

ИНФОРМАЦИОННЫЕ СИСТЕМЫ КАК ОСНОВНОЙ ОБЪЕКТ КИБЕРБЕЗОПАСНОСТИ

Мусаев Анвар Исакович,

Доцент кафедры «Коммуникация и информационные
технологии» Университета «Vatan», кандидат технических наук
(PhD).

Хакимова Регина Маратовна,

студент 3-курса Университета «Vatan»

***Аннотация.** В этой статье рассматривается понятие кибербезопасности и информационной безопасности, которая в настоящее время становится очень распространенной. Понятие “кибербезопасности” используется как синоним вместе с понятием “информационная безопасность”. Но объяснить угрозы в области информационных технологий с понятием “информационная безопасность”, которое считается классическим в настоящее время ввиду появлением новых видов типов угроз затруднительно. Исходя этого термин кибербезопасности рассматривается как новая парадигма в этом направлении.*

***Ключевые слова:** кибернетика, кибербезопасность, хакер, вирус, кибератака, информационная безопасность, система, объект, конфиденциальность, целостность, доступность.*

Введение

Все мы привыкли использовать интернет в повседневной деятельности. Поиск информации в сети Интернет осуществляется с использованием различных электронных устройств имеющей в своем составе управляющую систему этого цифрового устройства-операционную систему, компьютеры и мобильные устройства,

читаем, загружаем и сохраняем нужную информацию. При осуществлении этой деятельности мы используем интернет-сервисы и ресурсы, которые выполняют функции хранения, предоставления, визуализации и передачи контента. Угрозы нашей безопасности возникают в результате того, являются ли эти интернет-сервисы и источники искомого контента действительно безопасными или нет.

При использовании сети соблюдается и выполняется разработанные требования безопасности при использовании сети Интернет. Из этих самыми основными требованием является то, чтобы не загружать зараженный вирусом вредоносный контент, который при запуске содержимого выполняет вредоносные действия в этой системе в интересах хакера. С выполнением таких мер обеспечивается безопасность системы.

В настоящее время в средствах массовой информации все большую популярность приобретают термины кибербезопасность, кибератака, киберугрозы и хакерство. Эти понятия используются вместе с понятием информационной безопасности. Это требует различения двух понятий, которые должны объяснить суть вредоносных действий в области информационных технологий.

Научное обоснование использования этих терминов также считается неоднозначным. Изучая понятие Кибербезопасность, мы видим, что этот термин состоит из двух частей, это термины “кибер” и “безопасность”.

Слово кибер происходит от слова кибернетика (др.-греч.Κυβερνήτης-искусство управления судами) это понятие ввел в науку французский ученый, физик, математик Андре-Мари Ампер в 1834 году, назвав кибернетику «эффе́ктивным управлением» [1]. Это

понятие в значительной степени связано с системой государственного управления, благодаря которой управление может быть легко осуществлено государством, основанным на этой кибернетической точки зрения, для создания лучших условий проживания для своих граждан.

После этого в 1948 году американский ученый-математик, основатель кибернетики и искусственного интеллекта Норберт Винер впервые предложил кибернетику как современную науку [1]. В этом случае кибернетика включает изучение черного ящика и аналогичных систем, а также обратной связи, возникающей в системе управления, коммуникации и самоорганизации в живых организмах, машинах и организациях. Кибернетика фокусируется на том, как система (цифровая, механическая или биологическая) обрабатывает любую информацию, обрабатывает информацию, которая представляет собой две задачи, возложенные на нее, либо в результате изменения ее состава или функции в результате реакции на это информационное воздействие, либо в результате изменения части системы в результате других воздействий, который позволить системе лучше выполнять задачи по реагирования на это воздействие.[1]

Слово "безопасность системы" или "уровень безопасности" системы является общим показателем, оценивающей воздействий будущему существованию любой системы, ее выживанию в будущем.

Слово "кибер" обозначает эффективное управление в произвольной материальной, живой и нематериальной системе. В любой системе, когда его управление приводит к полезному или вредному результату, это оценивается, что система готов

существованию, выживанию в будущем или требуется исчезновению этой системы, ее выходу из строя. При оценке выполнения задач поставленные перед отдельными ее подсистемными частями, являющимися компонентами этой системы считается эффективными, полезными в управлении то эта система с точки зрения кибербезопасности обеспечен.

При выявлении системой несовершенных подсистем и выполняя процедуры удаления этих подсистем или качественное усовершенствование подсистем позволяет в дальнейшем выполнении функций всей системы считается что кибербезопасность этой системы обеспечена.

Вместе с тем понятие системы тоже является ключевым. Слово система происходит от латинского "Systema", древнегреческого "συστήμα", что означает "целое множество, состоящее из нескольких компонентов (элементов); сумма". Система — это совокупность простых элементов как единого целого, взаимосвязанного по определенным правилам для достижения единой цели. Каждый простой элемент в наборе также может быть системой в свою очередь. Совокупность объектов тоже является системой при выполнении функций для достижения единой цели.

В информационных системах функционирующих в интернете сервисах задачей является предоставления интересного контента и внедрение рекламы. При выполнении этих задач если источник контента выполняет и другие цели, например, распространяет зараженный контент преднамеренно или ввиду некомпетентности непреднамеренно в обоих случаях эта система обречен провалу, то

есть из-за необеспеченности кибербезопасности эта система потеряет подписчиков и в будущем перестает существовать.

Понятие кибербезопасности применяется к системе управления системой. Кибербезопасность — это наука, которая изучает как полезные, так и вредные эффекты, которые могут повлиять на общую часть управления любой системой, чтобы гарантировать ее существование в будущем.

В настоящее время кибербезопасность стала важной функцией цифровых электронных систем. Становление важной особенностью, в свою очередь, объясняется тем, что увеличивается количество способов дистанционного взаимодействия по сети с любыми цифровыми системами, даже эти вредоносные воздействия вызывают сбой системы, прекращение ее функционирования (исчезновение), изменение ее функционирования (модификация) или переориентацию системы на совершенно другую цель (redirect).

До сих пор в литературе понятие информационной безопасности широко используется и в научной сфере. 3 основных принципа информационной безопасности они направлены на обеспечение конфиденциальности информации (Confidentiality), целостности информации (Integrity) и постоянной готовности информации к использованию (Availability) [2, 3]. Основным объектом информационной безопасности является передаваемая или обрабатываемая информация.

Из этого можно сделать вывод, что использование понятия информационной безопасности при обеспечении безопасности объектов, организованных из сложных систем, не является эффективным, и более эффективным является применение к системе

дополнительных понятий, а не информации как основного объекта. По этой причине концепция кибербезопасности является оптимальной парадигмой для сложных систем. Основным объектом кибербезопасности являются целые информационные системы, которые и применяются и к другим объектам.

Объектом информационной безопасности является «информация», объектом кибербезопасности – «система». Существующие в настоящее время угрозы информационных технологий не может полностью объясниться через понятие информационной безопасности, финансирование преступлений с помощью криптовалют, захват информации с помощью социальной инженерии, мошенничество с помощью “ fishing-smishing-voicemishing-farming”, угрозы связанные с банковскими картами, воздействие деятельности системы, организации или личности, то есть распространение “фейковых” сообщений, “deepfake” подготовка и распространение информации, вредной для деятельности личности, общества и государства, в социальных сетях, создание секретных групп в социальных сетях, незаконное владение информационных объектов через ботнеты. Объяснение этих вредоносных информационных явлений с помощью концепции кибербезопасности является эффективным.

В обеспечении информационной безопасности большое значение имеет и обеспечение кибербезопасности. человек или предприятие подвергаются кибератаке deerfake. Deerfake-это угроза жизни реального человека путем создания его цифрового имиджа с использованием информационных технологий и, таким образом, распространения ложной информации о личности. В этом случае

целостность, конфиденциальность и доступность информации не нарушена с точки зрения информационной безопасности. С точки зрения кибербезопасности, deepfake влияет на этого человека на его жизнедеятельность. Наносит ущерб социальным, экономическим и жизненным интересам человека. А распространение этой ложной deepfake информации в интернете информационной системой, каналом блогера или источником мультимедийного контента типа инстаграмм, тик-ток или youtube поставить в сомнение этих систем и снизить рейтинг этих информационных систем, которые будет влиять на его существование в будущем.

Таким образом, оценка кибератаки deepfake с точки зрения кибербезопасности будет иметь более научную основу, чем оценка deepfake с точки зрения информационной безопасности.

Принимая во внимание классическое понятие компьютерных вирусов, с точки зрения информационной безопасности [4], для объяснения нарушения целостности, конфиденциальности и доступности передаваемой информации требуется более широкое объяснение, использование дополнительных терминов.

С точки зрения кибербезопасности, научное объяснение приводиться к тому что компьютерная система управления-операционная система-является объектом и предназначена для выполнения своих функций. Но из-за имеющегося недостатка в его объекте, а точнее из-за несовершенства его управления, эта операционная система не сможет выполнять свою функцию в результате заражения вирусом. В результате выживание этой системы, то есть использование этой операционной система-объекта в

будущем будет пересмотрен в связи с недостаточной кибербезопасности.

Заключение.

В современном мире информационные системы для жизни общества стали важной и неотъемлемой частью, и что его выдвигает его на первый план по обеспечению кибербезопасности. Для государства и общества становится необходимым в доступности этих информационных систем, что требует тратить ресурсы на обеспечение кибербезопасности. Расходуемые ресурсы подразделяются на материальные, научные и человеческие. Человеческие ресурсы связаны с уровнем образования и означают, что в этой области должны работать специалисты, знающие суть проблем кибербезопасности и пути их решения.

Литература.

1. Wiener N . Cybernetics or Control and Communication in the Animal and the Machine. — New York: The Technology Press and John Wiley & Sons, Inc. — Paris: Hermann et Cie, 1948.
2. Борьба с преступностью в киберпространстве: проблемы и решения, сборник материалов Республиканской научно-практической конференции, Академия МВД РУ, (24 февраля 2022 г.), Ташкент: MALIK PRINT Co., 2022. -482 С.
3. Акбаров D.E., Криптографические методы обеспечения информационной безопасности и их применение, “Ташкент, издательство “O‘zbekiston markasi ”, 2009 – 432 с.
4. Акбаров D.E, Мусаев A.И. Исследование основ существующих алгоритмов поточного шифрования и их классификация, Ташкент,

Axborotkommunikatsiyalar: tarmoqlar, texnologiyalar, yechimlar,
“UNICON.UZ”, 2009. C. 36-45.