УДК 004.056.53

А.В. Бедарев[1], А.В. Тарутин[2]
Пермский военный институт
войск национальной гвардии Российской Федерации, г. Пермь[1]
Пермский национальный исследовательский
политехнический университет, г. Пермь[2]

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

В данной статье рассмотрены аспекты основные методы и средства защиты информации на примере крупной организации. Обоснована структура специализированного Центра. Выделены функции, которые может обеспечивать такой Центр.

Ключевые слова: защита информации; методы защиты информации; средства защиты информации; персональные данные.

A.V. Bedarev[1], A.V. Tarutin[2]
Perm military Institute of the national guard of the Russian Federation, Perm[1]
Perm national research polytechnic university, Perm[2]

METHODS AND MEANS OF INFORMATION PROTECTION IN AUTOMATED SYSTEMS

This article discusses aspects of the main methods and means of information security on the example of a large organization. The structure of the specialized Center is justified. The functions that such a Center can provide are highlighted.

Keywords: information protection; methods of information protection; means of information protection; personal data.

Информация считается одним из богатств любой страны, её стратегическим национальным ресурсом. Масштабная информатизация повышает мобильность, комфорт и даёт множество удобств населению, но в то же время делает государство более уязвимым, так как у врагов появляется возможность воздействовать на важнейшую для жизни людей инфраструктуру. Таким образом защита информации и информационных процессов, технологий, сред становится стратегически важным направлением деятельности государства.

Информационная безопасность – это все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, безотказности, подотчётности, аутентичности и достоверности информации и средств её обработки.

Данное понятие является обширным и может иметь несколько трактовок. Если отследить действия правительства и принимаемые законы, можно сделать вывод, что в масштабах государства под информационной безопасностью понимается обеспечение состояния безопасности национальных интересов

страны, жизненно важных интересов личности, общества и государства в информационной сфере от внешних и внутренних угроз [1].

Безопасность данных (информации) – это состояние данных (информации), при котором обеспечены их (её) доступность, целостность и конфиденциальность.

Защита информация – это комплекс мер направленных на обеспечение безопасности [2].

Таким образом, безопасность можно считать состоянием объекта, и тогда защитой будет являться деятельность, направленная на обеспечение такого состояния.

Информационная безопасность важна не только в масштабах государства, но и в масштабах каждого человека. Все мы имеем персональные данные, которые в руках других людей могут нанести нам ущерб материальный, психологический или даже физический. Обеспечение личной информационной безопасности является ответственностью самого человека. Поэтому важно иметь фундаментальные знания в этой области.

Методы (они же способы) – это порядок и правила применения определённых принципов и средств защиты информации.

При обеспечении защиты информации допустимо, а порой необходимо, использовать сразу несколько методов. Методы делятся на два подвида:

- правовые (составляют легитимную основу построения и использования системы защиты);
- организационные (связанные с непосредственным воздействием на элементы системы защиты).

Защита информации обеспечивается с помощью различных средств. А метод определяет порядок, в котором используются эти средства.

Средство ЗИ – это техническое, программное средство, вещество или материал, предназначенные или используемые для защиты информации [3].

Следует заметить, что правовые способы осуществляются строительством нормативной базы. На уровне государства есть определенный перечень необходимых для выполнения действий:

- выработка государственной политики безопасности в информационной сфере;
- законодательно определить правовой статус информации, систем защиты информации, ИВС, владельцев информации и т.д.;
- создать структуру гос. органов в иерархическом порядке, которые будут работать над политикой безопасности;
- создание системы стандартизации, лицензирования и сертификации в области информационных технологий;
- обеспечение приоритетного развития отечественных защищённых информационных технологий;
- повышение уровня образования граждан в информационной сфере, воспитания у них патриотизма и бдительности;
- установление ответственности граждан за нарушение законодательства в информационной сфере.

Данный перечень позволяет наладить правовое регулирование в области информационных технологий.

Маскировка – это способ защиты информации, направленный на её криптографическое преобразование с целью скрыть от злоумышленника.

Маскировка может использоваться как при передаче информации по открытой или уязвимой сети, так и при её хранении на носителе или устройстве обработки. В первую очередь при маскировке используют криптографические средства ЗИ, которые шифруют информацию [4].

Препятствие – это способ ЗИ, при котором создаётся барьер на пути дестабилизирующего фактора.

Дестабилизирующим фактором может являться злоумышленник, вредоносное ПО, события и др. При создании препятствия посторонние воздействия на объект становятся невозможными или значительно затрудняются. Препятствия могут быть выстроены как на физическом пути, так и на логическом, таким образом, здесь применяются криптографические СЗИ и средства физической ЗИ [5].

Например, препятствие в виде замка – средство физической защиты, а пароль при входе в систему – КСЗИ.

Комплексом, включающим в себя вышеперечисленные методы и средства защиты информации может являться Центр информационных технологий, связи и защиты информации (ЦИТСиЗИ) основными функциями которого является:

1. Организация системы связи и обеспечение ее бесперебойной и безошибочной эксплуатации.

2. Обеспечение функционирования автоматизированных информационных систем, а также, в случае развития, – целостной структуры информационно-аналитического обеспечения предприятия.

3. Осуществление специальных мер по препятствованию техническим разведкам по вопросам защиты информации.

4. Создание условий работы в среде шифрованной связи с соблюдением требований безопасности.

5. Создание целостной системы в рамках ведомственных и межведомственных программ по расширению функционала Центра:

- здание ЦИТСиЗИ в каждом городе страны;
- крупный ЦОД 4 уровня сертификации (tier 4);
- использование сертифицированных ФСТЭК программно-аппаратных комплексов;
- VPN;
- пропускная система на объектах;
- запрет использования USB-накопителей;
- отсутствие WI-FI;
- отдел технической поддержки.

Состав способов защиты информации, позволяющий обеспечить защиту информации от выявленных угроз в зависимости от указанного класса защищенности на каждом объекте:

- маскировка информации;

- препятствия на пути злоумышленника;
- мотивация (побуждение);
- принуждение;
- регламентация доступа к информации;
- управление силами и средствами защиты.

Состав применяемых средств защиты информации информационной системы:

- средство физической ЗИ (пропускная система – турникет с охранным отделом, сейфы и железные двери в особо охраняемые помещения);
- криптографическое средство ЗИ (Криптон, Криптопровайдер, КриптоПро CSP);
- организационные средства (выплата премий, наличие системы штрафов, проведение плановых совещаний с инструктажем);
- средства антивирусной защиты (Kaspersky Endpoint Detection and Response);
- программно-аппаратные средства («Рубикон» выполняет функции МЭ, СОВ, маршрутизатора);
- VPN («Континент»);
- DLP (СёрчИнформ КИБ);
- SIEM (СёрчИнформ SIEM).

Таким образом, можно сделать вывод, что информация является одним из важнейших ресурсов организации и страны в целом.

Особенно в наше время, когда почти у каждого человека имеется своя страница в социальной сети и электронной почте скрывающие индивидуальную информацию о человеке: его личные данные, номера телефонов, историю в браузерах, банковские реквизиты, а также какую-либо информацию о друзьях, коллегах и семье, которая не должна выйти на широкое обозрение общественности.

Можно сказать, что в нашем информационном XXI веке вся жизнь человека находится во всемирной паутине. Если не обеспечить должного уровня защиты всех вышеперечисленных аспектов информации, то в руках злоумышленника это может являться мощнейшим оружием и может нанести моральный, материальный и иной вид ущерба.

Именно поэтому защита информации и технологий выступает как наиболее стратегически важное направление деятельности специалистов соответствующего ведомства.

Ведь прогресс не стоит на месте и в мире появляются всё новые и новые методы, средства и способы обхода барьеров, криптографических преобразований с целью хищения важной стратегической информации.

В ответ на это методы и средства защиты модернизируются в соответствующем органе с целью не допустить посторонних лиц к секретным сведениям, которые могут нанести непоправимый вред государству и проживающему в нем населения в целом.

Подобный орган защиты информации был представлен в настоящей статье.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Безбогов, А.А. Методы и средства защиты компьютерной информации: учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шмаков. – Тамбов: Из-во ТГТУ, 2006. – 196 с.

3. Данилов, А.Н. Основы информационной безопасности: учебное пособие / А.Н. Данилов, С.А. Данилова, А.А. Зорин. – Пермь: Из-во ПГТУ, 2008. – 556 с.

4. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

5. ГОСТ Р 50922-2006. Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения.

Сведения об авторах

Бедарев Артём Викторович – курсант Пермского военного института войск национальной гвардии Российской Федерации, Пермь, e-mail: onea_1@mail.ru

Тарутин Анатолий Владимирович – кандидат технических наук, доцент, доцент кафедры «Информационные технологии и автоматизированные системы», Пермский национальный исследовательский политехнический университет, Пермь, e-mail: itas-pnipu@yandex.ru

About the authors

Bedarev Artyom Victorovich – Cadet of Perm military Institute of the national guard of the Russian Federation, Perm, e-mail: onea_1@mail.ru

Tarutin Anatoliy Vladimirovich – Ph.D. in Technical Sciences, associate professor, associate professor of the Information Technologies and Automated Systems department, Perm National Research Polytechnic University, Perm, e-mail: itas-pnipu@yandex.ru