ВОПРОСЫ ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Е.А. СВИРСКИЙ

Рассматривается применение организационно-административных мер и методов защиты в условиях функционирования информационной системы в учреждении, организации, на предприятии, связанных с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к ее утечке. Организационные меры — это относительно недорогие методы и средства защиты, которые доступны для освоения всеми субъектами хозяйствования и, которые, в состоянии решить многие проблемы защиты информации в организации.

В системе организационного обеспечения информационной безопасности выделяются два направления — направление, связанное с реализацией мер организационно-правового характера и направление, связанное с реализацией мер организационно-технического характера. Организационное обеспечение базируется на нормативно-правовой базе управления системой защиты информации. Рассматривается возможный вариант создания нормативно-правовой базы управления системой защиты информации и организации доступа к ней специалистов.

Основные проблемы, связанные с обеспечением защиты информационных ресурсов, являются следствием недостаточной компетентности, как обслуживающего персонала информационных систем, так и пользователей в вопросах обеспечения информационной безопасности. Человеческий фактор является едва ли не определяющим в обеспечении защиты информации в информационных системах каждой организации. Рассматриваются вопросы организации мероприятий по повышению общей культуры пользования информационными ресурсами населением в целом и соблюдением принципов и правил информационной безопасности в частности.

О ВОЗМОЖНОСТЯХ ПРОТИВОДЕЙСТВИЯ СОВРЕМЕННЫМ ВЫЗОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ю.И. ИВАНЧЕНКО, Е.А. СВИРСКИЙ

Вызовы:

– быстрые темпы обновления знаний и, соответственно, изменений технологий и средств информатизации;

– деградация классического образования;

– усиливающаяся зависимость бизнеса, обороноспособности, общественной жизни и т.д. от информационных технологий усиливают кадровый «голод» и требуют выработки новых подходов к формированию кадрового обеспечения информационной безопасности.

Эти новые подходы необходимо сформулировать в расчете на предотвращение (недопущение, упреждение) событий безопасности. Это по нашему мнению возможно путем:

– воспитания культуры информационной безопасности в максимально широкой общественной среде»;

– создания профессиональных институтов высочайшей квалификации, способных выполнять роль ведущих (локомотивов) в решении не только текущих или уже известных проблем информационной безопасности, но и (а может быть и в большей степени) будущих.

В условиях упомянутых вызовов:

– повышение культуры информационной безопасности представляется возможным через «управляемое» самообразование на корпоративном уровне в рамках «Программ повышения осведомленности»;

– исследование проблем ИБ и поиск путей их решения, а также упреждение от воздействия быстро развивающегося деструктивного программного обеспечения на основе

новейших технологий, необходима управляемая (заказная на основе выявления тенденций) система научных исследований в сфере информационной безопасности и т.п.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В НАЦИОНАЛЬНОЙ СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Н.С. РОМАНОВСКИЙ, В.Ф. ГОЛИКОВ

Электронный документооборот с каждым годом набирает обороты, он проникает во все сферы жизни, начиная с банковского сектора и заканчивая маленькими фирмами. В связи с тем, что в системе электронного документооборота передаются юридически значимые документы, которые имеют одинаковую юридическую силу с документами на бумажном носителе с подписью и печатью организации, то это позволяет упростить процедуру передачи конфиденциальной информации, упростить процедуру хранения информации, а подписание документа электронной цифровой подписью обеспечивает достоверность, целостность, конфиденциальность передаваемой информации. В связи с этим электронный документооборот позволяет экономить материальные, людские и временные ресурсы.

Естественно встает вопрос о безопасности данной системы. Проанализирована схема, алгоритм функционирования электронного документооборота, модель нарушителя, его мотивы и цели. Используя программный продукт Microsoft Security Assessment Tool для оценки системы информационной безопасности на объекте защиты, который представляет собой большую анкету, касающуюся инфраструктуры, приложений, операций и персонала, сделали вывод, что безопасность системы электронного документооборота находится на высоком уровне.

МЕТОДЫ ОЦЕНКИ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ТЕХНИЧЕСКИХ ОБЪЕКТОВ

Л.С. СТРИГАЛЕВ

Оценка качества средств защиты технических комплексов хозяйственных объектов приобретает, как известно, все более актуальный характер. Такие оценки необходимы на стадии разработки, при оптимизации средств защиты и в процессе их функционирования. При этом наиболее важна адекватность оценки качества на стадии функционирования объекта, особенно если это связано с риском техногенной катастрофы. Недоработки же при проектировании средств защиты объекта, как правило, приводят в основном к снижению качества и потенциальных возможностей этих средств.

В этой связи, очевидна необходимость разработки методов оперативной оценки состоянии средств защиты, ориентированных на предоставление оператору, ситуатору (роботу-управленцу) или лицу, принимающему решение адекватной информации о состоянии объекта. В идеале необходимы методы технической компьютерной томографии качества средств защиты. В рамках этих же методов должны строиться частные и обобщенные критерии средств защиты, включая их предельные характеристики.

Одним из путей разработки таких методов является использование меры Кульбака-Лейблера, которая представляет собой взвешенный логарифм отношения правдоподобия и обладает свойством аддитивности. В докладе на простом примере иллюстрируется применение этой меры для оценки качества функционирования некоторой гипотетической системы. Методы, основанные на данной мере, позволяют оценивать предельные возможности системы, а также путем введения КПД оценивать потери информации при ее поэтапной обработке и осуществлять оптимизацию, как в цепи поэтапной обработки информации, так и системы в целом. При этом используемые критерии оптимизации имеют взаимосвязь с традиционными классическими критериями оптимальности.