ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Murodullayeva Rayhona Abdurahmon qizi
Ma'rufjonov Maqsudjon Mansurjon o'g'li
Nabiyev Iskandar Farxodjon o‘g‘li
Студенты Ферганского филиала ТУИТ
имени Мухаммеда аль-Хорезмий

Аннотация: В данной статье рассмотрены средства защиты информации в компьютерных системах и сетях, угрозы и виды атак, специфические организационные, технические или аппаратные, программные, правовые, физические, криптографические, средства защиты информации в каналах связи компьютерных сетей и защиты от вирусов широко освещаются. Различные виды информации вошли в нашу повседневную жизнь через международную компьютерную сеть Интернет, независимо от географического положения. Благодаря этой компьютерной сети быстро формируется информационное общество. Понятие государственных границ исчезает при путешествии в мир информации. Глобальная компьютерная сеть коренным образом меняет государственное управление, то есть подробно разъясняются проблемы управления механизмом распространения публичной информации, а также создание современных компьютерных систем и появление глобальных информационных сетей, проблемы защиты информации.

Ключевые слова: компьютер, технология, интернет, биометрический, онлайн, конфиденциальный, электронный, технический, сертификат, администратор, ресурс, версия, блокировка, брандмауэр.

В последние годы компьютерные технологии прочно вошли в нашу жизнь. В наше время людям очень сложно представить, как они работали без компьютеров, настолько они к ним привыкли. С появлением компьютеров люди стали активно пользоваться электронной почтой Интернета, Всемирной паутиной и услугами интернет-банкинга. Теперь каждое утро обычного человека стандартно просматривать ленту новостей, проверять содержимое личной почты, посещать различные популярные социальные сети, совершать покупки в интернет-магазинах, оплачивать различные услуги. начинается с Интернет развивался медленно, но верно. постоянный помощник в нашей повседневной работе. Интернет облегчает общение и устраняет языковые барьеры, теперь даже если ваш друг живет за тысячу километров от вас, в другом городе или даже в другой стране, при желании вы можете общаться с ним хоть целый день. Но при всех преимуществах Интернета он таит в себе и немало опасностей. Прежде

всего, это угроза личной и государственной безопасности. Интернет – это пространство, где личная информация, данные банковских карт могут быть легко украдены, в Интернете ведутся информационные войны, происходят информационные конфликты.

Таким образом, угроза информационной безопасности является одной из важнейших проблем жизни современного человека, и нам необходимо знать, откуда она исходит и как можно защититься.

Жизнь современного общества невозможно представить без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу ядерных реакторов, распределяют энергию, контролируют расписание поездов, управляют самолетами, космическими кораблями. Компьютерные сети и телекоммуникации предопределяют надежность и возможности систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и представление потребителям, тем самым внедряя информационные технологии. Однако именно высокий уровень автоматизации создает риск снижения безопасности (личной, информационной, государственной и т. д.). Доступность и широкое использование информационных технологий и компьютеров делают их весьма уязвимыми для разрушительных влияний.

Создание Интернет-технологий расширило возможности быстрого и простого получения информации из различных источников для всех – от простых граждан до крупных организаций. Государственные учреждения, научные и образовательные учреждения, коммерческие предприятия и частные лица стали создавать и хранить информацию в электронном виде. Эта среда предлагает большие преимущества по сравнению с предыдущим физическим хранилищем: хранилище очень компактно, передача происходит мгновенно, а доступ к обширным базам данных по сети очень обширен. Возможности эффективного использования информации привели к быстрому увеличению количества информации. Сегодня предприятия считают информацию своим самым ценным активом во многих коммерческих областях. Это, безусловно, очень позитивное событие, когда дело касается общественной информации и публичной информации. Но интернет-технологии для конфиденциальных и доверительных потоков информации создали наряду с удобством и новые проблемы. Угроза информационной безопасности в среде Интернет резко возросла. По данным исследования компьютерной преступности, проведенного в 1999 году Институтом компьютерной безопасности и ФБР, 57 процентов опрошенных организаций заявили, что подключение к Интернету является «местом, где чаще всего организуются атаки», а 30 процентов из них утверждают, что сеть была взломан,

26 процентов сообщили, что во время атаки была украдена конфиденциальная информация. По данным Федерального центра компьютерной преступности США (FedCIRC), в 1998 году было скомпрометировано около 130 000 правительственных сетей с 1 100000 компьютеров. Под «взломом компьютера» понимается запуск человеком специальной программы для получения несанкционированного доступа к компьютеру. Формы организации таких атак различны. Их разделяют на следующие виды . Удаленный доступ к компьютеру: программы, обеспечивающие анонимный доступ к Интернету или интрасети. Вход в компьютер, на котором вы работаете: на основе программ анонимного доступа к компьютеру. Удаленное отключение компьютера: на основе программ, которые подключаются к компьютеру удаленно через Интернет (или сеть) и отключают работу его или некоторых его программ (для его запуска достаточно перезагрузить компьютер). Отключение компьютера, на котором работает: с помощью программ деактивации. Сетевые сканеры: сеть фактически использует программное обеспечение для сбора информации, чтобы определить, какие компьютеры и программы, работающие в сети, уязвимы для вторжения. Поиск уязвимостей в программах: путем сканирования больших групп компьютеров в Интернете на наличие уязвимостей. Взлом паролей: с помощью программ, которые находят пароли, которые легко найти в файлах паролей. Сетевые анализаторы (снифферы): использование программ, прослушивающих сетевой трафик. У них есть возможность автоматически извлекать имена пользователей, пароли и номера кредитных карт из трафика. Предотвращение уклонения отправителя массива данных от подтверждения того, что он был отправлен, или получателя от подтверждения того, что он был получен. Множество дополнительных услуг (аудит, обеспечение доступа) и услуг поддержки (управление ключами, безопасность, управление сетью) дополняют эту базовую систему безопасности. Полная система безопасности веб-узла должна охватывать все области безопасности, перечисленные выше.

В этом случае в состав программных продуктов должны быть включены соответствующие средства (механизмы) безопасности. Совершенствование аутентификации предполагает преодоление недостатков, присущих многоразовым паролям: от систем одноразовых паролей до высокотехнологичных систем биометрической идентификации. Предметы, которые пользователи носят с собой, такие как специальные карты, специальные жетоны или дискеты, намного дешевле и безопаснее[3]. Для этих целей также пригодится уникальный, защищенный кодом прикладной модуль. Инфраструктура открытых ключей также является неотъемлемой частью безопасности веб-узла.

Распределенная система (люди, компьютеры), которая используется для обеспечения аутентификации, целостности и конфиденциальности данных (конфиденциальности), публикует электронный сертификат с помощью инфраструктуры открытых ключей (издатель сертификата). Он содержит идентификатор пользователя, его открытый ключ, некоторую дополнительную информацию для системы безопасности и цифровую подпись эмитента сертификата. В идеале эта система должна была бы создать цепочку сертификатов для пользователя в любых двух точках Земли. Эта цепочка позволяет кому-то подписать секретное письмо, перевести деньги на счет или создать электронный контракт, чтобы кто-то другой мог проверить источник документа и личность подписавшего. NIST работает в этом направлении с несколькими другими организациями.

Политика безопасности должна быть ясной и краткой. Должны существовать четкие и последовательные политики и процедуры обеспечения безопасности интрасети. Система сетевой безопасности сильна настолько, насколько сильна ее наиболее уязвимая область. Если в организации имеется несколько сетей с разными политиками безопасности, одна сеть может потерять репутацию из-за плохой безопасности другой сети. Организациям следует принять политику безопасности, обеспечивающую одинаковый уровень защиты повсюду. Важнейшим аспектом политики является выработка единого требования к прохождению трафика через межсетевые экраны. Кроме того, в политике должно быть указано, какие инструменты безопасности (например, инструменты обнаружения вторжений или сканеры уязвимостей) следует использовать в сети и как их следует использовать, а также должны быть определены стандартные конфигурации безопасности для разных типов компьютеров для достижения единообразного уровня. безопасности. Брандмауэр (интернет-экран, английские брандмауэры) следует использовать. Это самая основная защита организации. Контролирует входящий и исходящий сетевой трафик (информационный поток). Он может блокировать или отслеживать определенные типы трафика. Хорошо настроенный брандмауэр может отразить большинство компьютерных атак. Брандмауэры, интеллектуальные карты и другие технические и программные средства защиты следует использовать с умом. Межсетевые экраны и WWW-серверы должны быть проверены на устойчивость к угрозам простоя. В Интернете широко распространены атаки, направленные на остановку работы компьютера. Злоумышленники постоянно разрушают веб-сайты, перегружают компьютеры дополнительными задачами или наводняют сеть бесполезными пакетами. Атаки такого типа могут быть очень серьезными, особенно если злоумышленник достаточно умен, чтобы организовать продолжительные атаки. Потому что

источник этого не может быть найден. Сети, обеспокоенные своей безопасностью, могут организовать собственные атаки, чтобы смягчить ущерб, причиняемый такими атаками. Такой анализ должны проводить только опытные системные администраторы или специальные консультанты.

Криптосистемы должны широко использоваться. Злоумышленники часто проникают в сеть, извлекая пользователей и их пароли из трафика, подслушивая трафик, проходящий через ее чувствительные области. Поэтому соединения с удаленными компьютерами должны быть зашифрованы и защищены паролем. Это особенно необходимо, когда соединение осуществляется через Интернет-каналы или при общении со значимым сервером. Существует коммерческое и бесплатное программное обеспечение для шифрования трафика TCP/IP. Их использование предотвратит атаки. Наиболее надежным средством защиты информационных потоков и ресурсов в Интранете в сочетании со средой Интернета является совместное использование симметричных и симметричных криптосистем. Компьютеры должны быть настроены с учетом требований безопасности. Компьютерные операционные системы часто уязвимы для атак, если они установлены с нуля. Это связано с тем, что при первой установке операционной системы все сетевые устройства могут использоваться, но не могут использоваться правильно. Это открывает злоумышленнику возможность использовать множество методов для атаки на машину. Поэтому все ненужные сетевые устройства следует отключить от компьютера. Регламент оперативного внедрения исправлений программного обеспечения (Patching). Компании постоянно вносят исправления для устранения ошибок, обнаруженных в их программном обеспечении. Если эти ошибки не исправить, злоумышленник может использовать их для атаки на вашу программу и через нее на ваш компьютер. Системные администраторы должны сначала защитить критически важные хосты, установив исправления программного обеспечения на их наиболее критических системах. Это связано с тем, что исправления выпускаются часто и могут быть установлены не на все компьютеры. Исправления обычно следует получать только от компании-производителя программного обеспечения. Дефекты, обнаруженные в системе безопасности интрасети, необходимо устранить.

Организационные меры играют важную роль в создании надежного механизма защиты информации, поскольку вероятность несанкционированного использования конфиденциальной информации во многом определяется не техническими моментами, а злонамеренными действиями, халатностью пользователей или сотрудников службы безопасности. Предотвратить влияние этих аспектов техническими средствами практически невозможно. Для этого необходим комплекс организационных, правовых и организационно-

технических мер, исключающих (или хотя бы минимизирующих) риск конфиденциальной информации. Организация систематического контроля работы сотрудников с конфиденциальной информацией, учета, хранения и уничтожения документов и технических средств. Должны быть разработаны методические указания, регламентирующие порядок доступа сотрудников к конфиденциальной информации, порядок создания, учета, хранения и уничтожения конфиденциальных документов организации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ: (REFERENCES)

1. Русско-узбекский толковый словарь терминов информационной безопасности. 2-й сезон. Под общей редакцией Х. П. Хасанова. Ташкент, 2016 – 733 стр.
2. Аюпов Р.Х., Кабулов А.В. Криптография и криптовалюты. Т: УзМУ имени М.Улугбека, 2008-144 стр.
3. Р.Холдарбоев Р.Абдувахобова. Кибербезопасност ’’ Science and Education’’ Scientific Journal, July 2022
4. Umaraliyev, J., Abdurakhimov, O., & Isokjonova, S. (2023, June). USE AND EFFECTIVENESS OF INFORMATION TECHNOLOGIES IN MEDICINE. In Academic International Conference on Multi-Disciplinary Studies and Education (Vol. 1, No. 11, pp. 148-151).
5. Umaraliyev, J., Turdaliyev, K., Isoqjonova, S., & Abdurakhimov, O. (2023). ITS APPLICATIONS AND PROSPECTS IN EDUCATION. Interpretation and Researches, 1(11). search the horse
6. Muxtarov, F., & Tojidinov, A. (2023). Tarmoq xavfsizligini url filtirlash bilan yaxshilash. Research and implementation, 1(4), 39-44.
7. Muxtarov, F., & Sadirova, X. (2023). Korxonada axborot xavfsizligini ta’minlashning zamonaviy usullari. Engineering problems and innovations.