УДК 004.056 **DOI: 10.34670/AR.2021.33.43.034**

Информационная безопасность: проблемы и их методы решения

Хасаев Муслим Сатович

Студент,
Чеченский государственный университет им. А.А. Кадырова,
364024, Российская Федерация, Грозный, ул. А. Шерипова, 32;
e-mail: difficult.id@mail.ru

Магомедов Ислам Арбиевич

Ассистент,
Чеченский государственный университет им. А.А. Кадырова,
364024, Российская Федерация, Грозный, ул. А. Шерипова, 32;
e-mail: ismwork@mail.ru

Аннотация

Статья посвящена актуальной проблеме современности – проблеме информационной безопасности. Сегодня информационные системы играют ключевую роль в обеспечении эффективной работы коммерческих и государственных предприятий, министерств, ведомств, некоммерческих организаций. Важнейшей составляющей информационной безопасности становится защита от информации, заключающаяся в предупреждении разрушающего воздействия информации на электронные средства, системы и на людей. Информационная безопасность – это в первую очередь защита информации и ее сохранение. В век глобализации от надежности обеспечения информационной безопасности зависит национальная безопасность государства. Информация становится ключевым элементом практически всех систем социальной жизни. В любой области, будь то политическая безопасность, экономическая безопасность, экологическая безопасность, общественная безопасность, существует связывающий элемент, в роли которого выступает информационная безопасность.

Для цитирования в научных исследованиях

Хасаев М.С., Магомедов И.А. Информационная безопасность: проблемы и их методы решения // Экономика: вчера, сегодня, завтра. 2021. Том 11. № 10А. С. 296-301. DOI: 10.34670/AR.2021.33.43.034

Ключевые слова

Информационная безопасность, вирусы, хакеры, антивирусы, защита данных.

Введение

Информация – это знания об окружающем мире, которые повышает уровень осведомленности человека. Иными словами, под информацией понимается накопление, хранение и обработка данных любого вида.

Информационная безопасность (англ. information security, а также InfoSec) – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Получается, что информационная безопасность – это в первую очередь защита информации и ее сохранение.

Проблемы информационной безопасности в современном мире напрямую связаны с прогрессом в сфере информационных технологий. Наиболее совершенные информационные технологии и технические средства информации связаны со сферой противостояния или же с подготовкой к нему. Информационная безопасность внедрена практически во все сферы человеческой жизни. Она оказывает определенное влияние на состояние экономической, социальной, политической и других компонентов гражданской безопасности.

Основная часть

Прежде чем подробно рассмотреть понятие информационной безопасности, стоит выяснить, от кого и зачем необходимо защищать информацию. Само понятие «информационная безопасность» уходит в глубокую древность. Так как в древности не было Интернета, использовали гонцов для доставки важной информации. Но не исключался риск того, что информацией может завладеть неприятель. Поэтому вводился определенный шифр, который был известен только союзной стороне. К примеру, во времена правления Юлия Цезаря появилось такое понятие, как Шифр Цезаря, посредством которого писался код, который в последующем расшифровывался получателем. Это и была своего рода информационная безопасность. По мере развития технологий появился Интернет. В последующем его стали использовать для хранения данных и информации государственной и глобальной важности. Интернет стали использовать в сфере экономики, к примеру, банки, фондовые биржи и разные компании, в науке и других областях. В результате появились люди, которые хотели завладеть информацией в корыстных целях. Сегодня их называют хакерами.

Изначально хакерами звали тех, кто профессионально разбирался в программном обеспечении и кодах. Но в последнее время это понятие трактуется как взломщик, который создает компьютерные вирусы, взламывает базы данных и ворует информацию. Безусловно, это все наказуемо и контролируется на законодательном уровне.

Компьютерные «вирусы» называются так потому, что они именно «заражают» множество файлов и программ на компьютере и нарушают их работоспособность или вовсе выводят из строя [Абдулов, 2005]. Самое страшное то, что зараженные файлы в последующем заражают и другие, к примеру, когда они передаются по USB-накопителям, электронной почте или на дисках. Первый вирус был создан в 1986 году в целях наказания за воровство программного обеспечения (ПО).

Существуют следующие виды компьютерных вирусов.

1. Трояны. Или же, как их часто называют, троянцы. Они маскируются под безобидное ПО или файлы и после установки осуществляют вредоносную деятельность без ведома

пользователя.

2. Черви. Червям не требуется вмешательство пользователя, они заражают одну сеть и далее переходят на другие компьютеры, используя уязвимость сетей. Они самостоятельно размножаются и уничтожают информацию, а иногда и вовсе воруют.

3. Шпионское ПО. Из названия можно понять, что этот вид вредоносных программ следит за вами, то есть отслеживает все действия, совершенные пользователем (посещения сайтов, переходы, клики), также отслеживает, какие клавиши были нажаты в ходе процесса, тем самым можно узнать регистрационные данные и украсть их у человека.

4. Баги. Сами баги не являются вредоносным ПО, но они могут сильно нарушать работу программы и повлиять на информацию. Баг, по сути, это ошибка в коде, которую совершил программист при написании [Менциев, Чебиева, 2019]. Но главная проблема багов в том, что этим могут воспользоваться те же самые хакеры. То есть использовать изъян программы для обхода системы безопасности, и в дальнейшем изменения кода и воровства данных.

Существует еще один вид угроз, которые не зависят ни от программ, ни от людей, – это естественные угрозы. Естественные угрозы представляют собой природные явления, такие как ураганы, наводнения, пожары, катаклизмы и другое, что может вызвать утерю информации. Допустим, сгорит компьютер, утонет жесткий диск, на котором хранились данные.

Известны следующие принципы информационной безопасности:

1. Конфиденциальность. Данный принцип предполагает обеспечение информацию должным уровнем безопасности для предотвращения нежелательных утечек и нарушения. Также она должна сохраняться при обработке и передаче информации.

2. Целостность. Служит для предотвращения искажения информации.

3. Доступность. Это один из важнейших принципов. Подразумевает, что данные должны быть обеспечены должной защитой, но и должен соблюдаться эффективный и быстрый доступ к информации.

Для снижения рисков утерь и нарушений стоит также выбрать вид контроля безопасности:

1. Физический. Как раз-таки этот вид и связан с естественными угрозами. Это контроль внешней среды рабочего места: отслеживание температурных условий, оснащение камерами слежения, замки, сигнализации и другое [Магомедов, Мурзаев, 2019].

2. Административный. Вид контроля, который создает рамки для ведения бизнеса и контроля над людьми. Он включает в себя политику безопасности, федеральные законы и нормативные акты, дисциплинарные меры и так далее.

3. Логический. Этот вид еще называют техническим. Он основан на защите доступа к информации и к информационным системам посредством создания паролей, программного обеспечения (антивирус и такого рода программы), отслеживания действий.

К средствам защиты информационной безопасности относятся:

1. Организационные. Обеспечение компьютерным оснащением, кабельной системой и помещением.

2. Программные. То есть программы, которые позволяют хранить, обрабатывать, передавать и получать доступ к информации безопасно.

3. Аппаратные. Защита информации от утечки и взлома.

4. Аппаратно-программные. Это смешения двух средств, которые позволяют выступать в качестве одной программы.

К видам защиты информации относятся в первую очередь антивирусы, которые обезвреживают вирусы и восстанавливают зараженные файлы и программное оборудование. Также существуют облачные антивирусы. Data Leak Prevention (DLP) – это набор средств для предотвращения утечки информации, нарушения ее конфиденциальности. Криптография, которая была разобрана в начале статьи, часто используются для шифрования данных, для предотвращения воровства и утечки информации. Прокси-сервера выступают посредником между пользователями или же системами. Безусловно, надежным и эффективным средством защиты является также VPN, что в переводе означает «виртуальная частная сеть», это средство позволяет использовать частную сеть для передачи или получения информации.

Заключение

Таким образом, информация – важнейший ресурс общественной жизни. Информация становится ключевым элементом практически всех систем социальной жизни. В любой области, будь то политическая безопасность, экономическая безопасность, экологическая безопасность, общественная безопасность, существует связывающий элемент, в роли которого выступает информационная безопасность.

В век глобализации от надежности обеспечения информационной безопасности зависит национальная безопасность государства.

Библиография

1. Абдулов А.Н. Контуры информационного общества. М.: ИНИОП РАН, 2005. 162 с.
2. Андрианов В.И. Шпионские штучки и устройства для защиты объектов и информации. СПб., 2001. 254 с.
3. Атаманчук Г.В. Теория государственного управления. М.: Юридическая литература, 1997. 400 с.
4. Лихарев С.Б., Фомин Г.А. Обзор средств криптографической защиты информации в персональных компьютерах. М., 2004. 345 с.
5. Лысов А.В., Остапенко А.Н. Энциклопедия промышленного шпионажа. СПб., 2003.
6. Магомадов В.С. Исследование роли новейших информационных технологий в экономике совместного использования // ФГУ SCIENCE. 2019. С. 130-134.
7. Магомедов И.А., Мурзаев Х.А., Багов А.М. Роль цифровых технологий в экономическом развитии. IOP Publishing Limited, 2019.
8. Максимов Ю.Н. Защита информации в системах и средствах информатизации и связи. СПб., 2005.
9. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона. 2019. № 3 (54). С. 16.
10. Ярочкин В.И. Технические каналы утечки информации. М., 2005. 640 с.

Information security: problems and methods of their solution

Muslim S. Khasaev

Student,
Chechen State University named after A.A. Kadyrov,
364024, 32 Sheripova str., Grozny, Russian Federation;
e-mail: difficult.id@mail.ru

Islam A. Magomedov

Assistant,
Chechen State University named after A.A. Kadyrov,
364024, 32 Sheripova str., Grozny, Russian Federation;
e-mail: ismwork@mail.ru

Abstract

The article is devoted to an urgent problem of our time – the problem of information security. Today information systems play a key role in ensuring the efficient operation of commercial and state enterprises, ministries, departments, non-profit organizations. The most important component of information security is protection from information, which consists in preventing the destructive effect of information on electronic means, systems and people. Information security is, first of all, the protection of information and its preservation. In the age of globalization, the national security of the state depends on the reliability of information security. Information is becoming a key element in almost all systems of social life. In any area, be it political security, economic security, environmental security, public security, there is a connecting element, which is information security. Information security problems in the modern world are directly related to progress in the field of information technology. The most advanced information technologies and technical means of information are associated with the sphere of confrontation or with preparation for it.

For citation

Khasaev M.S., Magomedov I.A. (300) Informatsionnaya bezopasnost': problemy i ikh metody resheniya [Information security: problems and methods of their solution]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 11 (10A), pp. 296-301. DOI: 10.34670/AR.2021.33.43.034

Keywords

Information security, viruses, hackers, antiviruses, data protection.

References

1. Abdulov A.N. (2005) *Kontury informatsionnogo obshchestva* [The contours of the information society]. Moscow: Institute for Scientific Information on Social Sciences of the Russian Academy of Sciences.
2. Andrianov V.I. (2001) *Shpionskie shtuchki i ustroistva dlya zashchity ob"ektov i informatsii* [Spyware and devices for the protection of objects and information]. Saint Petersburg.
3. Atamanchuk G.V. (1997) *Teoriya gosudarstvennogo upravleniya* [The theory of public administration]. Moscow: Yuridiche-skaya literature Publ.
4. Likharev S.B., Fomin G.A. (2004) *Obzor sredstv kriptograficheskoi zashchity informatsii v personal'nykh komp'yutera*kh [Review of means of cryptographic protection of information in personal computers]. Moscow.
5. Lysov A.V., Ostapenko A.N. (2003) *Entsiklopediya promyshlennogo shpionazha* [Encyclopedia of Industrial espionage]. Saint Petersburg.
6. Magomadov V.S. (2019) Issledovanie roli noveishikh informatsionnykh tekh-nologii v ekonomike sovmestnogo ispol'zovaniya [Investigation of the role of the latest information technologies in the sharing economy]. *FGU SCIENCE*, pp. 130-134.
7. Magomedov I.A., Murzaev Kh.A., Bagov A.M. (2019) *Rol' tsifrovykh tekhnolo-gii v ekonomicheskom razvitii* [The role of digital technologies in economic development]. IOP Publishing Limited.
8. Maksimov Yu.N. (2005) *Zashchita informatsii v sistemakh i sredstvakh infor-matizatsii i svyazi* [Information protection in systems and means of informatization and communication]. Saint Petersburg.

9. Mentsiev A.U., Chebieva Kh.S. (2019) Sovremennye ugrozy bezopasnosti v seti Internet i kontrmery (obzor) [Modern security threats on the Internet and countermeasures (overview)]. *Inzhenernyi vestnik Dona* [Engineering Bulletin of the Don], 3 (54), p. 16.
10. Yarochkin V.I. (2005) *Tekhnicheskie kanaly utechki informatsii* [Technical channels of information leakage]. Moscow.