РАЗДЕЛ XX. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Бондаренко М.М., Бондаренко О.М., Костюкова Т.П.
 Организация информационной безопасности на рабочих местах

Уфимский государственный авиационный технический университет
 (Россия, Уфа)

doi:10.18411/lj-11-2018-175

idsp: lj-11-2018-175

Аннотация

В данной работе рассмотрены основные принципы построения защиты информации на автоматизированных рабочих местах, используемых в повседневной деятельности любой организации, использующей парк вычислительной техники.

Ключевые слова: защита информации, машинные носители информации, средства защиты информации, программное обеспечение.

Организация защиты информации в ежедневной деятельности организаций весьма актуальна, так при ее отсутствии может наблюдаться нарушение коммерческой тайны, даже потеря работоспособности предприятия[1], Причин утечки информации или угроз таких потерь множество, начиная от человеческого фактора, заканчивая слабым контролем ответственных лиц за техническую часть всей системы обеспечения безопасности информации (рис.1)[2].

Рисунок 1 – Трехмерная система защиты информации

Чаще всего угроза (рис.2) является следствием наличия уязвимых мест в защите информационных систем (таких как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Среди угроз необходимо выделить аспект информационной безопасности, характеризующийся такими понятиями, как доступность, конфиденциальность, целостность. Одной из наиболее часто применяемых классификаций угроз является: по причинам появления (стихийные, преднамеренные); по характеру воздействия (активные, пассивные); по расположению источников угроз (внешние, внутренние); по вероятности возникновения (весьма вероятные, вероятные, маловероятные); по величине ущерба (предельный, значительный, незначительный); по компонентам информационной системы (данные, программы, аппаратура, инфраструктура) [3-5].

Рисунок 2 – Угрозы потери информации (И-источники, О-отводы, П-перехват, ПЛТ-пользователи)

Основой математического описания защиты является модель системы защиты, в которой рассматривается взаимодействие множеств "области угроз" $T=\{t_i\}$, "защищаемой области" $O=\{o_j\}$ и "механизмов безопасности" $M=\{m_k\}$.

Взаимоотношения множеств «угроза-объект» образует граф $\{<T, O>\}$.

Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. В идеале каждый механизм защиты должен исключать соответствующий путь реализации угрозы $<t_i, o_j>$. Это достигается введением третьего набора M . Результатом является граф $\{<T, M, O>\}$.

Набор M в некоторой мере обеспечивают сопротивление злоумышленным действиям. При этом в графе ребро (t_i, o_j) обозначает незащищенный объект (уязвимое место). На данном этапе также определяют степень защищенности системы за счет сопоставления каждой дуге весового количественного коэффициента. Вводим понятие V -набора уязвимых мест, определяемое подмножеством декартова произведения $T*O$:

$v_r = <t_i, o_j>$. При этом декартово произведение $V*M$ определяет $B(b_l = <t_i, o_j, m_k>)$ - набор барьеров, которые представляют мероприятия осуществления угроз безопасности, перекрытые средствами защиты. В результате разработана система, состоящая из пяти векторов: $<T, O, M, V, B>$ и описывающая систему защиты внутренней информации организации с учетом наличия в ней уязвимостей. Таким образом, для систем защиты реализуется условие: для любой уязвимости информации имеется барьер, который устраняет эту уязвимость.

Прочность барьера $b_l = \langle t_i, o_j, m_k \rangle$ характеризует величину остаточного риска $Risk_l$ в отношении объекта o_j , при использовании механизма защиты m_k . Эта величина определяется по формуле:

$$Risk_l = p_k L_k (1 - R_k),$$

где p_l – вероятность угрозы; L_l – величина ущерба (уровень угрозы); R_l – степень сопротивляемости механизма защиты m_k , которая характеризует вероятность его преодоления.

Модель системы безопасности— это наиболее общая модель защиты автоматизированных рабочих мест, базирующаяся на том, что система безопасности должна иметь по крайней мере одно средство, обеспечивающее безопасность любого потенциального канала утечки информации.

Рассмотренные вопросы использования классификационного и формального подходов, методов анализа защищенности, нормативной документации, безусловно, не охватывают всего комплекса проблем, связанных с аттестацией безопасности АС. Но в тоже время они отражают основные направления необходимых исследований в этой области для повышения защищенности информации.

Методологическая база анализа защищенности информации, которая представляет различные способы описания систем защиты на основе графовых моделей, а также методы их анализа, имеющие прикладное значение, позволило вывести зависимости для количественной оценки защищенности информации.

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», [Электронный ресурс], ред. от 19.08.2018 «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798.
2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст]: учебное пособие / А.А. Малюк. — М.: ГЛТ, 2004. — 280 с.
3. Чипига А.Ф. Информационная безопасность автоматизированных систем [Текст]: учебное пособие / А.Ф. Чипига. — М.: Гелиос АРВ, 2010. — 336 с.
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Текст]: учебное пособие / В.Ф. Шаньгин. — М.: ДМК, 2014. — 702 с.
5. Петров С.В. Информационная безопасность [Текст]: учебное пособие / С.В. Петров, И.П. Слинкова, В.В. Гафнер. — М.: АРТА, 2012. — 296 с.

Добрынин П.А., Музылева И.В., Белокопытов Р.Н.
Разработка лабораторного стенда для проведения практических работ по
программированию датчиков

*Липецкий государственный технический университет
 (Россия, Липецк)*

doi:10.18411/lj-11-2018-176

idsp: ljjournal-11-2018-176

Аннотация

В работе описывается разработка лабораторного стенда. Обосновываются причины выбора тех или иных комплектующих стенда. Так же в статье говорится о цели создания стенда и о принципах работы с ним. Приведены структурная схема стенда и его схематическое изображение спереди.

Ключевые слова: стенд, датчики, микроконтроллер, Arduino.

Annotation

The work describes the development of a laboratory stand. The reasons for the choice of those or other components of the stand are justified. The article also speaks about the