Человеческий фактор, как основная опасность при защите информации

Куханова Анна Юрьевна
студентка
Московский городской университет управления Правительства Москвы, факультет государственного и муниципального управления, Москва, Россия
E–mail: anyuta.k@mail.ru

Защита информации в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются: массовое распространение средств электронной вычислительной техники; усложнение шифровальных технологий; необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой тайн; расширяющиеся возможности несанкционированных действий над информацией.

Кроме того, в настоящее время получили широкое распространение средства и методы несанкционированного и негласного добывания информации.

Поэтому особую роль и место в деятельности по защите информации занимают мероприятия по созданию комплексной защиты, учитывающие угрозы национальной и международной безопасности и стабильности, в том числе обществу, личности, государству, общественным институтам, суверенитету, экономике, финансовым учреждениям, развитию государства.

Основные методы и средства защиты информации зависят от типа информации, формы ее хранения, обработки и передачи, типа носителя информации, а также предполагаемого способа нападения и последствий его по влиянию на информацию (копирование, искажение, уничтожение).

В основном владелец информации не знает где, когда и каким образом будет осуществлено нападение, поэтому ему необходимо обнаружить сам факт нападения. Определение потенциальной ценности информации позволяет подумать в первую очередь о безопасности наиболее важных секретов, утечка которых способна нанести ущерб. При этом важно установить.

1. Какая информация нуждается в защите?
2. Кого она может интересовать?
3. Какова стоимость информации?
4. Какие элементы информации наиболее ценные?
5. Каков “срок жизни” этих секретов?
6. Во что обойдется их защита?

Как правило, человек является наименее надёжным звеном в системе защиты информации. Из всех известных удачных попыток преступлений в сфере компьютерной информации подавляющее большинство было совершено при помощи сообщников в учреждении, которое подвергалось атаке.

Для исключения самого слабого звена в информационной системе можно предложить следующие методы и средства защиты информации:

- ознакомить всех сотрудников с принципами защиты информации и принципами работы средств хранения и обработки информации.
- чётко классифицировать всю информацию по степени её закрытости и ввести правила обращения с документами ограниченного распространения.
- обязать сотрудников исполнять требования по защите информации, подкрепив это соответствующими организационными и правовыми нормами.
- обучать всех сотрудников современным средствам защиты информации.
- иметь в штате специалиста, профессионально разбирающегося в проблемах защиты информации.

- в ходе общих тренингов, поставив себя на место вероятного противника (конкурента), подумать, что он мог бы предпринять для получения несанкционированного доступа к вашей информации. Продумать ответные меры защиты.
- проводить обучающие психологические тренинги, которые способствовали выработки у сотрудников определённых алгоритмов ответа на компрометирующие вопросы, при которых возможна утечка информации.
- контроль, мониторинг и аудит деятельности сотрудников.
- обеспечение ответственности за несанкционированное разглашение.

Вопросы информационной безопасности, которые играют исключительно важную роль в управлении рисками организации, практически никогда не решаются настолько оперативно, чтобы учитывать все происходящие изменения.

Методы мониторинга деятельности персонала организации не только решают проблемы всестороннего контроля за поведением сотрудников, но и помогает выработать предупреждающие меры по предотвращению несанкционированного доступа к информации.

Литература

1. ФЗ №24 от 25 января 1995 года «Об информации, информатизации и защите информации».
2. Доронин А. "Бизнес-разведка". - М., 2004
3. Кирюшин Ю.Ф., Шатохин А.С., Поляков В.В. Подготовка специалистов в области информационной безопасности в АГУ. Тез. докл. Всерос. науч.-практ. конф. "Проблемы правового и организационно-технического обеспечения информационной безопасности России". Екатеринбург, 2001. С. 11-12
4. Мазуров В.А., Головин А.В., Поляков В.В. Информационная безопасность: основы правовой и технической защиты информации. Барнаул: Изд-во Алт. ун-та, 2005.
5. Материалы научно-практической конференции "Актуальные вопросы защиты информации: информационная безопасность Вологодской области". /30 марта 2006 года// Издательство «Официальный сайт Правительства Вологодской области»
6. Овчинский А.С. Нетрадиционные подходы противодействия организованной преступности на основе информационных технологий.// Издательство fact.ru.