Методы и способы обеспечения информационной безопасности хозяйствующего субъекта

Виталий Андреевич Кучковский
бакалавр 4 –го курса, ББББО-05-18
Институт кибербезопасности и цифровых технологий
Москва, Россия
vitaslol221@gmail.com
0000-0000-0000-0000

Сергей Александрович Тронин
кандидат экономических наук, доцент
Финансовый Университет при Правительстве РФ
Москва, Россия
tron1977@rambler.ru
0000-0000-0000-0000

Поступила в редакцию 16.01.2022
Принята 24.02.2022
Опубликована 15.04.2022

10.25726/k9453-8903-4632-o

Аннотация

В статье рассматриваются проблемы информационной безопасности, которые обостряются процессами проникновения во все сферы жизни человека технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Защита информации, так же, как и информационная безопасность, задача комплексная и многопланова, непосредственно направленная на обеспечение безопасности, реализуемая внедрением системы информационной безопасности Специалисты по информационной безопасности в настоящее время формируют понимание комплексной системы защиты информации. В привычном понимании информационная безопасность представляется непосредственно как состояние защищенности, способность противостоять и противодействовать угрозам.

Ключевые слова

защита информации, информационная безопасность, система элек-тронного документооборота, цифровые технологии.

Введение

Безопасность – это такое состояние информационной системы, при котором она может противостоять воздействию внешних и внутренних факторов. При этом, для работы самой системы она не создает тех или иных угроз для своего функционирования.

В области информационной защиты в настоящее время в России действует доктрина информационной безопасности. Данный документ содержит необходимую информацию в области информационной безопасности общества. Информационная безопасность – это состояние защищенности интересов человека, которые для него являются жизненно важными, а также защита интересов общества и государства в информационной сфере от воздействия внутренних и внешних факторов. Такое определение дает доктрина информационной безопасности России (Масалков, 2018).

В первую очередь государство должно защищать интересы личности и общества. Такого мнения придерживаются большинство представителей научного и социального сообщества. Используя

существующие механизмы государство должно обеспечивать экономическую и общественную безопасность.

За исполнением законов информационной безопасности организациями и гражданами следит государство. Государство осуществляет контроль за тем, чтобы каждый гражданин имел возможность получить необходимую информацию, препятствует доступу к данной информации третьих лиц, а также осуществляет иные действия в области обеспечения информационной безопасности (Бирюков, 2017).

Материалы и методы исследования

Многими сферами деятельности в настоящее время управляют различные инновационные технологии. Основываются данные технологии на применении локальных и глобальных компьютерных сетей.

Для решения вопросов безопасности данных при их обработки необходимо применять определенные процедуры и мероприятия. Незамедлительно необходимо решать возникающие проблемы на всех этапах деятельности, а не только при применении информационных технологий. В этой связи каждый этап работы с информацией должен сопровождаться контролем за деятельностью всех элементов системы информационной безопасности (Основы управления, 2016).

На рисунке 1 представим неформальные средства защиты информации.

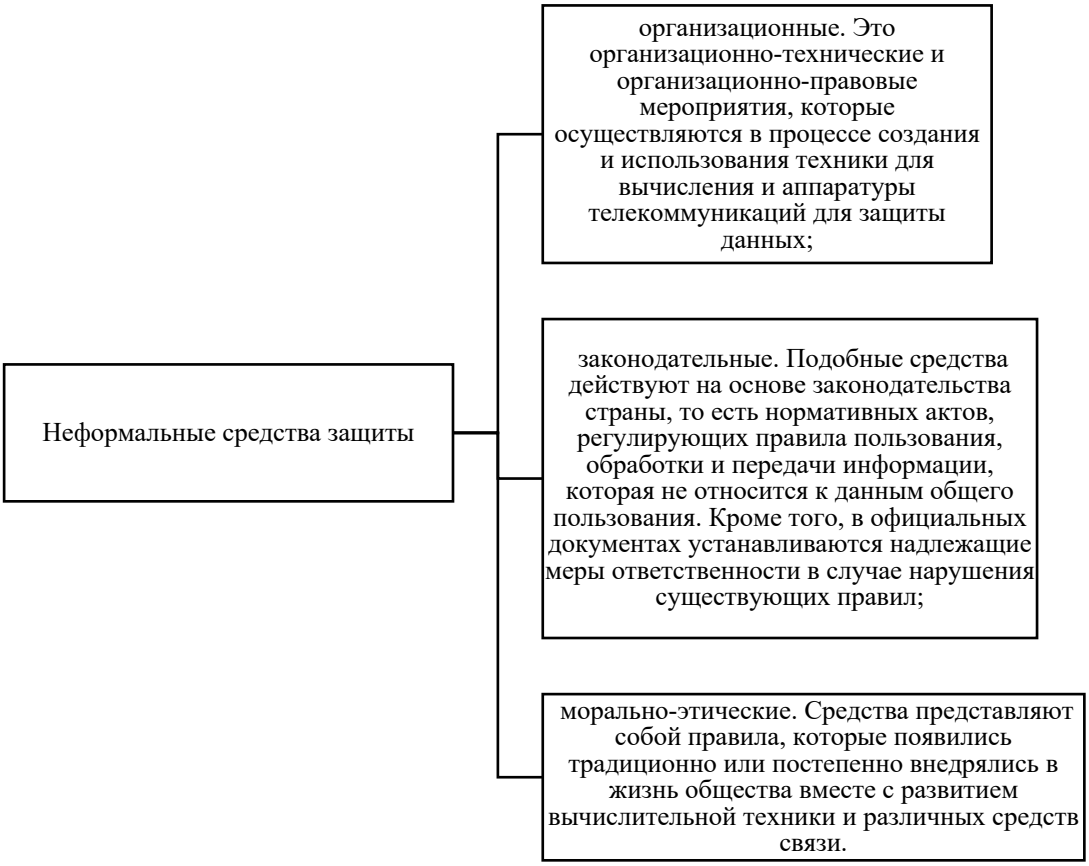

Рисунок 1. Неформальные средства защиты процесса переработки информации (Кузнецова, 2019)

Невозможно обеспечить полной безопасности информации, если в организации не осуществляется необходимая поддержка программно-технических средств для обеспечения защиты данных и незаконного доступа к защищенной информации.

Необходимо в обязательном порядке использовать все элементы системы защиты даже если организация использует в своей деятельности современные механизмы и оборудование.

Первым являются формальные средства, которые обеспечивают защиту информации без участия в данном процессе человека. Для таких программ разработаны специальные процедуры.

Вторая категория средств требует присутствия человека. Такие средства называются неформальными. При использовании таких средств человек осуществляет всю работу по управлению данными системами (Корнилов, 2015).

Проверку полномочий элементов автоматизированной системы необходимо обеспечить в каждой организации. Особое внимание необходимо уделять тем программам и пользователям, которые имеют доступ к наиболее важным сетевым ресурсам.

Результаты и обсуждение

Система инновационного контроля доступа используется для того, чтобы обеспечить такой вид контроля. Через специальное соединение происходит контроль соединений на каждом этапе работы, как на конечном, так и на первоначальном.

Для отдельных блоков и общего потока данных используют существующие методы обеспечения информационной безопасности. Целостность потока не может функционировать правильно, если не соблюдается целостность существующего блока.

За счет выполнения комплекса процедур и дифференцирования информации осуществляется сохранение целостности блока. Отправитель вносит дополнения в передаваемый блок криптографической суммой, а получатель в свою очередь, должен сравнить ее с криптографическим значением конкретного блока. В случае, если данные не совпадают, это означает искажение информации в блоке, однако этот способ не дает возможности раскрыть искажение всего блока в целом. Именно по этой причине следует контролировать целостность потока, реализующегося с помощью шифрования данных с применением изменяемых ключей (Комплексная, 2020).

Процесс проверки подлинности называют аутентификации. Данный процесс делится на взаимную и одностороннюю. Проверку подлинности информации только с одной стороны необходимо при односторонней аутентификации. Как отправитель, так и получатель данных осуществляет проверку информации при взаимной аутентификации.

В процессе засекречивания потока информации осуществляется заполнение текста и постановки программы трафика. Подобные механизмы осуществляются за счет шифрования и передачи по сетевым канал, а также за счет генерации объектами информационной системы. Такой механизм дает возможность получить данные о наблюдении за внешними признаками потоков, которые перемещаются по каналам связи (Межгосударственное, 2019).

Наиболее удобный и эффективный маршрут движения информации по сети, позволяет выбрать механизм управления маршрутизацией. При этом, выбор наиболее оптимального маршрута должен так осуществляться, что бы передаваемая по засекреченным каналам связи не подверглась утечке.

Для подтверждения тех или иных характеристик данных, которые передаются между объектами автоматизированных информационных систем, используют механизм освидетельствования или арбитража. При осуществлении данного механизма через арбитра проходит весь поток информации, который перемещается между отправителем и получателем (Поддержка, 2017).

Заключение

Подводя итог, необходимо отметить, что большую роль в жизнедеятельности общества играет именно информационная безопасность. Современные инновационные методы должны использовать для обеспечения экономической безопасности, вопросам обеспечения которой должно уделяться достаточно внимания в деятельности каждого субъекта хозяйственной деятельности.

Для обеспечения информационной безопасности необходимо использовать различные технические, аппаратные и программные средства, которые дадут возможность оградить от нелегального воздействия конфиденциальные данные.

Также важно уделять внимание организационным аспектам и стремится к сокращению затрат на осуществление защитных мер. При необходимости важно организовать эффективную защиту тех информационных данных, которые подлежат дополнительной защите.

Список литературы

1. Бирюков А. А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. М.: ДМК Пресс, 2017. 433 с.
2. Бирюков А.А. Информационная безопасность: защита и нападение. М.: ДМК Пресс, 2017. 433 с.
3. Бухтояров В.В., Жукова М.Н., Золотарев В.В., Попов А.М. Поддержка принятия решений при проектировании систем защиты информации: монография. М.: ИНФРА-М, 2017. 130 с.
4. Колобкова А.А. Учебные книги по французскому языку в России XVIII века / А.А. Колобкова // Проблемы современного образования. 2020. № 5. С. 163-171. DOI 10.31862/2218-8711-2020-5-163-171.
5. Корнилов М.Я. О сущности экономической безопасности // Проблемы теории и практики управления. 2015. № 8. С. 123-129.
6. Кузнецова Е.И. Экономическая безопасность: учебник и практикум. М.: Юрайт, 2019. 294 с.
7. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью: учебное пособие. М.: Горячая линия-Телеком, 2016. - 244 с.
8. Масалков А.С. Особенности киберпреступлений: инструменты нападения и защита информации. М.: ДМК Пресс, 2018. 224 с.
9. Мягкова С.Н., Литвинов С.В. Организация и проведение физкультурных парадов в СССРв 30-е годы XX в // Вестник спортивной истории. 2015. № 1. С. 12-20.
10. Озёрский С.В., Попов И.В., Рычаго М.Е., Улендеева Н.И. Информационная безопасность: практикум. Самара: Самарский юридический институт ФСИН России, 2019. 84 с.
11. Российская Федерация. Приказ ФСТЭК России от 11.02.2013 г. № 17. http://www.consultant.ru/document/cons_doc_LAW_108546/
12. Российская Федерация. Указы. О стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 31.12.2015 №683: редакция от 31 декабря 2015 года.
http://www.consultant.ru/document/cons_doc_LAW_191669/61a97f7ab0f2f3757fe034d11011c763bc2e593f/
13. Российская Федерация. Указы. О стратегии экономической безопасности Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 12.05.2017 № 208: редакция от 12 мая 2017 года. http://www.consultant.ru/document/cons_doc_LAW_216629/
14. Тараскин М.М., Захаров А.Г., Коваленко Ю.И., Москвитин Г.И. Комплексная защита информации в организации: монография. М.: РУСАЙНС, 2020. 353 с.
15. Торба О.И., Торба Д.О., Коваленко Ю.И., Тараскин М.М. Межгосударственное правовое нормативное обеспечение в области информационной безопасности: монография. М.: РУСАЙНС, 2019. 439 с.

Methods and methods of ensuring information security of an economic entity

Vitaly A. Kuchkovsky
4rd year bachelor's degree student, BBBO-05-18
Institute for Cybersecurity and Digital Technologies
Moscow, Russia
vitaslol221@gmail.com
0000-0000-0000-0000

Sergey A. Tronin
Candidate of Economics, Associate Professor
Department of Financial and Investment Management
Financial University under the Government of the Russian Federation
Moscow, Russia
tron1977@rambler.ru
0000-0000-0000-0000

Received 16.01.2022
Accepted 24.02.2022
Published 15.04.2022

10.25726/k9453-8903-4632-o

Abstract

The article discusses the problems of information security, which are exacerbated by the processes of penetration into all spheres of human life of technical means of data processing and transmission and, above all, computing systems. Information security, as well as information security, is a complex and multifaceted task, directly aimed at ensuring security, implemented by the introduction of an information security system, information security specialists are currently forming an understanding of an integrated information security system. In the usual sense, information security is presented directly as a state of security, the ability to resist and counter threats.

Keywords

information protection, information security, electronic document management system, digital technologies.

References

1. Birjukov A. A. Informacionnaja bezopasnost': zashhita i napadenie. 2-e izd., pererab. i dop. M.: DMK Press, 2017. 433 s.
2. Birjukov A.A. Informacionnaja bezopasnost': zashhita i napadenie. M.: DMK Press, 2017. 433 s.
3. Buhtojarov V.V., Zhukova M.N., Zolotarev V.V., Popov A.M. Podderzhka prinjatija reshenij pri proektirovanii sistem zashhity informacii: monografija. M.: INFRA-M, 2017. 130 s.
4. Kolobkova A.A. Uchebnye knigi po francuzskomu jazyku v Rossii XVIII veka / A.A. Kolobkova // Problemy sovremennogo obrazovanija. 2020. № 5. S. 163-171. DOI 10.31862/2218-8711-2020-5-163-171.
5. Kornilov M.Ja. O sushhnosti jekonomicheskoj bezopasnosti // Problemy teorii i praktiki upravlenija. 2015. № 8. S. 123-129.
6. Kuznecova E.I. Jekonomicheskaja bezopasnost': uchebnik i praktikum. M.: Jurajt, 2019. 294 s.
7. Kurilo A.P., Miloslavskaja N.G., Senatorov M.Ju., Tolstoj A.I. Osnovy upravlenija informacionnoj bezopasnost'ju: uchebnoe posobie. M.: Gorjachaja linija-Telekom, 2016. - 244 s.
8. Masalkov A.S. Osobennosti kiberprestuplenij: instrumenty napadenija i zashhita informacii. M.: DMK Press, 2018. 224 s.
9. Mjagkova S.N., Litvinov S.V. Organizacija i provedenie fizkul'turnyh paradov v SSSRv 30-e gody XX v // Vestnik sportivnoj istorii. 2015. № 1. S. 12-20.
10. Ozjorskij S.V., Popov I.V., Rychago M.E., Ulendeeva N.I. Informacionnaja bezopasnost': praktikum. Samara: Samarskij juridicheskij institut FSIN Rossii, 2019. 84 s.
11. Rossijskaja Federacija. Prikaz FSTJeK Rossii ot 11.02.2013 g. № 17. http://www.consultant.ru/document/cons_doc_LAW_108546/

12. Rossijskaja Federacija. Ukazy. O strategii nacional'noj bezopasnosti Rossijskoj Federacii: Ukaz Prezidenta Rossijskoj Federacii ot 31.12.2015 №683: redakcija ot 31 dekabrja 2015 goda. http://www.consultant.ru/document/cons_doc_LAW_191669/61a97f7ab0f2f3757fe034d11011c763bc2e593f/

13. Rossijskaja Federacija. Ukazy. O strategii jekonomicheskoj bezopasnosti Rossijskoj Federacii na period do 2030 goda: Ukaz Prezidenta Rossijskoj Federacii ot 12.05.2017 № 208: redakcija ot 12 maja 2017 goda. http://www.consultant.ru/document/cons_doc_LAW_216629/

14. Taraskin M.M., Zaharov A.G., Kovalenko Ju.I., Moskvitin G.I. Kompleksnaja zashhita informacii v organizacii: monografija. M.: RUSAJNS, 2020. 353 s.

15. Torba O.I., Torba D.O., Kovalenko Ju.I., Taraskin M.M. Mezhgosudarstvennoe pravovoe normativnoe obespechenie v oblasti informacionnoj bezopasnosti: monografija. M.: RUSAJNS, 2019. 439 s.