УДК 004.056.5

магістр Д.В. Малєєва
ДВНЗ «Національний гірничий університет»

ОРГАНІЗАЦІЙНІ ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ АКТИВІВ ОРГАНІЗАЦІЇ ВІД АНТРОПОГЕННИХ ЗАГРОЗ

У роботі розглянуться організаційні заходи захисту інформаційних активів, що необхідні для запобігання витоку інформації від антропогенних загроз.

Антропогенними джерелами загроз у сфері інформаційної безпеки виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові. Ця група представляє великий інтерес з точки зору організації захисту, так як дії суб'єкта завжди можна оцінити, спрогнозувати і прийняти адекватні заходи. Методи протидії в цьому випадку керовані і залежать від організаторів захисту інформації.

В якості антропогенного джерела загроз можна розглядати суб’єкт, що має доступ (санкціонований або несанкціонований) до роботи зі штатними засобами об'єкта. Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішні, так і внутрішні.

Розглянемо внутрішні суб'єкти (джерела), які, як правило, являють собою:

1) основний персонал (користувачі, програмісти, розробники);

2) представники служби захисту інформації;

3) допоміжний персонал (прибиральники, охорона);

4) технічний персонал (життєзабезпечення, експлуатація).

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

Людський фактор здатний «звести нанівець» будь-які найбільш витончені механізми безпеки. Це підтверджується численними статистичними даними, що свідчать про те, що переважна більшість інцидентів порушення безпеки пов'язана з діяльністю співробітників організації. Не дивно, що робота з персоналом є головним механізмом у системі захисту інформації.

Ключові принципи і правила управління персоналом з урахуванням вимог інформаційної безпеки визначені в міжнародному стандарті ISO/IEC 27001 і зводяться до необхідності виконання певних вимог безпеки, підвищення обізнаності співробітників і застосування запобіжних заходів до порушників. Наведемо основні:

1. Відповідальність за інформаційну безпеку включена в посадові обов'язки співробітників, включаючи відповідальність за виконання вимог політики безпеки, за ресурси, процеси та заходи щодо забезпечення безпеки.

2. Проводяться відповідні перевірки співробітників при прийомі на роботу, включаючи характеристики і рекомендації, повноту і точність резюме, освіту та кваліфікацію, а також документи, що засвідчують особу.

3. Підписання угоди про нерозголошення конфіденційної інформації кандидатом має бути обов'язковою умовою роботу прийому на.

4. Вимоги інформаційної безпеки, до співробітника описуються у трудових угодах. Там же має бути прописана відповідальність за порушення безпеки.

Головною умовою ефективної роботи з персоналом є узгоджена робота служби безпеки у різних напрямках, а саме внутрішня безпека, інформаційна безпека, правова безпека, технічна та інше. Та тісна взаємодія служби безпеки з іншими структурними підрозділами організації.

Головною метою організації процесу управління інформаційною безпекою, з одного боку, є виявлення осіб схильних до обману, а з іншого - здатність створення єдиної команди перевірених співробітників. Саме для

цього проводяться організаційні та організаційно-технічні заходи, використовуються особисті спостереження та бесіди.

Організаційні заходи, які проводяться в організації, повинні включати в себе:

– Регламентацію внутрішньо - корпоративних процедур, в тому числі розробку нормативних документів;

– Організацію контролю за діяльністю компанії;

– Навчальну та пояснювальну роботу з співробітниками;

– Профілактичну роботу з співробітниками(виявлення осіб, схильних до різноманітних правопорушень, роз'яснення наслідків правопорушень та ін.).

Важливу роль для забезпечення інформаційної безпеки відіграє обізнаність користувачів в питаннях безпеки та правила безпечної з точки зору захисту інформації поведінки. Основну роль тут відіграють менеджери організації.

Повинно проводитися навчання та контролювання знань користувачів з наступних питань:

– політика безпеки організації;

– правила вибору, зміни та використання паролів;

– правила отримання доступу до ресурсів інформаційної системи;

– правила поводження з конфіденційною інформацією;

– процедури інформування про інциденти, вразливості, помилки та збої програмного забезпечення та ін.

В організації повинно бути розроблено положення щодо захисту конфіденційної інформації та відповідні інструкції. Ці документи повинні визначати правила та критерії для категорювання інформаційних ресурсів за ступенем конфіденційності (наприклад, відкрита інформація, конфіденційна, суворо конфіденційна), правила маркування конфіденційних документів і правила поводження з конфіденційною інформацією, включаючи режими

зберігання, способи звернення, обмеження щодо використання та передачі третій осторонь і між підрозділами організації.

Повинні бути визначені правила надання доступу до інформаційних ресурсів, впроваджені відповідні процедури і механізми контролю, в тому числі авторизація та аудит доступу.

Також в організації повинен бути розроблений дисциплінарний процес, який буде працювати відносно порушників безпеки і який буде передбачати розслідування та ліквідацію наслідків інцидентів.

Треба розуміти, що успішна реалізація перелічених підходів можлива тільки при існуванні в організації діючої системи управління інформаційною безпекою, яка характеризується, перш за все, наявністю діючої політики безпеки і організаційної структури, вистроєної у відповідності з цією політикою, а також наявністю процесів, процедур та механізмів контролю.

Перелік літератури:

1. Голубченко О.Л. Політика інформаційної безпеки. Луганськ:вид-во СНК ім. В. Даля. 2009

2. «Руководство по защите от внутренних угроз информационной безопасности» Владимир Скиба, Владимир Курбатов. «Питер», 2008.