ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ И СЕТЕВЫХ ДАННЫХ

PROVIDING INFORMATION SECURITY
TO PROTECT COMPUTER AND NETWORK DATA

УДК 004.056.57+ 004.056.53

Смирнов Виталий Михайлович, Старший преподаватель кафедры информатики и математики, Московский университет МВД имени Владимира Яковлевича Кикотя, г. Москва

Филиппова Полина Игоревна, курсант, Московский университет МВД имени Владимира Яковлевича Кикотя, г. Москва

Smirnov Vitaly Mikhailovich, Senior Lecturer of the Department of Informatics and Mathematics, Moscow University of the Ministry of Internal Affairs named after Vladimir Yakovlevich Kikot, Moscow

Filippova Polina Igorevna, student, Moscow University of the Ministry of Internal Affairs named after Vladimir Yakovlevich Kikot, Moscow

Аннотация

В статье рассматриваются методы и способы обеспечения информационной безопасности компьютерных и сетевых данных. Цель исследования: определить наиболее лучшие средства для обеспечения конфиденциальности, целостности и доступности информации. Отображены история развития компьютерных технологий, подробное описание информации, её категорий и потребителей, перечислены различные виды сетевых атак, виды используемых вредоносных программ. Также представлены способы защиты от несанкционированного доступа, отказа в обслуживании персонального компьютера и взлома

информационных систем. В заключении показана актуальность данной темы и степень важности обеспечения безопасности данных.

Annotation

The article discusses the methods and ways of ensuring information security of computer and network data. Objective of the study: to determine the best means to ensure the confidentiality, integrity and availability of information. The history of the development of computer technologies, a detailed description of information, its categories and consumers are displayed, various types of network attacks, types of malicious programs used are listed. Methods of protection against unauthorized access, denial of service of a personal computer and hacking of information systems are also presented. The conclusion shows the relevance of this topic and the degree of importance of ensuring data security.

Ключевые слова: информационная безопасность, конфиденциальность, целостность, доступность, персональный компьютер

Keywords: information security, confidentiality, integrity, availability, personal computer

На сегодняшний день сложно представить человека, не использующего персональный компьютер, ноутбук, мобильный телефон для выхода в глобальную сеть интернет с целью поиска, передачи, загрузки, хранения интересующей его информации. В процессе развития информационных технологий человечество прошло несколько этапов, от рукописи с использованием перьевой ручки до появления первых пишущих машин, создания первых электронно-вычислительных машин и наконец, появления современных персональных компьютеров. К сожалению, массовая компьютеризация и информатизация общества привела к появлению глобальных преступных сообществ и организаций, занимающихся противоправной деятельностью в сфере компьютерной и информационной безопасности. Ввиду этого организация эффективного противодействия взлому

и несанкционированному доступу к данным со стороны злоумышленников является особо актуальной.

Под информацией следует понимать совокупность сведений и данных, представленных в какой-либо форме: текстовой, звуковой, числовой, графической или видеозаписи. Разумеется, следует четко разграничивать её назначение: массовая для широкого круга потребителей, специальная профессиональная для узкого круга людей, секретная и личная. В настоящее время под понятием «хакер» подразумевают злоумышленников в компьютерной и сетевой среде, которые используя различные уязвимости и слабые места в операционной системе, осуществляют различные электронные атаки. Так или иначе, хакеры могут получить доступ к любому роду информации об одном гражданине или целом государстве, что может представлять угрозу государственной безопасности. Используя специализированные программы, они совершают атаки на операционную систему в целях искажения, несанкционированного использования или уничтожению информационных ресурсов, компьютерной техники.

В соответствии с Доктриной информационной безопасности Российской Федерации[1] от 5 декабря 2016 г. №646 под обеспечением информационной безопасности подразумевается осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер

---

[1]Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"// СПС «КонсультантПлюс»

по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Одной из основных задач является защита конфиденциальности, целостности и доступности данных.

В процессе противодействия взлому и незаконному доступу к данным следует разделять виды угроз для общего понимания направления атаки и возможного варианта её пресечения, такие как : различные вредоносные программы (вирусы, трояны, черви), ddos- атаки, спам, фишинг, ip-спуфинг, социальная инженерия. Для обеспечения безопасности компьютерных и сетевых данных необходимо использовать сетевой экран, который способен распознавать попытки взлома, проверенную версию антивируса, регулярно устанавливать новые обновления системы, а также отслеживать входящий трафик, устанавливать соединение с сайтами при помощи VPN.

Помимо использования различных действенных утилит и программ следует внимательно проверять личные сообщения на электронной почте, не заполнять сомнительные анкеты от неизвестных лиц, не вводить личные данные и номер карты на подозрительных сайтах, не переходить по неизвестным ссылкам, не отвечать на спам сообщения.

В целях противодействия и пресечения компьютерной преступности в Уголовном Кодексе[2] Российской Федерации от 13.06.1996 N 63-ФЗ посвящена целая глава 28 - преступления в сфере компьютерной информации и ряд статей - 272 (Неправомерный доступ к компьютерной информации), 273 (Создание, использование и распространение вредоносных компьютерных программ), 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей),

---

[2]"Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ// СПС «КонсультантПлюс»

274.1 (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации).

В заключении хочется сказать о том, что количество преступлений в сфере компьютерной и информационной безопасности стабильно растет ввиду

технологического прогресса, массового использования гражданами сети интернет и появления сайтов с полезной информацией. Ввиду этого МВД , ФСБ , ФСТЭК , службе информационной безопасности предприятия и другим государственным органам следует вести эффективную работу, своевременно принимать грамотные решения, оперативно выявлять, предупреждать и пресекать хакерскую деятельность, регулярно изучать и анализировать новые данные в сфере информационных технологий. Только подходя к делу ответственно и профессионально возможно достигать высоких результатов и организовывать компьютерную безопасность на должном уровне.

Литература

1. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"
2. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ
3. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
4. Указ Президента РФ от 9 мая 2017 г. N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы"

Literature

1. Decree of the President of the Russian Federation of 05.12.2016 N 646 "On approval of the Doctrine of information security of the Russian Federation"
2. "The Criminal Code of the Russian Federation" dated 13.06.1996 N 63-FZ
3. Federal Law "On Information, Information Technologies and Information Protection" dated July 27, 2006 N 149-FZ
4. Decree of the President of the Russian Federation of May 9, 2017 N 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017 - 2030"