можуть надати владі тимчасові переваги, але ними треба вміти грамотно скористатися.

Список використаних джерел:

1. Осипенко А. Л. Боротьба зі злочинністю в глобальних комп'ютерних мережах: Міжнародний досвід: монографія. М., 2004. С.185.
2. Ефективне попередження злочинності: в ногу з новітніми досягненнями / Матеріали Десятого Конгресу Організації Об'єднаних Націй з профілактики злочинності і поводження з правопорушниками: A / CONF.187 / 10. Відень, 10–17 квітня 2000 року, п. 5.
3. Будапештська Конвенція про комп'ютерні злочини: [Електронний ресурс]. – Режим доступу: https://rm.coe.int/1680081580

Ключові слова: інтернет ресурси, заборонений контент, кіберзлочин, інформаційні технології.

Ключевые слова: интернет ресурсы, запрещенный контент, киберпреступление, информационные технологии.

Keywords: internet resources, prohibited content, cybercrime, information technology.

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

Пальчук Андрій Вікторович
Національний університет «Одеська юридична академія»,
студент 4 курсу факультету кібербезпеки
та інформаційних технологій

РОЗРОБКА КОМПЛЕКСУ ЗАХИСНИХ ЗАХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Конфіденційна інформація входить в сферу підвищеного інтересу конкуруючих компаній. Для недобросовісних конкурентів, корупціонерів та інших зловмисників особливий інтерес представляє інформація про склад менеджменту підприємств, їх статус та діяльності фірми [1].

Термін «безпека інформації» описує ситуацію, яка виключає доступ для перегляду, модерації і знищення даних суб'єктами без наявності відповідних прав. Це поняття включає забезпечення захисту від витоку і крадіжки інформації за допомогою сучасних технологій та інноваційних пристроїв.

Захист інформації включає повний комплекс заходів по забезпеченню цілісності та конфіденційності інформації за умови її доступності для користувачів, що мають відповідні права.

Цілісність – поняття, що визначає збереження якості інформації та її властивостей.

Конфіденційність передбачає забезпечення секретності даних і доступу до певної інформації окремим користувачам.

Доступність – якість інформації, що визначає її швидке і точне знаходження конкретними користувачами.

Мета захисту інформації – мінімізація шкоди внаслідок порушення вимог цілісності, конфіденційності та доступності.

Керівництво підприємства або організації має розробити та впровадити концепцію щодо забезпечення інформаційної безпеки. Цей документ є основоположним для розробки внутрішніх регламентів і системи захисних заходів. Розробку політики безпеки часто доручають запрошеним експертам щодо захисту інформації, здатним провести аудит як інформаційної системи, так і організаційної структури компанії і її бізнес-процесів і розробити актуальний комплекс заходів щодо захисту інформації.

Технічні заходи можуть перешкоджати людям робити несанкціоновані дії, але не можуть перешкоджати їм робити те, що дозволяють їм виконувати їхні робочі функції. Таким чином, щоб запобігти порушенню довіри, а не просто відшкодувати збиток, який виникає, слід залежати, перш за все, від усвідомлення людьми того, що роблять інші люди в організації. Але навіть технічно обґрунтована система з інформованим і пильним управлінням та користувачами не може бути позбавлена всіх можливих вразливостей. Залишковим ризиком

потрібно керувати за допомогою процедур аудиту, резервного копіювання та відновлення, що підтримуються загальною настороженістю та творчими реакціями. Більше того, організація повинна мати адміністративні процедури, щоб доводити особливі дії до відома того, хто може законно дізнатись про доцільність таких дій, і ця особа повинна фактично зробити запит.

Надалі концепція безпеки може стати основою для впровадження DLP-системи та інших програмних продуктів, що вирішують завдання захисту інформаційних ресурсів та інфраструктури компанії.

У концепції забезпечення інформаційної безпеки підприємства визначаються: інформаційні масиви компанії, що підлягають захисту, підстави захисту (встановлені законом або комерційні) [2].

Описуються програмні засоби, фізичні та електронні носії інформації, визначається їх цінність для компанії, критичність зміни або втрати. Цей розділ готується в тісній взаємодії з усіма підрозділами компанії. Система оцінки інформації повинна припускати і установку рівня доступу співробітників до ресурсів; основні принципи захисту інформації.

Зазвичай до них відносяться конфіденційність, комерційна доцільність, відповідність вимогам законодавства. Стратегія забезпечення інформаційної безпеки компанії цілком і повністю будується на цих принципах. Крім того, необхідно визначити політики і правила, ґрунтуючись на яких вибудовується інформаційна система компанії і загальна система захисту інформації; модель загроз інформаційній безпеці, релевантна для компанії в цілому і її окремих бізнес-одиниць, а також модель гіпотетичного порушника. Їм може виявитися конкурент, хакер, але частіше за все інсайдер.

Концепція сама по собі не вирішує завдання відповідальності співробітників компанії за неправомірне поводження з інформацією, в тому числі за її розголошення. Для вирішення цього завдання необхідно впровадити додаткову систему

організаційних заходів захисту інформації, які включають інформування, ознайомлення під розпис, внесення в трудові договори відповідних положень про захист інформації, що становить комерційну таємницю.

Після розробки концепції необхідно приступати до її впровадження. Система пропонованих заходів повинна пройти узгодження у всіх причетних підрозділах компанії, так як питання бюджетування завжди обмежує можливості щодо захисту інформації, складності проведених заходів і придбання програмних продуктів.

Забезпечення безпеки повинно ґрунтуватися на одночасному застосуванні всього комплексу заходів, передбачених законом або пропонованих фахівцями. Технічні та організаційні заходи необхідно співставляти з можливостями організації та інформаційної системи [3].

Система заходів, рекомендована для більшості компаній, перед якими стоїть питання захисту інформації, покликана забезпечити дотримання основних ознак її безпеки:

• доступність відомостей. Під цим визначенням розуміється можливість і для авторизованого суб'єкта в будь-який час отримати необхідні дані, і для клієнтів в регулярному режимі отримувати інформаційні послуги;

• цілісність інформації. Це означає її незмінність, відсутність будь-яких сторонніх, неавторизованих втручань, спрямованих на зміну або знищення даних, порушення системи їх розташування;

• конфіденційність або абсолютна недоступність даних для неавторизованих суб'єктів;

• відсутність відмови або неможливість заперечувати приналежність дій або даних;

• автентичність або можливість достовірного підтвердження авторства інформаційних повідомлень або дій в системі.

До технічних засобів і заходів забезпечення інформаційної безпеки відносяться не тільки програмні продукти, наприклад,

DLP-системи, а й інші інструменти, що знаходяться в розпорядженні компанії [4].

Заходи захисту інформації з технічної точки зору повинні спиратися на модель побудови інформаційної системи підприємства, що дозволяє вибудувати оборону проти зазіхань на конфіденційні відомості.

Встановлення політики безпеки є основною відповідальністю керівництва в організації. Керівництво зобов'язане зберігати та захищати активи та підтримувати якість послуг. З цією метою він повинен запевнити, що операції проводяться розсудливо, зважаючи на реалістичні ризики, що виникають внаслідок надійних загроз. Цей обов'язок може бути виконаний шляхом визначення політики високого рівня безпеки, а потім переведення цієї політики в конкретні стандарти та процедури відбору та виховання персоналу, перевірки та аудиту операцій, складання планів дій на випадок надзвичайних ситуацій тощо. За допомогою цих дій керівництво може запобігти, виявити та відновити втрати. Стягнення залежить від різних видів страхування: резервних копій, резервних систем та сайтів обслуговування, самострахування за рахунок резервів готівки та придбаної страховки для компенсації витрат на стягнення.

Список використаних джерел:

1. Семененко В. А. Информационная безопасность: Учебное пособие. 2-е изд., стереот. – М.: МГИУ, 2005. – 215 с.

2. Гайворонський М.В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с.

3. Дронь М.М., Малайчук В. П., Петренко О. М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.

4. Сороковская А. А. Информационная безопасность предприятия: новые угрозы и перспективы [Электронный ресурс]. – Режим доступа: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032–035.pdf.

Ключові слова: Захист, інформаційна безпека, організація, безпека організації.

Ключевые слова: Защита, информационная безопасность, организация, безопасность организации.
Keywords: Protection, information security, organization, security of the organization.
***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*

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

Саніцька Інна Валеріївна
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ СИСТЕМИ IOS: ПРОБЛЕМИ РЕАЛІЗАЦІЇ

Безпека системи є головною складовою зменшення кількості злочинів, здійснюваних у кіберпросторі. Поява сучасних технологій та стрімкий розвиток IT-сфери створює сприятливе середовище для вибору користувачами новітніх засобів для реалізації найрізноманітніших задач, включаючи соціальні мережі та спілкування.

Однією з найбезпечніших мобільних операційних систем вважається iOS. iOS – це мобільна операційна система для смартфонів, електронних планшетів, а також програвачів і деяких інших пристроїв, що розробляється і випускається американською компанією Apple [1].

Оскільки смартфони стають все більш поширеними по всьому світу, компаніям неминуче доводиться боротися з проблемами, пов'язаними з безпекою та конфіденційністю цих пристроїв. технологія збереження конфіденційності вдосконалюється, проблеми з конфіденційністю користувачів не були повністю розглянуті самою технологією. Відповідні регуля-