

УДК 33

DOI: 10.34670/AR.2023.22.72.032

Экономические аспекты обеспечения информационной безопасности

Зассеев Астан Аланович

Аспирант,
Северо-Кавказский горно-металлургический институт –
Государственный технологический университет,
362021, Российская Федерация, Владикавказ, ул. Николаева, 44;
e-mail: info@skgmi-gtu.ru

Магазиева Зарема Абусамитовна

Ассистент,
Грозненский государственный нефтяной технический университет,
364024, Российская Федерация, Грозный, пр. Исаева, 100;
e-mail: info@gstou.ru

Алиев Ислам Магомедович

Старший научный сотрудник отдела материаловедения,
Комплексный научно-исследовательский институт
Российской академии наук;
доцент кафедры физической электроники,
Чеченский государственный университет им. А.А. Кадырова,
364093, Российская Федерация, Грозный, ул. Асланбека Шерипова, 32;
e-mail: ialiew@mail.ru

Аннотация

Информационная безопасность – это практика предотвращения неразрешенного доступа, использования, выявления, изменения, изучения либо уничтожения данных. В статье рассматривается проблема, которая актуальна и по сей день – проблема информационной безопасности. Приводится определение термина «информационная безопасность». Четко определена деятельность, которая находится в компетенции органов защиты информации. Представлены основные виды угроз информации и методы защиты информации. В современном обществе информационную безопасность необходимо выводить на первый план, дабы избежать потерю важных файлов, документов, отчетов и вообще всей информации различного рода. Лица, имеющие доступ к какой-либо важной информации, должны быть максимально бдительными. Также не стоит забывать о том, что мы живем в информационном веке, где какое-либо хищение информации может произойти на огромной дистанции при помощи всего лишь одного цифрового гаджета. Отсюда можно понять, что информация, ради ее же безопасности, должна храниться в надежном и защищенном месте, доступ к ней должен иметь только определённый круг лиц. А в случае,

если это действительно ценная и важная информация, стоит обратить внимание на мероприятия по защите информации, которые были указаны в исследовании.

Для цитирования в научных исследованиях

Зассеев А.А., Магазиева З.А., Алиев И.М. Экономические аспекты обеспечения информационной безопасности // Экономика: вчера, сегодня, завтра. 2023. Том 13. № 8А. С. 349-355. DOI: 10.34670/AR.2023.22.72.032

Ключевые слова

Информация, безопасность, данные, защита, угроза, хищение, механизмы.

Введение

Информационная безопасность – это практика предотвращения неразрешенного доступа, использования, выявления, изменения, изучения либо уничтожения данных. Является универсальным понятием, которое используется вне зависимости от формы, которую могут принимать какие-либо данные и сведения [Бабаш, 2016].

Ключевой задачей информационной безопасности является сбалансированное сохранение конфиденциальности, целостности и доступности данных, с учётом целесообразности использования и без какого-либо вреда производительности организации. Этого добиваются с помощью многоэтапного процесса управления, который предоставляет возможность распознать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и способности управления угрозами [Гафнер, 2017].

Основная часть

Основные угрозы информационной безопасности [Громов, 2017]:

- модификация (это введение в информацию различных изменений, говоря дословно, модификаций, помимо сопряженных с адаптацией программы для электронно-вычислительных машин или какой-либо базы данных);
- хищение (это совершённое с корыстной целью незаконное изъятие или обращение посторонней собственности в пользу виновного или иных лиц, которое причиняет вред разной тяжести (в зависимости от того, что именно было украдено и в каком количестве) владельцу);
- утрата (необдуманные действия собственника данных или определенной информации, которые предоставляются в АС на разнообразных носителях, документах и в файлах, либо же личности, которому была предоставлена и доверена определенного рода информация в силу его служебных обязательств и полномочий в рамках АС, в результате которых информация была утеряна и стала имуществом других лиц);
- блокирование (невозможность применения различных данных при их сохранности);
- уничтожение (чередa действий, специализированных для реализации программными либо же аппаратными средствами необратимого удаления информации, в том числе и остаточных данных).

В основе информационной безопасности лежит работа по защите данных, информации и их носителей, но кроме того обеспечению её конфиденциальности и целостности, недопущение к

какой-либо компрометации в критических условиях. К подобным ситуациям относятся природные, техногенные и социальные катастрофы, компьютерные перебои, физическое хищение и тому подобные явления.

В то время, как делопроизводство многих организаций в обществе до сих пор основано на бумажных носителях, требующих определенных мер предоставления информационной безопасности, наблюдается постоянный рост количества инициатив по введению цифровых технологий в фирмах, что влечёт за собою привлечение профессионалов по безопасности информационных технологий с целью защиты данных, сведений и информации в целом. Эти специалисты гарантируют информационную безопасность технологий и всех цифровых носителей информации. Необходимо отметить, что под компьютером в данном случае предполагается не только электробытовой персональный ПК, но и цифровые устройства любой сложности и направления, включая самые примитивные, а иногда даже и изолированные, на типе электронных калькуляторов и бытовых приборов, вплоть до промышленных систем управления и суперкомпьютеров, которые связаны между собой компьютерными сетями. Наикрупнейшие компании и организации, в силу жизненной значимости и ценности информации для их бизнеса, берут специалистов по информационной безопасности, как правило, себе в состав [Малюк, 2016].

В их цели и задачи входит обезопасить все без исключения технологии от вредоносных кибератак, нередко направленных с целью похищения значимой и засекреченной информации или на перехват управления внутренними структурами организаций. Информационная безопасность, как область занятости, существенно раскрутилась и увеличилась в своих масштабах за прошедшие года. В ней появилось большое число профессиональных квалификаций, к примеру, такие как безопасность сетей и связанной инфраструктуры, охрана программного обеспечения и баз данных, проверка информационных систем, составление плана непрерывности бизнеса, обнаружение электронных записей и компьютерная криминалистика.

Одни из самых масштабно проведенных исследований в этой сфере помогли составить статистику, которая говорит о том, что крупные организации и фирмы уже подтверждают нехватку информационных специалистов, по результатам опроса, который был проведен в 2017 году, почти 70% крупных организаций нуждаются в квалифицированных работниках информационной защиты. А при проведении прогнозов на 2022 год, эксперты, составившие статистику, утверждают, что к 2022 году нехватка специалистов данного рода увеличится, недостаток будет составлять практически 2 миллиона [Мирславская, 2021].

Методы защиты информации [Полетаев, 2020]:

- регламентация (метод организации правового регулирования общественных взаимоотношений, который заключается в наделении их участников индивидуальными юридическими правами.);
- препятствие (физическое преграждение пути к проникновению в охраняемую информацию);
- побуждение (способ, который стимулирует субъектов ИС никак не преступать определенные установленные порядки.);
- управление доступом к данным (осуществление надзора за данными, документами, файлами и другими носителями информации, а также осуществлять доступ к информации только определённым лицам;
- противодействие различным хакерским атакам (в случае если информация находится в цифровом виде) (метод, при котором потребуется задействовать сильную системную

защиту от постороннего внедрения в систему информации и информационных носителей;

- применение различных методов шифровки данных (криптография) (шифровка данных поможет повысить уровень конфиденциальности информации и при случаи несанкционированного проникновения в нее способна поставить в тупик).

Субъект информационных взаимоотношений способен понести убытки не только от несанкционированного доступа, но и от неисправности системы, которые способны спровоцировать различные перебои и перерывы в работе. Но более того, для множества открытых организаций сама защита от несанкционированного доступа к различного рода информации стоит по значимости вовсе не на первом месте, но это совсем не значит, что ролью безопасности информации можно пренебречь [Чипига, 2017].

Заключение

Сделаем вывод. В современном обществе информационную безопасность необходимо выводить на первый план, дабы избежать потерю важных файлов, документов, отчетов и вообще всей информации различного рода. Лица, имеющие доступ к какой-либо важной информации, должны быть максимально бдительными. Также не стоит забывать о том, что мы живем в информационном веке, где какое-либо хищение информации может произойти на огромной дистанции при помощи всего лишь одного цифрового гаджета. Отсюда можно понять, что информация, ради ее же безопасности, должна храниться в надежном и защищенном месте, доступ к ней должен иметь только определённый круг лиц. А в случае, если это действительно ценная и важная информация, стоит обратить внимание на мероприятия по защите информации, которые были указаны выше.

Библиография

1. Бабаш А.В. Информационная безопасность. Лабораторный практикум. М.: КноРус, 2016. 98 с.
2. Гафнер В.В. Информационная безопасность. Ростов-на-Дону: Феникс, 2017. 243 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации. Старый Оскол, 2017. 298 с.
4. Дворянкин О. А. Интеллектуальная собственность в России. какой путь-эволюционный и революционный нужен сейчас? //Юрист. – 2006. – №. 12. – С. 42-46.
5. Дворянкин О. Что мы теряем от контрафакт. Кто получает дивиденды //Интеллектуальная собственность. Авторское право и смежные права. – 2006. – №. 3. – С. 31-40.
6. Зарубин, С. Л. Применение цифровых финансовых активов в реальном секторе экономики / С. Л. Зарубин // . – 2023. – Т. 13, № 1-1. – С. 40-48.
7. Козинец, Н. В. Вопросы регламентации отношений, возникающих в сфере защиты прав потребителей при осуществлении электронной торговли / Н. В. Козинец // Конституция Российской Федерации и современный правопорядок : Московская юридическая неделя. Материалы XV Международной научно-практической конференции: в 5-ти частях, Москва, 28–30 ноября 2018 года. Том Часть 4. – Москва: Общество с ограниченной ответственностью "Перспектив", 2019. – С. 290-292. Д.А. Пашенцева, Н.М. Ладнушкиной. – Москва: Издательство "Саратовский источник", 2021. – С. 296-300.
8. Козинец, Н. В. Правовой анализ современных договорных конструкций, применяемых в сфере информационных технологий / Н. В. Козинец // Право и права человека в современном мире: тенденции, риски, перспективы развития : Материалы Всероссийской научной конференции, посвященной памяти профессора Ф.М. Рудинского, Москва, 15 апреля 2021 года / Под общей редакцией В.В. Строева,
9. Козинец, Н. В. Современные вызовы ИОТ (Интернет вещей): общие вопросы и правовое регулирование / Н. В. Козинец // Проблемы реализации прав человека и гражданина в условиях современных социальных трансформаций : Материалы Международной научно-практической конференции, посвященной памяти профессора Ф.М. Рудинского, Москва, 21 апреля 2022 года / Под общей редакцией Д.А. Пашенцева, Н.М. Ладнушкиной. – Саратов: Издательство "Саратовский источник", 2022. – С. 237-241.

10. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М., 2016. 181 с.
11. Мирославская М.Г. Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. СПб., 2021. С. 59.
12. Полетаев В.С. Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности на основе анализа данных тематических интернет-ресурсов. Уфа, 2020. С. 112.
13. Свидетельство о государственной регистрации базы данных № 2021621138 Российская Федерация. Научные и учебно-методические материалы с кейсовыми технологиями "Цифровая экономика и информационная безопасность: правовые проблемы" : № 2021620978 : заявл. 20.05.2021 : опубл. 31.05.2021 / И. М. Рассолов, Н. В. Козинец, О. Г. Филипенкова
14. Сорокина, С. Г. Кодовый характер названия научной статьи / С. Г. Сорокина// XXI век: итоги прошлого и проблемы настоящего плюс. – 2015. – Т. 3, № 6(28). – С. 261-266.
15. Фан-Юнг Г. Ю. Методологические и смысловые особенности употребления термина "химическая промышленность" в отношении некоторых дореволюционных предприятий //Современная наука: актуальные проблемы теории и практики.– С. 20-26.
16. Чипига А.Ф. Информационная безопасность автоматизированных систем. М.: Гелиос АРВ, 2017. 229 с.
17. Чудаев, А. В. Специфика инвестиционного менеджмента в инновационном секторе / А. В. Чудаев // Инновации и инвестиции. – 2022. – № 8. – С. 123-127.
18. Kobylitsky, A. N. The Prediction of Suburban Passenger Traffic with Econometric Models / A. N. Kobylitsky, A. V. Chudaev // IOP Conference Series: Materials Science and Engineering : International Science and Technology Conference "FarEastCon 2019", V, 2020. – P. 052073. – DOI 10.1088/1757-899X/753/5/052073.
19. Learning Path of Distance Education in Regional Universities: Challenges and Opportunities / S. Kokhan, S. Vlasava, A. Eshiev [et al.] // Conference "INTERAGROMASH 2021". Precision Agriculture and Agricultural Machinery Industry, Volume 2 : Conference proceedings, Ростов-на-Дону, 24–26 февраля 2021 года. – Ростов-на-Дону: Springer, 2022. – P. 341-355. – DOI 10.1007/978-3-030-80946-1_34. – EDN AEXNAW.

Economical aspect of information security

Astan A. Zasseev

Postgraduate,
North Caucasian Mining and Metallurgical Institute –
State Technological University,
362021, 44, Nikolaeva str., Vladikavkaz, Russian Federation;
e-mail: info@skgmi-gtu.ru

Zarema A. Magazieva

Assistant,
Grozny State Oil Technical University,
364024, 100, Isaeva ave., Grozny, Russian Federation;
e-mail: info@gstou.ru

Islam M. Aliev

Senior Researcher of the Department of Materials Science,
Integrated Research Institute of the Russian Academy of Sciences;
Chechen State University,
364049, 32, Sheripova str., Grozny, Russian Federation;
e-mail: ialiew@mail.ru

Abstract

Information security is the practice of preventing unauthorized access, use, discovery, alteration, examination, or destruction of data. The article deals with a problem that is relevant to this day, the problem of information security. The definition of the term "information security" is given. The activities that are within the competence of information protection authorities are clearly defined. The main types of threats to information and methods of information protection are presented. In today's society, information security must be brought to the fore in order to avoid the loss of important files, documents, reports, and in general all information of various kinds. Persons with access to any important information should be as vigilant as possible. Also, do not forget that we live in the information age, where any theft of information can occur at a great distance with just one digital gadget. From this it can be understood that information, for the sake of its own security, must be stored in a safe and secure place, only a certain circle of people should have access to it. And if this is really valuable and important information, you should pay attention to the information protection measures that were indicated in the study.

For citation

Zasseev A.A., Magazieva Z.A., Aliev I.M. (2022) Ekonomicheskie aspekti obespecheniya informatsionnoi bezopasnosti [Economical aspect of information security]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 13 (8A), pp. 349-355. DOI: 10.34670/AR.2023.22.72.032

Keywords

Information, security, data, protection, threat, theft, mechanisms.

References

1. Babash A.V. Information security. Laboratory workshop. Moscow: KnoRus, 2016. 98 p.
2. Gafner V.V. Information security. Rostov-on-Don: Phoenix, 2017. 243 p.
3. Gromov Yu.Yu. Information security and information protection. Stary Oskol, 2017. 298 p.
4. Dvoryankin O. A. Intellectual property in Russia. which path-evolutionary and revolutionary - is needed now? //Lawyer. – 2006. – no. 12. – pp. 42-46.
5. Dvoryankin O. What we lose from counterfeit. Who receives dividends //Intellectual property. Copyright and related rights. - 2006. – No. 3. – pp. 31-40.
6. Zarubin, S. L. The use of digital financial assets in the real sector of the economy / S. L. Zarubin //. – 2023. – Vol. 13, No. 1-1. – pp. 40-48.
7. Kozinets, N. V. Issues of regulation of relations arising in the field of consumer protection in the implementation of electronic commerce / N. V. Kozinets // The Constitution of the Russian Federation and modern law and order: Moscow Legal Week. Materials of the XV International Scientific and Practical Conference: in 5 parts, Moscow, November 28-30, 2018. Volume Part 4. – Moscow: Prospect Limited Liability Company, 2019. – pp. 290-292. D.A. Pashentseva, N.M. Ladnushkina. – Moscow: Publishing House "Saratov source", 2021. – pp. 296-300.
8. Kozinets, N. V. Legal analysis of modern contractual structures used in the field of information technology / N. V. Kozinets // Law and human rights in the modern world: trends, risks, development prospects : Materials of the All-Russian Scientific Conference dedicated to the memory of Professor F.M. Rudinsky, Moscow, April 15, 2021 / Under the general editorship of V.V. Stroev,
9. Kozinets, N. V. Modern challenges of IOT (Internet of Things): general issues and legal regulation / N. V. Kozinets // Problems of realization of human and citizen rights in the conditions of modern social transformations : Materials of the International Scientific and Practical Conference dedicated to the memory of Professor F.M. Rudinsky, Moscow, April 21, 2022 / Under the general editorship of D.A. Pashentsev, N.M. Ladnushkina. – Saratov: Publishing House "Saratov source", 2022. – pp. 237-241.
10. Malyuk A.A. Information security: conceptual and methodological foundations of information protection. M., 2016. 181 p.
11. Miroslavskaya M.G. Construction of network security management centers in information and telecommunication

-
- networks. St. Petersburg, 2021. P. 59.
12. Poletaev V.S. Information and analytical system for forecasting threats and vulnerabilities of information security based on data analysis of thematic Internet resources. Ufa, 2020. p. 112.
 13. Certificate of state registration of the database No. 2021621138 Russian Federation. Scientific and educational materials with case technologies "Digital economy and information security: legal problems" : No. 2021620978 : application 20.05.2021 : publ. 31.05.2021 / I. M. Rassolov, N. V. Kozinets, O. G. Filipenkova
 14. Sorokina, S. G. The code character of the title of a scientific article / S. G. Sorokina// XXI century: results of the past and problems of the present plus. – 2015. – Vol. 3, No. 6(28). – pp. 261-266.
 15. Fang-Jung G. Y. Methodological and semantic features of the use of the term "chemical industry" in relation to some pre-revolutionary enterprises //Modern science: actual problems of theory and practice.– pp. 20-26.
 16. Chipiga A.F. Information security of automated systems. Moscow: Helios ARV, 2017. 229 p.
 17. Chudaev, A.V. Specifics of investment management in the innovation sector / A.V. Chudaev // Innovations and investments. – 2022. – No. 8. – pp. 123-127.
 18. Kobylitsky, A. N. The Prediction of Suburban Passenger Traffic with Econometric Models / A. N. Kobylitsky, A. V. Chudaev // IOP Conference Series: Materials Science and Engineering : International Science and Technology Conference "FarEastCon 2019", V, 2020. – P. 052073. – DOI 10.1088/1757-899X/753/5/052073.
 19. Learning Path of Distance Education in Regional Universities: Challenges and Opportunities / S. Kokhan, S. Vlasava, A. Eshiev [et al.] // Conference "INTERAGROMASH 2021". Precision Agriculture and Agricultural Machinery Industry, Volume 2 : Conference proceedings, Rostov-on-Don, February 24-26, 2021. – Rostov-on-Don: Springer, 2022. – P. 341-355. – DOI 10.1007/978-3-030-80946-1_34. – EDN AEXNAW.