ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ЧТО ЭТО ТАКОЕ В СОВРЕМЕННЫХ РЕАЛИЯХ

Богомолова Л.В.

Богомолова Людмила Валерьевна – студент,
кафедра «Вычислительные системы, сети и информационная безопасность»,
Российский университет транспорта, г. Москва

Аннотация: *в статье рассматривается понятие информационной безопасности, ее общий смысл, рассмотрены виды атак, а также виды угроз, отличия между кибербезопасностью и информационной безопасностью*
Ключевые слова: *информационная безопасность, угрозы информационной безопасности, атаки, виды угроз.*

INFORMATION SECURITY: WHAT IS IT IN MODERN REALITIES

Bogomolova L.V.

Bogomolova Lyudmila Valerievna - student,
DEPARTMENT OF "COMPUTER SYSTEMS, NETWORKS AND INFORMATION SECURITY",
RUSSIAN UNIVERSITY OF TRANSPORT, MOSCOW

Abstract: *the article discusses the concept of information security, its general meaning, the types of attacks, as well as the types of threats, the differences between cybersecurity and information security*
Keywords: *information security, information security threats, attacks, types of threats.*

В настоящее время жизнь без доступа к интересующей информации в любое время и в любом месте с помощью бесчисленных типов устройств стала невообразимой. Однако его безопасность стала более важной, чем сам доступ к информации. Почему же?

Потому что средства связи и коммуникации, а также все точки доступа, которые мы используем, например, социальные сети, интернет-магазины, онлайн-банки, мессенджеры, потенциально очень уязвимы.

Для защиты данных от утечки или хищения или, например, взлома программы или компьютерной системы в современной реалии есть отрасль, которая называется информационная безопасность.

Информационная безопасность включает в себя инструменты и процессы, которые компании и системы применяют в качестве защиты информации. Сюда могут относить параметры политики, которые предотвращают доступ неавторизованных пользователей к деловой или личной информации.

Информационная безопасность — есть область, которая постоянно растет и развивается, которая включает обширный спектр отраслей, от безопасности сети и инфраструктуры вплоть до тестирования, а также аудита.

Здесь происходит защита конфиденциальных сведений от несанкционированного доступа, а также действий, включая проверку, запись и любое другое нарушение или уничтожение. Суть заключается в том, чтобы создать безопасность и конфиденциальность критически важных данных, таких как данные учетной записи клиента, финансовые данные или интеллектуальная собственность.

Последствия инцидентов безопасности охватывают кражу личных данных, фальсификацию сведений, а также их удаление. Атаки могут нарушить рабочие процессы и причинить ущерб репутации фирмы или компании, а также иметь ощутимую стоимость.

3 принципа информационной безопасности

Три ключевых принципа, которым необходимо соответствовать ИБ – конфиденциальность, целостность, доступность. Поговорим про каждую из них отдельно.

— Принцип конфиденциальности: гарантирует возможность получения информации только легитимным пользователям. Это означает внедрять в действие контроль, чтобы обеспечить необходимую степень безопасности с данными организации, активами и информацией на разных стадиях деловых операций с целью предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите посредством рядовых организаций вне зависимости от ее формата.

— Принцип целостности: информация в системе обязана быть актуальной, верной и полной. Целостность также обеспечивает предотвращение искажения данных, сохранение точности и полноты данных. То есть, данные никак не могут быть отредактированы несанкционированным способом.

— Принцип доступности: означает, что к информации может получить доступ только тот, кто имеет на это право, а также значит, что информация будет доступна, когда в этом возникнет необходимость. Атака вида «отказ в обслуживании» считается одним из факторов, которые могут препятствовать доступности данных.

Информационная безопасность против кибербезопасности

Информационная безопасность отличается от кибербезопасности как масштабом, так и целью. Эти два термина часто используются взаимозаменяемо, но, если быть точнее, кибербезопасность — это подкатегория информационной безопасности. Информационная безопасность — это широкая область, охватывающая множество областей, таких как физическая безопасность, безопасность конечных точек, шифрование данных и сетевая безопасность. Он также тесно связан с обеспечением безопасности информации, которая защищает информацию от таких угроз, как стихийные бедствия и отказы серверов.

Кибербезопасность в первую очередь касается угроз, связанных с технологиями, с помощью методов и инструментов, которые могут предотвратить или смягчить их. Другой родственной категорией является безопасность данных, которая фокусируется на защите данных организации от случайного или злонамеренного доступа к неавторизованным сторонам.

Активные и пассивные атаки

Информационная безопасность предназначена для защиты организаций от вредоносных атак. Существует два основных типа атак: активные и пассивные. Считается, что активные атаки сложнее предотвратить, и основное внимание уделяется их обнаружению, смягчению последствий и восстановлению после них. Пассивные атаки легче предотвратить с помощью строгих мер безопасности.

Активная атака

Активная атака включает в себя перехват сообщения или сообщения и его изменение для злонамеренного воздействия. Существует три распространенных варианта активной атаки:

- Прерывание — злоумышленник прерывает исходное общение и создает новые вредоносные сообщения, выдавая себя за одну из общающихся сторон.
- Модификация — злоумышленник использует существующие коммуникации и либо воспроизводит их, чтобы обмануть одну из общающихся сторон, либо модифицирует их, чтобы получить преимущество.
- Изготовление — создание фальшивых или синтетических сообщений, как правило, с целью достижения отказа в обслуживании (DoS). Это предотвращает доступ пользователей к системам или выполнение обычных операций.

Пассивная атака

При пассивной атаке злоумышленник отслеживает, контролирует систему и незаконно копирует информацию, не изменяя ее. Затем они используют эту информацию для нарушения работы сетей или компрометации целевых систем.

Злоумышленники не вносят никаких изменений в связь или целевые системы. Это затрудняет обнаружение. Однако шифрование может помочь предотвратить пассивные атаки, поскольку оно запутывает данные, затрудняя их использование злоумышленниками.

Угроза безопасности информации

Угроза безопасности информации – это возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию.

Виды угроз:

1. Основные нарушения:

2. Характер происхождения угроз.

Три наиболее выраженные угрозы:

· подверженность физическому искажению или уничтожению;

·возможность несанкционированной (случайной или злоумышленной) модификации;

· опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

Источники угроз (под источником понимается непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию):

· люди;

· технические устройства;

· модели, алгоритмы, программы;

· технологические схемы обработки;

· внешняя среда.

Предпосылки появления угроз:

объективные (количественная или качественная недостаточность элементов системы) – причины, не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

субъективные – причины, непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Список литературы / References

1. Особенности системы информационнойбезопасности как элемента международной безопасности в современном мире [Электронный ресурс]. Режим доступа: http://publishing-vak.ru/file/archive-politology-2017-1/19-pelevina.pdf\ (дата обращения: 08.01.2023).