Научная статья
Original article
УДК 004.056.5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

INFORMATION SECURITY

Чесноков Алексей Дмитриевич, студент 2 курс, факультет "Инфокоммуникационных сетей и систем (ИКСС)" Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч-Бруевича

Chesnokov Alexey Dmitrievich, 2nd year student, Faculty of "Infocommunication Networks and Systems (IKSS)" St. Petersburg State University of Telecommunications named after Professor M. A. Bonch-Bruevich

Аннотация. В статье анализируются особенности информационной безопасности. Рассматриваются понятие и составные компоненты информационной безопасности, виды защиты в рамках ключевой характеристики сущности информационной безопасности и направления, по которым осуществляется информационная безопасность личности. Выявляются признаки информационного оружия, принципы, особенности и ключевые программно-технические инструменты обеспечения информационной безопасности.

Annotation: The article analyzes the features of information security. The concept and components of information security, types of protection within the framework of the key characteristics of the essence of information security and the

directions in which information security of an individual is carried out are considered. Identifies signs of information weapons, principles, features and key software and hardware tools for ensuring information security.

Ключевые слова: информационная безопасность, информационная среда, информация, защита информации, обеспечение информационной безопасности.

Key words: information security, information environment, information, information protection, information security.

Введение

На фоне осуществляемого перехода общества от индустриального к информационному повышается значимость умения ориентироваться в постоянно возрастающем потоке информации, эффективно работая с ней [1]. Возможности глобальной сети, активно использующиеся во всех сферах общественной жизни, основаны на информационных ресурсах, представляющих собой совокупность данных, которые организованы в информационных системах для получения достоверных сведений в различных областях знаний и практической деятельности [2]. Однако одновременно с увеличением роли информации повышается и важность её защиты, обеспечивающейся посредством инструментов информационной безопасности.

Целью работы является изучение особенностей информационной безопасности. Для её достижения были использованы методы анализа и синтеза научных публикаций и литературных источников по рассматриваемой теме.

Понятие и сущность информационной безопасности

Информационная безопасность (ИБ) представляет собой невозможность причинения вреда свойствам объекта безопасности, которые обусловлены информацией и информационной инфраструктурой [3]. ИБ включает:

– состояние защищённости информационного пространства, благодаря которому обеспечивается его формирование и развитие в интересах государства, граждан и организаций;

– состояние информации, исключающее или значительно затрудняющее нарушение таких её свойств, как целостность, конфиденциальность и доступность;

– состояние инфраструктуры, позволяющее использовать информацию строго по назначению и без негативного воздействия на систему;

– экономическую составляющую, содержащую телекоммуникационные и информационные системы и структуры управления, такие как системы сбора, кумуляции и обработки данных, общеэкономического анализа и прогнозирования хозяйственного развития, управления, координирования и принятия решений;

– финансовую составляющую, охватывающую информационные сети и базы данных, системы финансовых расчётов и обмена.

Ключевой характеристикой сущности ИБ является свойство защищённости, включающее следующие две разновидности защиты [4]:

Активная

Защита нацелена на предупреждение несанкционированного доступа к информации. Её приоритетами являются:

– защита личных данных, т.е. социальных ценностей и иных конфиденциальных сведений;

– эксплуатация средств ИБ;

– эксплуатация и защита объектов критической инфраструктуры;

– международные интересы.

Пассивная.

Защита распространяется на условия для общественного и экономического развития. В качестве её приоритетных направлений рассматриваются:

– свобода обращения информации;

– развитие культуры;

– развитие онлайн-демократии;

– развитие экономики;

– развитие ИТ-сектора;

– международное сотрудничество.

Важным аспектом комплексной ИБ является ИБ личности, актуальная как при спонтанном информационном взаимодействии в Интернете, так и при длительном присутствии в профессиональном виртуальном мире [5]. ИБ личности включает следующие направления:

– защита от внешней агрессивной информации;

– защита от неэтичных, оскорбляющих моральные ценности и чувства данных;

– защита от реализованной на базе коммуникационных и информационных технологий некачественной педагогической продукции, не отвечающей педагогика-эргономическим требованиям;

– защита от заимствования результатов представленной в электронном виде интеллектуальной собственности;

– защита психического и физического здоровья от возможного негативного воздействия, оказываемого в процессе использования коммуникационных и информационных технологий.

Особенности обеспечения информационной безопасности

Обеспечение ИБ позволяет эффективно противостоять информационной преступности, оказывающей информационное воздействие на информационное пространство и его отдельные элементы в противоправных целях. В частности, инструменты и методы ИБ направлены на противодействие информационному оружию, посредством которого [6]:

– осуществляются неправомерный доступ, модифицирование, уничтожение, копирование, блокирование, распространение, предоставление и прочие неправомерные действия в отношении данных;

– нарушается порядок доступа к сведениям и оказывается общее неблагоприятное воздействие на данные;

– реализуется воздействие на средства обработки информации.

Защита информации включает совокупность мер по обеспечению конфиденциальности и целостности информации при условии сохранения её доступности для имеющих соответствующие права пользователей [7]. Под целостностью понимается сохранность качества и свойств информации, под конфиденциальностью – обеспечение приватности данных и доступа к определённым сведениям отдельным пользователям, под доступностью – качество данных, определяющее их оперативное и точное нахождение конкретным пользователем.

Обеспечение ИБ основывается на следующих принципах [8]:

1) Принцип системности. Согласно ему, защитные меры должны быть нацелены на предотвращение информационных атак со стороны внешних и внутренних источников, а также учитывать применяемые средства защиты и каналы закрытого доступа. Средства защиты должны использоваться адекватно вероятным видам угроз и функционировать в виде комплексной системы защиты, технически дополняя друг друга [9-11].

2) Принцип прочности. Устанавливает, что правила обеспечения ИБ должны охватывать все зоны безопасности, иметь равную надёжность защиты и позволять определять вероятные угрозы.

3) Принцип многоуровневой защиты. Ориентирован на создание рубежей защиты информационной системы, состоящих из последовательно расположенных зон безопасности, ключевая из которых располагается внутри всей системы.

4) Принцип бесперебойности. В соответствии с ним, функционирование системы ИБ должно быть непрерывным и бесперебойным.

5) Принцип благоразумности. Выражается в разумности применения защитных мер с требуемой степенью безопасности. В основе этого принципа лежит целесообразность высоких материальных затрат и рациональность их дальнейшего использования. Так, себестоимость защитных мер не должна превышать размера вероятного ущерба, расходы на обслуживание и работоспособность защитной системы.

В качестве основной меры защиты информации используется контроль доступа, призванный исключить возможность несанкционированного доступа к информации [12]. К ключевым программно-техническим инструментам ИБ относятся идентификация и аутентификация, сочетание которых даёт возможность провести процедуру авторизации, установив личность пользователя. Для аутентификации могут использоваться следующие типы информации:

– данные, известные пользователю (PIN-код, пароль, контрольный вопрос);

– предмет, принадлежащий конкретному пользователю (паспорт, водительское удостоверение и иные личные документы);

– биометрические данные, позволяющие автоматизировано распознавать пользователя по уникальным психологическим (подпись, почерк, походка, ритм речи, голос и прочее), биохимическим (ДНК) и/или физиологическим (отпечатки пальцев, геометрия кисти, сетчатка и радужная оболочка глаза, и прочее) признакам, присущим только конкретному индивиду [13].

После успешной идентификации и аутентификации пользователя следует этап авторизации, заключающийся в определении разрешённых для доступа информационных ресурсов и возможных для выполнения действий, таких как запуск, просмотр, создание, удаление либо изменение отдельных данных [14]. В основе авторизации доступа к сведениям и иным вычислительным услугам лежат административные процедуры и политики, предписывающие возможность и условия доступа к информации.

Помимо совершенствования систем ИБ, важным компонентом обеспечения защиты данных выступает аудит информационных систем [15]. Он заключается в получении объективных и систематизированных данных о текущем состоянии применяемых информационных технологий и позволяет своевременно выявлять и устранять их уязвимые места.

Заключение

Сущность информационной безопасности заключается в формировании активной защиты в отношении приоритетных интересов, связанных с использованием информационных ресурсов, направленной на создание условий для нормального развития общества и экономики [16-18]. Обеспечение информационной безопасности представляет собой комплексную задачу, что обусловлено сложностью и многоплановостью информационной среды. Решение проблемы по обеспечению информационной безопасности требует применения организационных, законодательных и программно-технических мер [19], которые должны быт задействованы в совокупности, поскольку в случае пренебрежения хотя бы одним из этих аспектов повышается вероятность утраты информации, роль которой в современной жизни общества приобретает всё большее значение [20].

Список литературы

1. Сидельникова Н.В., Беседина Т.В. Информационная безопасность // Образование. Карьера. Общество. 2018. № 1 (56). С. 71-72.
2. Грачева Е.А. Информационная безопасность // The Newman in Foreign Policy. 2020. Т. 3, № 54 (98). С. 57-59.
3. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Информационная безопасность: учеб. Пособие, под общ. ред. В.Н. Ясенева. / Нижний Новгород: Нижегородский гос. ун-т им. Н.И. Лобачевского, 2017. 198 с.
4. Устинов Д. Сущность информационной безопасности // Международный журнал гуманитарных и естественных наук. 2017. № 12. С. 146-151.
5. Роберт И.В. Информационная безопасность личности // Труды международного симпозиума «Надёжность и качество». 2018. Т. 1. С. 68-71.
6. Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36-40.

7. Карев А.С., Бирих Э.В., Сахаров Д.В., Виткова Л.А. Проблемы информационной безопасности в интернете вещей // В сборнике: Интернет вещей и 5G. 2016. С. 66-70.
8. Буйневич М.В., Покусов В.В., Израилов К.Е. Способ визуализации модулей системы обеспечения информационной безопасности // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2018. № 3. С. 81-91.
9. Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. № 4. С. 66-73. DOI: 10.34219/2078-8320-2021-12-4-66-73.
10. Буйневич М.В., Израилов К.Е., Покусов В.В., Ярошенко А.Ю. Основные принципы проектирования архитектуры современных систем защиты // Национальная безопасность и стратегическое планирование. 2020. № 3 (31). С. 51-58.
11. Израилов К.Е., Покусов В.В. Актуальные вопросы взаимодействия элементов комплексных систем защиты информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017): сборник научных статей VI Международной научно-технической и научно-методической конференции (Санкт-Петербург, 2017). 2017. С. 255-260.
12. Зарипова Г.К., Рамазонов Ж.Ж. Информационная безопасность (обязанности) // Научные исследования. 2019. № 1 (27). С. 51-54.
13. Чурилин Г.Н., Максимова Е.А. Биометрия в информационной безопасности // НБИ технологии. 2019. Т. 13, № 4. С. 30-36.
14. Никитин В.Н., Обеспечение информационной безопасности ИТС / Никитин В.Н., Лагутенко О.И., Ковцур М.М. // Электросвязь. 2014. № 1. С. 29-31.
15. Буйневич М.В., Ганов Г.А., Израилов К.Е. Интеллектуальный метод визуализации взаимодействий программ в интересах аудита

информационной безопасности операционной системы // Информатизация и связь. 2020. № 4. С. 67-74.

16. Миняев А.А. Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информатизация и связь. 2020. № 6. С. 29-36.
17. Миняев А.А., Будько М.Ю. Метод оценки эффективности системы защиты информации территориально распределенных информационных систем // Информатизация и связь. 2017. № 3. С. 119-121.
18. Будько М.Ю., Миняев А.А. Метод оценки эффективности системы защиты персональных данных // Информатизация и связь. 2016. № 2. С. 85-87.
19. Виткова Л.А., Чечулин А.А., Сахаров Д.В. Выбор мер противодействия вредоносной информации в социальных сетях // Вестник Воронежского института ФСИН России. 2020. № 3. С. 20-29.
20. Герлинг Е.Ю., Кулишкина Е.И., Гаврилов А.С., Виткова Л.А. Анализ и выявление психологических аспектов внутренних угроз на объектах связи // Известия высших учебных заведений. Технология легкой промышленности. 2018. Т. 39. № 1. С. 13-16.

Bibliography

1. Sidelnikova N.V., Besedina T.V. Information security // Education. Career. Society. 2018. No. 1 (56). pp. 71-72.
2. Gracheva E.A. Information Security // The Newman in Foreign Policy. 2020. Vol. 3, No. 54 (98). pp. 57-59.
3. Yasenev V.N., Dorozhkin A.V., Sochkov A.L., Yasenev O.V. Information security: textbook. Allowance, under the total. ed. V.N. Yasenev. / Nizhny Novgorod: Nizhny Novgorod state. un-t im. N.I. Lobachevsky, 2017. 198 p.
4. Ustinov D. The essence of information security // International Journal of the Humanities and Natural Sciences. 2017. No. 12. S. 146-151.
5. Robert I.V. Personal Information Security // Proceedings of the International Symposium "Reliability and Quality". 2018. V. 1. S. 68-71.

6. Krasov A.V., Shterenberg S.I., Fakhrutdinov R.M., Ryzhakov D.V., Pestov I.E. Analysis of information security of an enterprise based on the collection of user data from open resources and monitoring of information resources using machine learning // T-Comm: Telecommunications and transport. 2018. V. 12. No. 10. S. 36-40.
7. Karev A.S., Birikh E.V., Sakharov D.V., Vitkova L.A. Problems of information security in the Internet of things // In the collection: Internet of things and 5G. 2016. S. 66-70.
8. Buynevich M.V., Pokusov V.V., Izrailov K.E. The method of visualization of the modules of the information security system // Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". 2018. No. 3. S. 81-91.
9. Buynevich M.V., Pokusov V.V., Izrailov K.E. Threat model of information and technical interaction in an integrated information security system // Informatization and communication. 2021. No. 4. S. 66-73. DOI: 10.34219/2078-8320-2021-12-4-66-73.
10. M. V. Buinevich, K. E. Izrailov, V. V. Pokusov, and A. Yu. Basic principles for designing the architecture of modern protection systems // National Security and Strategic Planning. 2020. No. 3 (31). pp. 51-58.
11. Izrailov K.E., Pokusov V.V. Actual issues of interaction of elements of complex information security systems // Actual problems of infotelecommunications in science and education (APINO-2017): collection of scientific articles of the VI International scientific-technical and scientific-methodical conference (St. Petersburg, 2017). 2017. S. 255-260.
12. Zaripova G.K., Ramazonov Zh.Zh. Information security (duties) // Scientific research. 2019. No. 1 (27). pp. 51-54.
13. Churilin G.N., Maksimova E.A. Biometrics in information security // NBI technologies. 2019. V. 13, No. 4. S. 30-36.
14. Nikitin V.N., Information security of ITS / Nikitin V.N., Lagutenko O.I., Kovtsur M.M. // Electrosvyaz. 2014. No. 1. S. 29-31.

15. Buynevich M.V., Ganov G.A., Izrailov K.E. An intelligent method for visualizing program interactions in the interests of an operating system information security audit // Informatization and communication. 2020. No. 4. S. 67-74.
16. Minyaev A.A. Method and methodology for evaluating the effectiveness of the protection system of geographically distributed information systems // Informatization and communication. 2020. No. 6. S. 29-36.
17. Minyaev A.A., Budko M.Yu. Method for evaluating the effectiveness of the information security system of geographically distributed information systems // Informatization and communication. 2017. No. 3. S. 119-121.
18. Budko M.Yu., Minyaev A.A. Method for evaluating the effectiveness of the personal data protection system // Informatization and communication. 2016. No. 2. S. 85-87.
19. Vitkova L.A., Chechulin A.A., Sakharov D.V. The choice of measures to counteract malicious information in social networks // Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. 2020. No. 3. S. 20-29.
20. Gerling E.Yu., Kulishkina E.I., Gavrilov A.S., Vitkova L.A. Analysis and identification of psychological aspects of internal threats at communication facilities // News of higher educational institutions. Light industry technology. 2018. V. 39. No. 1. S. 13-16.

© Чесноков А.Д., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022

Для цитирования: Чесноков А.Д., ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ/ Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.