ПОНЯТИЕ КИБЕРБЕЗОПАСНОСТИ, ТЕМЫ И ОСНОВНЫЕ НАПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Гайшун А.С.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Подключенная электронная информационная сеть стала важной частью нашей обычной жизни. Эта сеть используется в организациях любого типа: медицинских, финансовых, образовательных – без нее в наши дни эффективная работа невозможна. В сети происходят сбор, обработка, хранение и обмен огромного количества данных. Чем больше цифровой информации собирается и чем больше ею размениваются, то важнее становится защита этой информации для обеспечения национальной безопасности и экономической стабильности.

Кибербезопасность – это комплекс мер и технологий, направленных на обеспечение защиты информации от киберугроз. Под киберугрозами понимаются различные виды угроз, которые могут нанести вред компьютерным системам, сетям и данным. К таким угрозам относят: вредоносное программное обеспечение, кибератаки, утечки данных, фишинг и другие виды киберпреступности. Также выделяют 3 уровня кибербезопасности: личный, корпоративный и государственный. На своем личном уровне нужно заботится о защите своей учётной записи, своих данных и своих гаджетов. На корпоративном уровне долгом всех работников считается забота о защите репутации организации, ее клиентов и данных. На государственном уровне на кон поставлены национальная безопасность, охрана порядка и благополучие граждан.

Чем больше ты пропадаешь в интернете, тем больше твоя аутентификация (онлайн и оффлайн) может воздействовать на тебя и твою жизнь. Твоя оффлайн-аутентификация – это ты сам, тот ты, кто повседневно общается с коллегами и своей семьей дома, на учёбе. Близкие знают твои личные данные, например фамилия, имя или возраст, место проживания. Твоя онлайн-аутентификация – это ты в киберпространстве.

Киберпространство – это сложная среда, которая возникает в результате взаимодействия людей, программного обеспечения и услуг в интернете и поддерживается распределенными по всему миру физическими устройствами информационных и коммуникационных технологий (ИКТ) и подключёнными сетями. Твоя онлайн-аутентификация – это то, как ты представляешь себя в сети. Эта онлайн-аутентификация должна демонстрировать минимальное количество данных о тебе, чтобы не привлечь внимание злоумышленников. [1, с.19]

Основные темы кибербезопасности включают в себя:

1. Защита от вредоносного программного обеспечения – разработка антивирусных программ, брандмауэров и других средств защиты от вредоносных программ.

2. Защита от кибератак – обеспечение защиты данных и систем от несанкционированного доступа и атак. Чтобы не войти в число пострадавших от кибератак ты должен: не экономить на безопасности(т.е. не пользоваться “пиратским” ПО, или ПО загруженное с неофициальных и подозрительных сайтов); использовать пароли с сочетанием цифр, заглавных и строчных букв и специальных символов, при этом надо изменять пароль как минимум раз в год; и разумеется быть бдительным при открытии электронных писем или сайтов.

3. Защита персональных данных – обеспечение конфиденциальности и целостности персональной информации пользователей.

4. Безопасность в облаке – обеспечение безопасности данных, хранящихся и обрабатываемых в облачных сервисах. Желательно не хранить данные в одном месте.

5. Защита от кибершпионажа – предотвращение утечек конфиденциальной информации и шпионажа через компьютерные системы.

Для защиты своих данных рекомендуется: регулярно обновлять свой компьютер и программное обеспечение; как можно реже использовать аккаунт с правами администратора; быть осторожным, когда нажимаете на ссылки и загружаете приложения; быть осторожным, когда открываете прикрепленные к письмам файлы и даже изображения; не доверять всплывающим окнам, в которых предлагается что-то загрузить; соблюдать осторожность в файлообменных системах; использовать антивирусное ПО (например, Kaspersky). [2]

А к основным направлениям кибербезопасности относят:

1. Криптографию – науку о способах обеспечения конфиденциальности данных, их целостности и подлинности путем шифрования данных.

2. Сетевую безопасность – обеспечение защиты сетевых ресурсов от несанкционированного доступа.

3. Управление доступом – контроль доступа к информационным ресурсам и управление привилегиями.

4. Безопасность приложений – обеспечение безопасности программного обеспечения.

5. Инцидентное реагирование – совокупность действий по выявлению и устранению кибератаки на базу данных компании, прекращению утечки данных, с целью минимизации ущерба и максимизации скорости возвращения организации к нормальной работе.

Таким образом можно сделать вывод, что кибербезопасность играет ключевую роль в современном информационном обществе, и ее значимость будет продолжать расти по мере развития цифровых технологий. Понимание основных тем и направлений кибербезопасности поможет эффективно защитить информацию и данные от киберугроз. Важно осознавать угрозы киберпреступности и принимать необходимые меры для обеспечения безопасности в цифровом мире.

Литература

1. Лутонин А. С. Введение в кибербезопастность. : Учебное пособие для студентов вузов. [Текст] / А.С. Лутонин – Санкт-Петербург, 2022. – 63с.

2. Как защитится от кибератак. // [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/research/knowledge-base/kak-zashchititsya-ot-kiberatak/ Дата доступа: 25.03.2024.

ВРЕДОНОСНЫЕ ПРОГРАММЫ И ИХ КЛАССИФИКАЦИЯ. ОСНОВНЫЕ КАНАЛЫ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ И ДРУГИХ ВРЕДОНОСНЫХ ПРОГРАММ

Гутырчик К.А., Котович Е.Д.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В нынешнее время, в эпоху цифровых технологий и программирования пользователи подвергаются высоким рискам, связанным с угрозой их компьютерной и персональной безопасности, а также утечками пользовательских данных в сети Интернет. Данные процессы в большинстве своих случаев возникают в связи с нахождением вредоносных или же вирусных программ и плагинов на персональном устройстве пользователя. Вредоносные программы являются одним из главных инструментов злоумышленников для нанесения ущерба за получение пользовательской информации и данных, а также внедрения своих вредоносных материалов. В данной сфере, важным аспектом является понимание классификации, видов, а также методов заражения таковыми программами. [3]

Современным обществом принято выделять следующие типы вредоносных программ:

1. Файловые вирусы — это программы, способствующие заражению исполняемых файлов, добавляя в них свой код. Этот процесс позволяет им передаваться на другие компьютеры через уже зараженные файлы. [4]