СИСТЕМНЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Федоренко В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Аннотация. В докладе рассмотрены основные аспекты комплексной системы защиты информации и системный подход объединяющий разнородные методы и средства противодействия различным видам угроз.

Важнейшим ресурсом современного общества является информация, проблема защиты которой весьма актуальна как для различных стран и организаций, особенно для вооруженных сил.

Обеспечение безопасности функционирования военной организации нашей страны требует привлечения всех имеющихся средств защиты во всех структурных подразделениях и на всех этапах технологического цикла обработки информации. Наибольший эффект может быть достигнут только в том случае, когда все используемые средства, методы и меры объединяются в единый целостный механизм – комплексную систему защиты информации (КСЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий [1].

Защита информации требует к себе системного подхода, сущность которого состоит в создании защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические.

В современных условиях КСЗИ также должна иметь несколько уровней защиты, перекрывающих друг друга [2]. Чтобы добраться до закрытой информации, злоумышленнику необходимо «взломать» все уровни.

На каждом рубеже угрозы нарушению безопасности должны быть обнаружены и по возможности ликвидированы, а в случае невозможности ликвидации, их распространению должны препятствовать последующие рубежи. При этом, чем сложнее защита каждого рубежа, тем больше времени потребуется злоумышленнику для его преодоления и тем вероятнее его обнаружение. Из этого следует, что защита каждого рубежа должна взаимно дополнять друг друга и эффективность всей системы защиты будет оцениваться как минимальное время, которое злоумышленник должен затратить на преодоление всех её рубежей. За это время (безопасное время) он должен быть обнаружен и обезврежен сотрудниками службы безопасности.

Количество и пространственное расположение зон и рубежей выбираются таким образом, чтобы обеспечить требуемый уровень безопасности защищаемой информации, как от внешних, так и внутренних злоумышленников. Чем более ценной является защищаемая информация, тем большим количеством рубежей и зон целесообразно окружать ее источник и тем сложнее злоумышленнику обеспечить разведывательный контакт с ее носителями.

В модели КСЗИ необходимо выделить следующие зоны (рубежи, барьеры) защиты: 1) территория, занимаемая организацией; 2) здание (здания) на территории, в котором расположены средства обработки информации; 3) помещения внутри здания, в которых расположены ресурсы автоматизированных систем и защищаемая информация; 4) линии (каналы) связи и источники питания, находящиеся как в пределах одного и того же здания, так и проходящие между различными зданиями на охраняемой территории и выходящие за пределы объекта; 5) аппаратные средства (терминалы пользователей, устройства ввода-вывода данных, центральные процессоры, аппаратные средства шифрования и дешифрования данных, внешние запоминающие устройства, устройства уничтожения информации, другое периферийное оборудование; 6) программные средства, в том числе операционная система и специальные программы, осуществляющие функции защиты и тестовый контроль механизма защиты в КСЗИ; 7) файлы и данные (включая бумажную информацию).

Для каждой из приведенных выше зон возможны четыре степени защиты информации: предотвращение, обнаружение, ограничение, восстановление [1].

На современном этапе необходимо совершенствовать способы борьбы с этим видом нарушений, которые должны носить системный характер, а также учитывать причины и условия их совершения. Все это обуславливает необходимость углубленного изучения принципов организации КСЗИ; способов анализа и оценки угроз безопасности информации; критериев и условий отнесения информации к защищаемой по видам тайн и степеням конфиденциальности и др.

Список использованных источников:

1. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – СПб: НИУ ИТМО, 2011 – 112 с.

2. Системный подход к защите информации [Электронный ресурс] – Режим доступа: https://helpiks.org/7-90293.html.