МЕТОДЫ И СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Руденя В.Ю.

Магистрант кафедры проектирования информационно-компьютерных систем, Белорусский государственный университет информатики и радиоэлектроники (БГУИР), г.Минск

Аннотация

Статья посвящена рассмотрению существующих методов защиты информации на предприятиях, описано какими средствами достигается информационная безопасность предприятий.

Ключевые слова: методы и средства, информационная безопасность, безопасность предприятия.

Методами обеспечения защиты информации на предприятиях являются следующие [1]:

1. Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.п.).

2. Управление доступом – метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия.

Управление доступом включает следующие функции защиты [2]:

– идентификацию пользователей, персонала и ресурсов информационной системы (присвоение каждому объекту персонального идентификатора);

– аутентификацию (установления подлинности) объекта или субъекта по предъявленному им идентификатору;

– проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

– регистрацию обращений к защищаемым ресурсам; реагирование (сигнализация, отключение, задержка работ, отказ в запросе при попытках несанкционированных действий).

3. Маскировка – метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

4. Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

5. Принуждение – метод защиты информации, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и

использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.

6. Побуждение – метод защиты информации, который побуждает пользователей и персонал системы не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Указанные выше методы обеспечения информационной безопасности реализуются с помощью одного или комплекса следующих основных средств: ***физических, аппаратных, программных, аппаратно-программных, криптографических, организационных, законодательных и морально-этических*** [3].

Физические средства защиты предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

Аппаратные средства защиты – это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

Программные средства защиты предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля. Программные средства защиты информации являются наиболее распространенным видом защиты, обладая следующими положительными свойствами: универсальностью, гибкостью, простотой реализации, возможностью изменения и развития. Данное обстоятельство делает их одновременно и самыми уязвимыми элементами защиты информационной системы предприятия [4].

Аппаратно-программные средства защиты – средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы.

Криптографические средства – средства защиты с помощью преобразования информации (шифрование).

Организационные средства – организационно-технические и организационноправовые мероприятия по регламентации поведения персонала.

Законодательные средства – правовые акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил.

Морально-этические средства – нормы, традиции в обществе, например: Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ в США.

Все рассмотренные средства защиты разделены на ***формальные*** (выполняющие защитные функции строго по заранее предусмотренной процедуре без 76 непосредственного участия человека) и ***«неформальные»*** (определяемые целенаправленной деятельностью человека либо регламентирующие эту деятельность) [5].

Шифрование может быть *симметричным* и *асимметричным*. Первое основывается на использовании одного и того же секретного ключа для шифрования и дешифрования. Второе характеризуется тем, что для шифрования используется один общедоступный ключ, а для дешифрования – другой, являющийся секретным, при этом знание общедоступного ключа не позволяет определить секретный ключ.

Наряду с шифрованием внедряются следующие ***механизмы безопасности*** [6]:

- цифровая электронная подпись;
- контроль доступа;
- обеспечение целостности данных;
- обеспечение аутентификации;
- постановка трафика;
- управление маршрутизацией;
- арбитраж или освидетельствование.

Механизмы цифровой подписи основываются на алгоритмах ассиметричного шифрования и включают две процедуры: формирование подписи отправителем и ее опознавание получателем. Первая процедура обеспечивает шифрование блока данных либо его дополнение криптографической, контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знания которого достаточно для опознавания отправителя.

Механизмы контроля доступа осуществляют проверку полномочий объектов АИС (программ и пользователей) на доступ к ресурсам сети. При доступе к ресурсу через соединение контроль выполняется как в точке инициации, так и в промежуточных точках, а также в конечной точке.

Механизмы обеспечения целостности данных применяются к отдельному блоку и к потоку данных. Целостность блока является необходимым, но не достаточным условием целостности потока и обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков [7].

Механизмы постановки трафика, называемые также механизмами заполнения текста, используют для засекречивания потока данных. Они основываются на генерации объектами АИС блоков, их шифровании и организации передачи по каналам сети. Тем самым нейтрализуется возможность получения информации посредством наблюдения за внешними характеристиками потоков, циркулирующих по каналам связи.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по небезопасным физически ненадежным каналам.

Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами АИС, третьей стороной. Для этого вся информация, отправляемая или получаемая объектами, проходит через арбитра, что позволяет ему впоследствии подтверждать упомянутые характеристики.

СПИСОК ЛИТЕРАТУРЫ

1. Методы обеспечения защиты информации // Студопедия [Электронный ресурс]. – 2018. – Режим доступа: https://studopedia.ru/3_26071_metodi-obespecheniya-zashchiti-informatsii.html. – Дата доступа: 01.05.2018.

2. Манин, С.А. Методы и средства обеспечения информационной безопасности / С.А. Манин, М.В. Двадненко. – Краснодар: КубГТУ, 2016.

3. Методы и средства обеспечения информационной безопасности организации // Веселка [Электронный ресурс]. – 2018. – Режим доступа: https://www.e-reading.club/chapter.php/31223/53/Kuznecov_-_Informaciya__sbor%2C_zashchita%2C_analiz._Uchebnik_po_informacionno-analiticheskoii_rabote.html. – Дата доступа: 01.05.2018.

4. Хайитова, И. И. Методы и средства обеспечения безопасности / И.И. Хайитова. – М.: Молодой ученый №4, 2017.

5. Защита информационных объектов // Варнинг [Электронный ресурс]. – 2018. – Режим доступа: http://www.warning.dp.ua/tel28.htm. – Дата доступа: 01.05.2018.

6. Методы и средства построения систем информационной безопасности (СИБ). Структура СИБ // Финлит.онлайн [Электронный ресурс]. – 2018. – Режим доступа: http://finlit.online/osnovyi-ekonomiki/metodyi-sredstva-postroeniya-sistem-48636.html. – Дата доступа: 03.05.2018.

7. Ажмухамедов, И. М. Системный подход к обеспечению конфиденциальности при хранении данных на электронных носителях / И.М. Ажмухамедов, Р.Ю. Переверзева. – Астрахань: АГТУ, 2012.