УДК 004.056

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

В.Д. Буслаев – 18рпт, 3 курс, ФТС
В.С. Журба – 18рпт, 3 курс, ФТС
Научный руководитель – ст. преподаватель Е.И. Подашевская
БГАТУ, г. Минск, Республика Беларусь

В среднем по миру насчитывается около 33–34 млрд. устройств подключённых к интернету, примерно 9,5–10 млрд. из них: планшеты, ноутбуки и смартфоны. По статистике, каждые 11 секунд они подвергаются атаке киберпреступников, чья прибыль, на сегодняшний день, превышает доходы от торговли наркотиками. Однако, всякая информация, расположенная в компьютерных системах, может быть утрачена не только в результате взлома и последующего хищения, а также в результате уничтожения оборудования и неисправности системы в целом, а также человеческого фактора. Способами защиты от подобных причин утрат информации могут выступать применения технических средств, специализированного программного обеспечения, а также использование устройств и аппаратных средств.

Обычные компьютерные вирусы, в начале своего возникновения, отличались довольно низкой мобильностью, они подобно паразитам встраивались в существующие файлы и за счёт внешних носителей (флешки и дискеты) путешествовали с ними. В начале 2000-х годов, вредоносным программам, что называется "приделали ноги", в результате чего возникло новое понятие: "компьютерный червь", либо "сетевой червь". В отличие от обычных вирусов, сетевые черви распространяются через интернет без участия пользователя. Для заражения компьютеров они используют уязвимости программного обеспечения. Под уязвимостью понимается некоторая ошибка в программном коде, практически всегда это ошибка программиста при написании этого кода.

Главной угрозой компьютерного мира до 2010 года являлись сетевые черви, с их помощью осуществлялся захват и последующая передача компьютера под контроль хакерам. Следующим этапом развития вирусов выступили так называемые троянские программы. Троянские программы представляют собой программы, которые, как правило, выдают себя за безобидное приложение, вредоносные действия которых осуществляются через некоторое время после попадания на компьютер. Как правило, трояны целенаправленно используют против пользователей или конкретных компаний. Действуют такие программы следующим образом: первоначально они незаметно проникают в компьютеры, после чего могут годами находиться в системе, чтобы впоследствии в нужный момент выполнить приказ преступника.

Существует несколько методов защиты информации, к которым относятся:

– - формирование условий вынуждающих пользователей соблюдать правила обращения с данными;

– - преобразование данных (криптография);

– - создание препятствия на предполагаемом пути злоумышленника, создаваемое программными и физическими средствами;

– - осуществление мероприятий или внедрение нормативно-правовых актов, способствующих побуждению пользователей к должному поведению при взаимодействии с базами данных;

– - осуществление управления, либо воздействие на элементы защищаемой компьютерной системы.

Реализация методов защиты информации осуществляется с помощью определённой категории средств. Такими средствами являются: технические и организационные.

Наиболее интересным способом защиты является использование биометрических данных (отпечатки пальцев, технологии Face ID и др.), однако и эти способы защиты не гарантируют полноценной безопасности, достаточно приобрести фотографию ладони, чтобы полностью воссоздать модель отпечатка пальца, тем же методом можно обойти блокировку Face ID, воссоздав модель лица.

К одной из наиболее новых конечных целей взлома злоумышленниками относится добыча криптовалюты с использованием чужих ПК. Для этого применяются программы, именуемые "Дроперами", с помощью которых осуществляется скрытная установка вредоносных ПО, встроенных в их код, на взламываемый компьютер. Дроперы позволяют осуществлять установку других программ, необходимых злоумышленнику, выступая в роли проводника.

С целью предотвращения неправомерного доступа к персональной информации прибегают к использованию идентификации и аутентификации. Идентификацией называют присвоение личного уникального образа или имени пользователю. Аутентификацией именуется совокупность методов проверки сходства пользователя с теми образами, которым разрешен допуск к некоторой информации. Использование аутентификации и идентификации позволяют предоставить либо ограничить допуск к данным.

Список использованной литературы

1. Баранова Е.К. Информационная безопасность и защита информации : учебное пособие / Баранова Е.К., Бабаш А.В. – 4-е изд., перераб. и доп. Москва : РИОР : ИНФРА-М, 2019. – 322 с.

2. Внуков А.А. Защита информации: учебное пособие для вузов / А.А. Внуков. – 3-е изд., перераб. и доп. Москва : Издательство Юрайт, 2020. – 161 с.

3. Партыка Т.Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. – 5-е изд., перераб. и доп. Москва : ФОРУМ : ИНФРА-М, 2020. – 432 с.