АНАЛИЗ АЛГОРИТМОВ, СРЕДСТВ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

А.В. Корвель
Научный руководитель – В.Ф. Алексеев
канд.техн.наук, доцент
Белорусский государственный университет информатики и радиоэлектроники

Средства и методы защиты, применяемые при создании систем защиты информации, представляют собой использование специальных программ или программно-аппаратных комплексов (антивирусов, контроля доступа и т.д.), технических средств (генераторы помех, системы видеонаблюдения и т.д.), инженерных и инженерно-технических средств (системы сигнализации, двери, ограждения и т.д.), внедрение правил работы в ИС (принятие политики безопасности). Можно предложить следующую классификацию методов и средств защиты информации (рисунок 1).

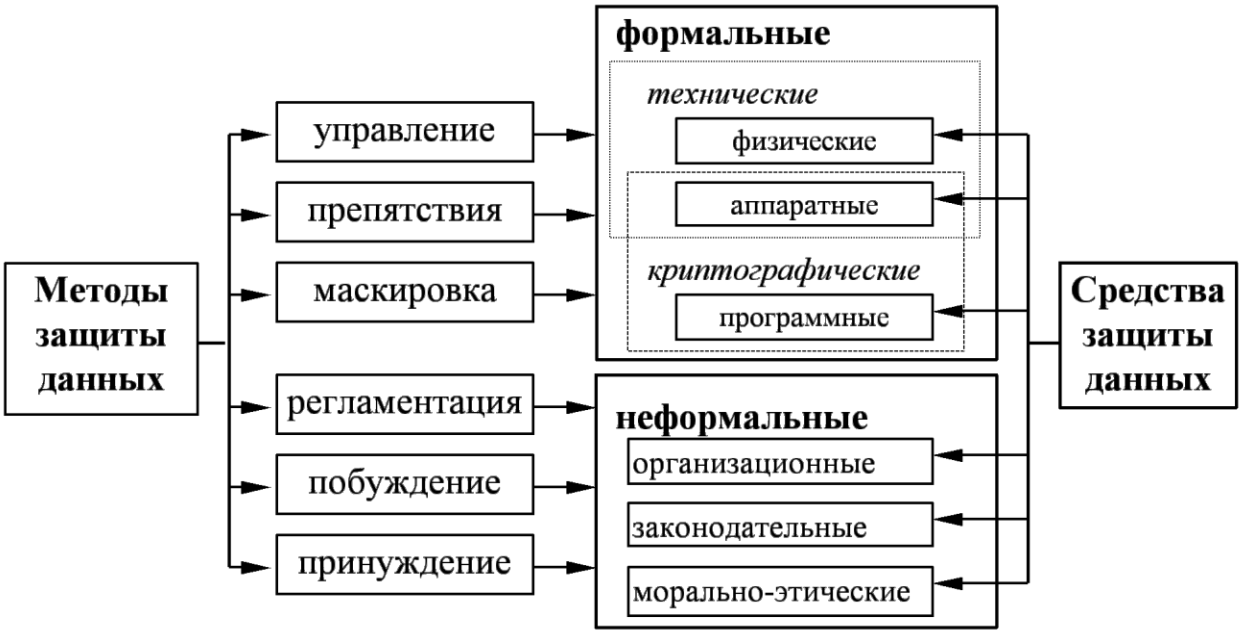

Рисунок 1 – Классификация методов и средств защиты информации

К методам и средствам организационной защиты информации относятся организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации информационной системы (ИС) для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться ИС; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности ИС.

Основные виды мероприятий, которые должны проводиться на различных этапах жизненного цикла ИС:

– на этапе создания ИС: при разработке ее общего проекта и проектов отдельных структурных элементов – анализ возможных угроз и методов их нейтрализации; при строительстве и переоборудовании помещений –

приобретение сертифицированного оборудования, выбор лицензированных организаций; при разработке математического, программного, информационного и лингвистического обеспечения – использование сертифицированных программных и инструментальных средств; при монтаже и наладке оборудования – контроль за работой технического персонала; при испытаниях и приемке в эксплуатацию – включение в состав аттестационных комиссий сертифицированных специалистов;

– в процессе эксплуатации ИС – организация пропускного режима, определение технологии автоматизированной обработки документов, организация работы обслуживающего персонала, распределение реквизитов разграничения доступа пользователей к элементам ИС (паролей, ключей, карт и т.п.), организация ведения протоколов работы КС, контроль выполнения требований служебных инструкций и т.п.;

– мероприятия общего характера – подбор и подготовка кадров, организация плановых и предупреждающих проверок средств защиты информации, планирование мероприятий по защите информации, обучение персонала, участие в семинарах, конференциях и выставках по проблемам безопасности информации и т. п.

Можно выделить четыре уровня правового обеспечения информационной безопасности.

Первый уровень образуют международные договоры, к которым присоединилась Беларусь, и законы Беларуси.

Второй уровень правового обеспечения информационной безопасности составляют подзаконные акты, к которым относятся указы Президента Республики Беларусь и постановления Правительства.

Третий уровень правового обеспечения информационной безопасности составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами.

Под инженерно-техническими средствами защиты информации понимают физические объекты, механические, электрические и электронные устройства, элементы конструкции зданий, средства пожаротушения и другие средства.

Важнейшей составной частью инженерно-технических средств защиты информации являются технические средства охраны, которые образуют первый рубеж защиты ИС и являются необходимым, но недостаточным условием сохранения конфиденциальности и целостности информации в ИС.

К аппаратным средствам защиты информации относятся электронные и электронно-механические устройства, включаемые в состав технических средств ИС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств ИС.

Под программными средствами защиты информации понимают специальные программы, включаемые в состав программного обеспечения ИС исключительно для выполнения защитных функций.

Под идентификацией, применительно к обеспечению информационной безопасности ИС, понимают однозначное распознавание уникального имени

субъекта ИС. Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта).

Анализ показывает, что для перекрытия одних и тех же уязвимостей, могут быть использованы различные наборы средств и методов защиты, которые отличаются друг от друга показателями качества защиты и стоимостью внедрения, т.е. критериями эффективности защиты [1–3].

Библиографический список

1. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

2. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

3. Зегжда Д. П. Основы безопасности информационных систем : Учебное пособие для вузов по специальности "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем " / Д. П. Зегжда, А. М. Ивашко . – М. : Горячая Линия-Телеком, 2000 . – 452 с.