ОСНОВНЫЕ ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.А. Какорин, *студент*
Волгоградский государственный университет
(Россия, г. Волгоград)

DOI:10.24412/2500-1000-2023-2-2-25-27

Аннотация. *В статье рассмотрены основные принципы информационной безопасности. Основные компоненты информационной безопасности чаще всего сводятся к так называемой триаде: конфиденциальность, целостность и доступность. Информационная безопасность – это набор методов, предназначенных для защиты данных от несанкционированного доступа или изменения.*

Ключевые слова: *информационная безопасность, целостность, доступность, конфиденциальность.*

Если предприятие или организация обрабатывает персональные данные, хранит бухгалтерскую информацию, клиентскую базу, профили сотрудников или коммерческую тайну, эти данные должны быть защищены. Я уверен, что и любой человек не захочет, чтобы другие люди получили его личные данные, читали его сообщения, смотрели личные фотографии, получили доступ к его почте или облачному хранилищу. Вся информация нуждается в защите, вот поэтому важна информационная безопасность. Благодаря широкому использованию цифровых технологий количество информации в организациях, нуждающихся в защите от угроз безопасности, постоянно растет. Всем, от крупных глобальных корпораций до небольших компаний, всем, кто использует технологии для ведения своего бизнеса, нужна помощь в предотвращении нарушений безопасности.

Информационная безопасность – это различные меры по защите информации от посторонних лиц [1]. Например, нашу личную информацию мы защищаем двухфакторной аутентификацией, разрешения пользователей, настройкой брандмауэра. Информационную безопасность следует понимать как защиту всей информации. Эта информация может быть физической, например, тетрадь с вашими рукописями, флеш накопитель с данными, или цифровой, например, электронная медицинская карта или цифровой документ.

Информационная безопасность основывается на трех основных свойствах информации: конфиденциальность, целостность и доступность. Эти принципы, с аспектами которых вы можете сталкиваться ежедневно, и именно они лежат в основе стандартов защиты данных.

Конфиденциальность ограничивает доступ к информации, доступ имеют только те лица, у которых есть на это право. Например, только вы знаете PIN-код или пароль для разблокировки телефона или компьютера, пароль электронной почты, пароль от личного кабинета Госуслуг и т.д. Когда узнают пароль или пытаются разными способами войти в ваш личный кабинет, воспользоваться телефоном, компьютером или почтовом ящиком, то нарушается конфиденциальность. Термин целостность подразумевает сохранность информации в исходном состоянии и не подвергается изменению без разрешения собственника. Если злоумышленник получит доступ к вашей электронной почте, удалит часть писем, изменит текст некоторых писем, все это приведет к нарушению целостности. Целостность гарантирует, что данные.

могут быть изменены только авторизованными пользователями, защищая информацию как достоверную и представляя организацию или сайт как заслуживающие доверия. Доступность означает, что в любой момент вы можете воспользоваться информацией, для которой у вас есть доступ. Например, вы можете войти в свой

личный кабинет портала государственных услуг Российской Федерации или личный кабинет студента в любое время. Если в это время происходит атака хакерами серверов, то доступ к личным кабинетам будет недоступен, а это поставит под угрозу доступность. Доступность требует, чтобы информация была доступна авторизованным пользователям в любое время, когда они в ней нуждаются. Для этого необходимо обновлять системы и создавать резервные копии программного обеспечения [2].

Информация может быть публичной и конфиденциальной. Доступ к публичной информации есть у всех, а к конфиденциальной информации доступ ограничен и к нему имеют доступ только ограниченный круг лиц [3]. Так как к публичной информации есть доступ у всех лиц, то может показаться, что она не нуждается в защите. Но это не так, на нее не распространяется только принцип конфиденциальности, но она соответствовать двум другим принципам – целостности и доступности. Например, давайте рассмотрим сайт Большой российской энциклопедии. В ней представлены различные сведения, универсальные словари – вся эта уникальная информация находится в открытом доступе, и ее может просмотреть любой желающий. Но сайт все же нужно защитить, чтобы никто не нарушал его работу (например, не менял важную информацию в словарях, заметках или не нарушил его работу).

Если провести параллель между «цифровой» и «доцифровой» эпохой, то можно увидеть похожую структуру. Раньше важная документация хранилась в сейфах, нанимался персонал для охраны и шифровались сообщения на бумажных носителях для защиты данных. Сегодня же для защиты цифровой информации используются по факту те же меры защиты: специалисты в области информационной безопасности создают защищенные пространства (виртуальные «сейфы»), используют защитное программное обеспечение («привлекают охрану»), и пользуются криптографическими методами для шифрования цифровой информации.

Самым слабым звеном в информационной безопасности считается человеческий фактор. Самая большая часть всех инцидентов информационной безопасности – это результат непреднамеренного действия человека. Возможностей для этого множество: от ошибок ввода данных при работе с локальными сетями или Интернетом до потери носителя информации, от пересылки данных по незащищенным каналам связи непреднамеренной загрузки вирусов с различных сайтов.

Заключение. С развитием цифровизации общества развивается информационная безопасность, которая отвечает за защиту данных и обеспечение их конфиденциальности, целостности и доступности. Защита требует комплексного подхода. Он выражается в разработке соответствующих политик информационной безопасности, найме сотрудников, ответственных за информационную безопасность, управление документооборотом, контролем и мониторингом пользователей, внедрением современных механизмов аутентификации и др.

Библиографический список

1. Галушкин, А.А. К вопросу о значении понятий "национальная безопасность", "информационную безопасность", "национальная информационная безопасность" / А.А. Галушкин // Правозащитник. – 2015. – № 2. – С. 8. – EDN RTDVEB.

2. Дегтярев, Д.И. Безопасная компиляция и архитектуры защищенных модулей / Д.И. Дегтярев, О.А. Какорина // Безопасность информационных систем и технологий в условиях цифровой экономики : Материалы IX Всероссийской научно-практической конференции с международным участием, Волгоград, 27–28 октября 2021 года / Редколлегия: О.А. Какорина, Ю.С. Бахрачева, Т.А. Попова. – Волгоград: Волгоградский государственный университет, 2021. – С. 23-26.

3. Автоматизация процесса определения класса защищенности информационной системы и мер для ее защиты / С.П. Сазонов, Н.И. Федонюк, М.А. Кузнецова [и др.] // Защита информации. Инсайд. – 2021. – № 3 (99). – С. 44-46.

BASIC PRINCIPLES OF INFORMATION SECURITY

I.A. Kakorin, *Student*
Volgograd State University
(Russia, Volgograd)

Abstract. *The article deals with the basic principles of information security. The main components of information security are most often reduced to the so-called triad: confidentiality, integrity and availability. Information security is a set of techniques designed to protect data from unauthorized access or alteration.*

Keywords: *information security, integrity, accessibility, confidentiality.*