ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Марченко Анастасия Алексеевна

Студент ФГБОУ ВО «Армавирский государственный педагогический университет», г. Армавир

Научный руководитель доцент, к.п.н. кафедры информатики и ИТО Егизарьянц А.А.

PROTECTION OF INFORMATION IN INFORMATION SYSTEMS

Marchenko Anastasiya Alekseevna

Student of Armavir state pedagogical University, Armavir

АННОТАЦИЯ

Обработка персональных данных, которая является обязательной для любого учреждения или организации, требует внедрения информационных систем, персональных данных и, конечно же, их защиты. Известно, что в современном мире информация имеет определённую, а часто очень высокую ценность. Как и любую ценность её нужно защищать. Защита необходима, например, от потерь из-за случайного удаления, сбоев вирусов, несанкционированного доступа к информации и так далее.

Ключевые слова: информация, информационная система, защита информационной системы, интернет, несанкционированный доступ.

ABSTRACT

The processing of personal data, which is mandatory for any institution or organization, requires the implementation of information systems, personal data and, of course, their protection. It is known that in the modern world information has a certain, and often very high value. Like any value, it must be protected. Protection is necessary, for example, from losses due to accidental deletion, virus failures, unauthorized access to information, and so on.

Keywords: information, information system, information system protection, Internet, unauthorized access.

Информационная система — это взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации для достижения цели управления. Современное понимание данного термина предполагает использование компьютера в качестве основного технического средства переработки данных. Отличие информационной системы заключается в том, что она должна быть разработана с учётов IT- технологий [2, с.558].

В современных условиях существуют следующие типы информационных систем: обучающие системы, системы управления, справочныесистемы, экспертные системы.

Все типы информационных систем подвержены угрозам, особенно количество угроз информационной безопасности резко возрастает, если имеется доступ в интернет, что отражается на методах и средствах защиты. Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например неконтролируемого доступа к персональным компьютерам или нелицензионного программного

обеспечения. Но даже лицензионное программное обеспечение не лишено уязвимостей[3, с.99].

Рассмотрим подробнее угрозы, которые могут возникнуть в аспекте информационной безопасности:

1.Угрозы конфиденциальности- неправомерный доступ к конфиденциальной информации.

2. Угрозы целостности- любое преднамеренное преобразование данных, содержащихся в информационной системе.

3. Угрозы доступности- полная или временная невозможность получения доступа к ресурсам информационной системы [1, с.96].

По степени преднамеренности действий угрозы делятся на: случайные(стихийные действия, аварии, ошибки при разработке информационной системы, сбои и отказы информационной системы и так далее) и преднамеренные (специально созданные угрозы, они менее изучены за счёт их высокой динамичности и постоянного пополнения новыми угрозами, что затрудняет борьбу с ними).

По расположению источника угрозы: внутренние и внешние, по размерам наносимого ущерба: общие(данные угрозы наносят ущерб объекту безопасности в целом) , локальные (данные угрозы наносят ущерб условиям существования отдельных частей объекта безопасности), частные (данные угрозы причиняют вред отдельным свойствам элементов объекта или отдельным направлениям его деятельности) и другие [6, с.204].

Таким образом, для защиты информационных систем выстраиваются системы защиты информации, которые делятся на два подхода: эпизодический и комплексный.

Эпизодический подход подразумевает проведение защитных мероприятий при наличии определённых угроз. К примеру, обязательная антивирусная проверка сторонних носителей информации или использование криптографических систем шифрования [4, с.309-310].

При комплексном подходе различные меры используют в комплексе, образуя контур безопасности системы.

Для создания надежной системы информационной безопасности важны три аспекта:

1. Доступность — это гарантия того, что авторизованные пользователи могут иметь доступ и работать с информационными ресурсами и системами которые им необходимы при этом обеспечивается требуемая производительность. Обеспечение доступности включает меры для поддержания доступности информации, несмотря на возможность помех, включая отказ системы и преднамеренные попытки нарушения доступности.

2. Целостность — гарантия того, что информация останется неизменной и корректной. Обеспечение целостности предполагает предотвращение и определение неавторизованного создания, модификации или удаления информации.

3. Конфиденциальность — это гарантия того, что информация может быть прочитана и проинтерпретирована только теми людьми и процессами, которые авторизированы это делать. Обеспечение конфиденциальности включает в себя процедуры и меры, предотвращающие раскрытие информации неавторизованными пользователями [5, с.325].

Защита компьютеров от несанкционированного доступа является одной из основных проблем защиты информации. Нужен комплекс

решений для минимизирования угроз информационной безопасности. Должно обеспечиваться отсутствие или ограничение свободного доступа неавторизованного пользователяи потенциальных нарушителей непосредственно к аппаратным составляющим и корпусу компьютера. Необходимо обеспечить защиту системы установкой пароля, производить первоначальную загрузку путём задания пароля в BIOS. Также возможно использовать электронный замок, обладающий собственным «доверенным» периметром загрузки, который наполностью препятствует запуску компьютера с не доверенной операционной системой или с использованием внешних носителей [9, с.544].

Немаловажно предпринять защиту от несанкционированного доступа с использованием программных средств. Необходимо установить антивирус с максимально широким функционалом для защиты сетевой инфраструктуры и сервера, желательно управляемый централизованно, постоянно обновляемый [8, с.702].

Должен быть обеспечен защитный «периметр», включающий в себя демилитаризованную зону в виде отдельной изолированной подсети на стыке, отвечающим за сопряжение с внешними сетями и Интернет. Это достигается работающими аппаратными файрволами.Также допускается организация защиты соединения непосредственно информационной системы с нужным ресурсом через программные VPN-клиенты, шифрующие трафик в создаваемом VPN-туннеле [7, с.432].

Таким образом, обеспечение безопасности информационных материалов- это целый комплекс мероприятий, не единовременная мера, а непрерывный процесс. Разработка системы защиты должна проводиться одновременно с проектированием защищаемой системы.

Список использованной литературы:

1. Blinov A.M. Information Security: A Study Guide. Part 1. - St. Petersburg: Publishing house of St. Petersburg State University of Economics, 2010. - 96 p.

2.Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

3. Mayers G. J. Advances in computer architecture. 2nd ed. NY: JonhWilley&Sons, 1982.

4. Mytnik A. A. Business process automation in university using E-Decanat 2.0 software/ A.A. Mytnik, A.P. Klishin // The 1 th International Global Virtual Conference-Workshop, April 2013. –Zilina: EDIS, 2013.-P.308-310.

5. Konheim, Alan G., 1934- Computer security & cryptography / by Alan G. Konheim

6. Vostretsova, E.V. Fundamentals of information security: a tutorial for university students / E. V. Vostretsova. - Yekaterinburg: Ural Publishing House.University, 2019 - 204 p.

7.Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.

8.Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2017. — 702 с.

9.Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2018. — 544 с.