standard/65694.html.

2. COBIT-5 FRM 0813 (2009, Nov. 27). [Online]. Available: http://www.wikiitil.ru/books/Cobit-5_frm_rus_0813.pdf.

3. WIKI ITIL [Online]. Available http://www.wikiitil.ru/

4. ISO/IEC 27005:2011, ISO/IEC 27005, Второе издание, 2011, 94с.

5. ISO/IEC 27002-2013 Свод норм и правил управления ИБ [Online]. Available: http://cryptohistory.ru/pages/uib-05/.

6. Kevin D Mitnick and William L Simon. The art of deception : controlling the human element of security. Indianapolis, Ind.: Wiley Pub., 2002. isbn: 0471237124 9780471237129076454280X 9780764542800.

7. ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls [Online]. Available: https://www.iso27001security.com/html/27002.html

8. Robert B Cialdini. Inuence : science and practice. Harlow; London: Pearson Education, 2009. isbn: 9780205609994 0205609996 9780205663781 0205663788.

9. D. Gragg. \A multi-level defense against social engineering". In: SANS Reading Room, March 13 (2003).

10. Jamison W. Scheeres. Establishing the human _rewall: re-ducing an individual's vulnerability to social engineering. Air Force Institute of Technology., 2008.

11. James Randi. Why Magicians Are a Scientist's Best Friend- Wired Science - Wired.com. Mar. 2012. url: http://www.wired.com/wiredscience/2012/03/opinion-randimagic-scientists/

12. Verizon. 2012 Data Breach Investigations Report. Mar. 2012. url: http://www .verizonbusiness.com/resources/reports / rp _ data - breach - investigations - report -2012_en_xg.pdf.

13. Symantec. Internet Security Threat Report, Vol. 17 Main Report. Apr. 2012. url: http : / / www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf.

14. David Kennedy. The Social-Engineer Toolkit (SET). url: https : / / www . trustedsec . com / downloads / social engineer-toolkit/

15. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report 1 st Quarter 2012. July 2012. url: http://www.antiphishing.org/reports/apwg_trends_report_q1_2012.pdf

16. Gregory L. Orgill et al. \The urgency for e_ective user privacy-education to counter social engineering attacks on secure computer systems". In: ACM Press, 2004, p. 177. isbn: 1581139365. doi: 10.1145/1029533.1029577. url: http://portal.acm.org/citation.cfm?doid=1029533.1029577

17. G. Rossling and M. Muller. \Social engineering: a serious underestimated problem". In: SIGCSE bulletin 41.3 (2009), p. 384. url: http://atlas.tk.informatik.tu-darmstadt.de/Publications/2009/p384.pdf

18. Jack Wiles and Jennifer Jabbusch. Low Tech Hacking Street Smarts for Security Professionals. Syngress Media Inc, 2011. isbn: 9781597496650 1597496650

19. Concepts United Kingdom Ministry of Defence - The Development and Doctrine Centre (DCDC). A Guide To Red Teaming. May 2010. url: http : / / www . mod . uk / NR /rdonlyres/B0558FA0-6AA7-4226-A24C-2B7F3CCA9A7B/0/RedTeamingGuiderevised12Feb10Webversion

20. Mike Spykerman. Typical spam characteristics - How to e_ectively block spam and junk mail. 2003. url: http://www.policypatrol.com/spam-filter-article.htm.

21. IETF. RFC 5322 - Internet Message Format. url: https://tools.ietf.org/html/rfc5322.

22. Sharan B Merriam. Fallstudien som forskningsmetod. Lund: Studentlitteratur, 1994. isbn: 9144390718 9789144390710.

23. Idar Magne Holme and Bernt Krohn Solvang. Forskningsme- todik : om kvalitativa och kvantitativa metoder. [Lund]: Studentlitteratur, 1997. isbn: 9144002114 9789144002118.

24. Mats Alvesson and Kaj Sk• oldberg. Tolkning och reektion : vetenskaps_loso_ och kvalitativ metod. Lund: Studentlitteratur, 1994. isbn: 9144381611 9789144381619.

25. Michael Workman. \Gaining Access with Social Engineering: An Empirical Study of the Threat". In: Information Systems Security 16.6 (Dec. 2007), pp. 315{331. issn: 1065- 898X, 1934-869X. doi: 10.1080/10658980701788165.

26. Malcolm Pattinson et al. \Why do some people manage phishing e-mails better than others?" In: Information Management & Computer Security 20.1 (2012), pp. 18{28. issn: 0968-5227. doi: 10.1108/09685221211219173.

27. Tom N. Jagatic et al. \Social phishing". In: Commun. ACM 50.10 (Oct. 2007), 94{100. issn: 0001-0782. doi: 10.1145/ 1290958.1290968. url: http://doi.acm.org/10.1145/1290958.1290968

28. Tim Thornburgh. \Social engineering: the "Dark Art"". In: Proceedings of the 1st annual conference on Information security curriculum development. InfoSecCD '04. New York, NY, USA: ACM, 2004, 133{135. isbn: 1-59593-048-5. doi: 10.1145/1059524.1059554. url: http://doi.acm.org/10.1145/1059524.1059554

29. R. Tims. Social Engineering: Policies and education a must". In: SANS Institute, February 16 (2001).

30. ISO/IEC. ISO/IEC 27002:2005 - Information technology Security techniques - Code of practice for information security management. Oct. 2005.

31. Sarah Granger. Social Engineering Fundamentals, Part I: Hacker Tactics | Symantec Connect Community. Dec. 2001. url: http://www.symantec.com/connect/articles/

32. ISO/IEC. ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements. Oct. 2005.

33. S_a hackas du utan teknik - IDG.se. Apr. 2012. url: https://www.idg.se/2.1085/1.440154/sa-hackas-du-utanteknik

34. Manpower Work Life. Fyra av tio bryter mot IT-policynp_a jobbet. Oct. 2012. url: http://www.manpower.se/mpnet3/Content.asp?NodeID=5958