Павленков М.Н., Байрушин Ф.Т.
Об методах и средствах защиты информации

*ФГБОУ ВО «Бакирский государственный университет»
(Россия, Уфа)*

doi: 10.18411/lj-06-2021-132

Аннотация

В статье рассматривается понятие подходов к разработке методов и средств защиты информации, классические методы шифрования и стандартные криптографические системы, а также встроенные в ОС и внешние средства защиты информации.

Ключевые слова: информационная безопасность, защита информации, обеспечение конфиденциальности, программное обеспечение, канал утечки информации.

Abstract

The article discusses the concept of approaches to the development of methods and means of information security, classical encryption methods and standard cryptographic systems, as well as built-in OS and external information security tools.

Keywords: information security, information protection, confidentiality, software, information leakage channel.

Вопросы, связанные с методами и средством защиты информации, возникают в нашей жизни и требуют к себе особого внимания. В настоящее время до сих пор актуален вопрос о каналах утечки информации, которые образуются при эксплуатации персональной электронно-вычислительной машиной. Посмотрев со стороны защиты информации данные технические устройства являются прекрасным примером для изучения почти всех каналов утечки информации от радиоканала и до материально-вещественным. Персональные электронно-вычислительные машины могут работать в нескольких режимах, как независимо друг от друга, так и контактируя с другими электронно-вычислительными машинами по компьютерным сетям, учитывая факт, что ЭВМ могут быть, как локальными, так и глобальными.

Под защитой информации считается деятельность, направленная на устранение утечек защищаемой информации и несанкционированных действий на защищаемую информацию. Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных влияний на защищаемую информацию.

Согласно ГОСТ Р 50922-96, под защитой информации рассматривается действие, направленное в сторону устранения утечки информации, которая находилась под защитой, несанкционированного и непреднамеренного воздействия на оберегаемую информацию. Функция безопасности информации — это требуемый итог защиты информации. Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения охраняемой информации, также ее оглашения, несанкционированного доступа к находящейся под защитой информации и приобретения защищаемой информации злоумышленниками. Безопасность информации от несанкционированного воздействия — это движение, направленное на устранение воздействия на информацию, находящуюся под защитой, с учётом нарушений поставленных прав и (или) определенных условий поправки информации, влекущая к ее искажению, ликвидации, блокировке доступа к информации и к потере, нейтрализации или дефекта носителя той или иной информации. Помимо этого, существует защита информации от непреднамеренного воздействия.

Непреднамеренное воздействие на защищаемую содержит в себе ошибки пользователя, сбои программных и технических средств. Защита происходит посредством устранения воздействия на защищаемую информацию накладок пользователя, технических и программных средств информационных систем, которые были направлены на переработку информации также к ее искажению, ликвидации, блокировке доступа к информации и к потере, нейтрализации или дефекта носителя информации. И последнее, защита информации от разглашения — это операция, которая отвечает за устранение несанкционированной огласки информации, находящейся потребителем и не имеющим разрешения к данной информации.

В Российской Федерации существует Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция), в которой указывается необходимость защиты информации, содержащейся в информационных системах, а также государственная информационная система. Данный закон обязывает владельца информации обеспечить её защиту информации от неправомерного доступа, редактирования, уничтожения, блокирования, копирования и других неправомерных действий посредством принятия правовых, организационных и технических мер, которые, в свою очередь, были направлены на соблюдение конфиденциальности информации.

Распространение информации — это действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц. В свою очередь, предоставление информации — это такие действия, направленные на получения информации, определенным кругом лиц или передачу информации определенному кругу лиц.

Информация в зависимости от порядка предоставления или распространения подразделяется на следующие типы:

- информацию, свободно распространяемую;
- информацию, которая в соответствии с ФЗ подлежит предоставлению или распространению;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, распространение которой в РФ ограничивается или запрещается.

Существуют несколько видов угроз:

- угроза нарушения конфиденциальности;
- угроза нарушения целостности;
- угроза отказа служб;
- искусственные;
- естественные.

Первый вид угроз заключается в том, что он становится известен лишь определенному кругу лиц, кто не располагает полномочиями для получения данной информации. Следующий тип угрозы включает в себя ряд изменений информации, которая хранится в вычислительной системе или передаваемой из одной системы в другую. То есть, целостность информации подразумевает из себя существование информации в неискаженном виде, иначе неизменном. Третья угроза возникает в тех случаях, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Помимо вышеперечисленных угроз, можно другие виды и подвиды, например по природе возникновения, то есть искусственные и естественные. Первые — это угрозы, вызванные деятельностью человека, а вторые — угрозы, которые были вызваны посредством природных явлений. Также по степени преднамеренности проявления, например, угрозы случайного действия, то есть, вызванные наплевательским отношением человека.

Наиболее эффективными подходами защиты информации является контроль функционирования системы защиты, то есть постоянное улучшение средств и методов контроля над функциональностью механизмов защиты, системный подход к построению систем защиты, повышения качества способов борьбы с вирусами.

Защита информации предоставляет собой принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа как описывалось уже ранее, изменения, предоставления, а также иных неправомерных действий такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

Под защитой информации от несанкционированного доступа следует выделить следующие меры:

- правовые,
- морально-этические,
- организационные,
- финансовые
- технологические.

К правовым относятся меры контроля за исполнением нормативных актов общегосударственного значения, механизмы развития и совершенствования нормативно — правовой базы, регулирующей вопросы защиты информации. Второй тип не является обязательными, но они достаточно эффективны в борьбе с внутренними нарушителями. Следующий тип, третий, к ним относятся меры и мероприятия, упорядоченные внутренними инструкциями организации, эксплуатирующей информационную систему. Примером такой защиты является присвоение грифа секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Четвертая мера предлагает ввести специальные доплаты при работе с защищенной информацией, а также систему вычетов и штрафов за нарушение режимных требований. Последний тип, механизмы безопасности реализуются на основе программно-аппаратных средств, например, систем идентификации и аутентификации или охранной сигнализации.

Стоит указать, что способы информационной безопасности, выбранные для реализации в информационной системе должны в полной мере обеспечивать блокирование угроз информационной безопасности, включенных в модель угроз информационной безопасности.

Регулярное по плану применение всех перечисленных методов и средств в настоящее время защиты информации даёт наиболее надежную безошибочность системы безопасности и не допускает разглашение конфиденциальной информации.

1. Хорошко А. В., Чекатков А. А. Методы и средства защиты информации : научная литература / В. А. Хорошко, А. А. Чекатков — Издательство Юниор, 2003. — С. 177. — ISBN 966-7323-29-3.
2. Вострецова В. Е. Основы информационной безопасности : научная литература / В. Е. Вострецова — Издательство Уральского университета, 2019. — С. 92. — ISBN 978-5-7996-2677-8.
3. Безбогов А. А., Яковлев В. А., Шамкин Н. В. Методы и средства защиты компьютерной информации : научная литература / А. А. Безбогов, В. А. Яковлев, Н. В. Шамкин — Издательство ТГТУ, 2006. — С. 12. — ISBN 5-8265-0504-4.
4. Федеральный закон N 149-ФЗ от 27.07.2006 г. «РОССИЙСКАЯ ФЕДЕРАЦИЯ ФЕДЕРАЛЬНЫЙ ЗАКОН ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ» [Электронный ресурс] // КонсультантПлюс : надежная правовая поддержка / Режим доступа : / URL: <http://base.www.consultant.ru/> (дата обращения 22.02.2021 г.).
5. Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] // Консорциум кодекс / Режим доступа : / URL: <http://docs.cntd.ru/> (дата обращения 22.02.2021 г.).