МОДЕЛИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА ЗАЩИЩАЕМЫХ ОБЪЕКТАХ

М.Турдиматов
Доцент Ферганского филиала ТАТУ
Боратова Гулмира Рахмоналиевна,
Мастер Ферганского филиала ТАТУ
boratova.gulmira@mail.ru

АННОТАЦИЯ

Проанализированы стандарты в области защиты информации. Схематично представлены структура угроз информационной безопасности и процесс их реализации. Приведен перечень защищаемых объектов и их взаимосвязь с системой защиты.

Ключевые слова: *защищаемый объект, угрозы безопасности информации, система защиты информации, объект защиты информации.*

ABSTRACT

The standards in the field of information security are analyzed. The structure of information security threats and the process of their implementation are schematically presented. A list of protected objects and their relationship with the protection system is given.

Keywords: *Protected object, information security threats, information protection system, information protection object.*

ВВЕДЕНИЕ

Перечень понятий и терминов в области защиты информации достаточно широк и разнообразен. В статье приведен их анализ, на основе которого схематично представлены процессы воздействия угроз на защи- щаемый объект, структурированы угрозы и уязвимости, объект защиты и защищаемый объект. Источник является непосредственной причиной возникновения угрозы, которая воздействует на защищаемый объект.

Исходя из стандартизированных терминов в области защиты информации можно сделать вывод, что в общем виде защищаемым объектом является объект, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности. Объект становится защищаемым тогда, когда в его состав включается система защиты информации.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

Перечень защищаемых объектов может быть весьма разнообразным. Это могут быть объекты информатизации, информационные системы, ресурсы информационной системы, информационная технология, программные средства, сети связи, автоматизированные системы. Главной отличительной особенностью защищаемого объекта является наличие объекта защиты и системы защиты.

Под объектом защиты понимается информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации. К объектам защиты могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации. В законодательстве Республики Узбкистан насчитывается более 30 видов защищаемой информации (информации ограниченного доступа).

Источник угрозы безопасности информации – это субъект, являющийся непосредственной причиной возникновения угрозы безопасности информации. Это могут быть физические лица, явления, материальные объекты. Угроза представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Угроза, воздействуя на защищаемый объект, может нарушить состояние защищенности информации, при котором обеспечены ее конфиденциальность, целостность и доступность. Следовательно, и угрозы по виду воздействия можно разделить на угрозы нарушения конфиденциальности, целостности и доступности информации. Под конфиденциальностью информации понимается состояние, при котором доступ к ней осуществляют только субъекты, имеющие на него право. Информация целостна, когда отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Изменение может быть осуществлено в форме замены информации, введения новой информации, а также уничтожения или повреждения информации. В состоянии доступности субъекты, имеющие права доступа к информации, могут реализовать их беспрепятственно. Условием реализации угрозы может быть недостаток или слабое место в информационной системе. В качестве фактора, воздействующего на защищаемую информацию, выступает явление, действие или процесс, результатом которого могут быть утечка,

искажение, уничтожение защищаемой информации, блокирование доступа к ней. В качестве условий и факторов реализации угроз можно выделить утечку информации, несанкционированное, преднамеренное и непреднамеренное воздействие на информацию.

Под утечкой информации понимается неконтролируемое распространение защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также получение защищаемой информации разведками и другими заинтересованными субъектами. Доступ будет считаться несанкционированным тогда, когда происходит получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Обладатель информации или санкционированный им пользователь имеют доступ к носителям информации, т.е. указанные лица имеют возможность получать и использовать защищаемую информацию. Для реализации права доступа к защищаемой информации санкционированных пользователей и невозможности доступа к ней иных субъектов собственником (обладателем) информации разрабатываются правила доступа, устанавливающие порядок и условия доступа к информации и ее носителям.

Утечка информации возможна по техническому каналу, под которым понимается совокупность носителя защищаемой информации, физическая среда распространения и техническое средство, осуществляющее перехват информации, т.е. неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Основным классификационным признаком технических каналов утечки информации является физическая природа носителя защищаемой информации. В соответствии с ним технические каналы утечки информации подразделяются на акустические, радиоэлектронные, оптические и материально-вещественные.

Отличие заключается в характере воздействия. При несанкционированном воздействии оно осуществляется с нарушением установленных прав и (или) правил доступа. При непреднамеренном – в воздействии ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий. Защита информации рассматривается как деятельность,

направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Проанализировав приведённые выше определения безопасности информации и угроз безопасности информации, можно сделать вывод, что защита информации – это деятельность, направленная на обеспечение безопасности информации.

ЗАКЛЮЧЕНИЕ

Как видно из определений, объект защиты (защищаемая информация, ресурсы) включён как в защищаемый объект, так и систему защиты. Именно объект защиты является точкой соприкосновения системы защиты и объекта, на котором циркулирует информация, и делает такой объект защищаемым. Важным элементом системы защиты информации является техника защиты информации, которая активно или пассивно воздействует на сообщение, на носитель с защищаемой информацией или средство разведки, делая невозможным перехват.

Техника защиты информации включает в себя систему взаимодополняющих средств защиты информации (физической, криптографической), средств контроля эффективности, средств и систем управления, предназначенных для обеспечения защиты информации.

REFERENCES

1. Мухтаров Ф.М., Шкляровский Б.А.. “Предпосылки обеспечение конфиденциальности информационных ресурсов в электронном правительстве”, Сборник докладов республиканской научно-технический конференции “Значение информационно-коммуникационных технологий в инновационном развитии реальных отраслей экономики” часть 1 , г.Ташкент, 6-7 апреля 2017 г., ТУИТ, 23-25 стр..
2. Akbarov, D. E., & Umarov, S. A. (2021). Mathematical characteristics of application of logical operations and table substitution in cryptographic transformations. *Scientific-technical journal*, *4*(2), 6-14.