УДК 004.62

Ахметов Р.Д.
студент магистратуры
кафедра "Информационных систем"
Тимергалин А.Р.
студент магистратуры
кафедра "Информационных систем"
Князев О.А.
студент магистратуры
кафедра "Информационных систем"
Набережночелнинский институт-филиал
Казанского Федерального Университета
Республика Татарстан, г. Набережные Челны

ИЗУЧЕНИЕ ПРОБЛЕМ КИБЕРБЕЗОПАСНОСТИ И МЕТОДОВ ЕЁ ОБЕСПЕЧЕНИЯ

Аннотация: В данной статье рассматриваются современные проблемы в области кибербезопасности, разновидности киберпреступлений, методы обеспечения информационной безопасности.
Ключевые слова: кибербезопасность, киберпреступления, киберэтика, облачные вычисления, информационная безопасность.

Akhmetov R.D.
student of magistracy
Department of Information Systems
Timergalin A.R.
student of magistracy
Department of Information Systems
Knyazev O.A.
student of magistracy
Department of Information Systems
Naberezhnye Chelny Institute-Branch
of Kazan Federal University
Republic of Tatarstan, Naberezhnye Chelny

STUDY OF CYBER SECURITY PROBLEMS AND METHODS OF ITS ENSURING

Abstract: This article examines modern problems in the field of cybersecurity, types of cybercrimes, methods of ensuring information security.

Key words: cybersecurity, cybercrime, cyberethics, cloud computing, information security.

Сегодня человек может отправлять и получать любую форму данных, будь то электронная почта, аудио или видео, одним нажатием кнопки, но задумывался ли он когда-нибудь о том, насколько безопасно его идентификатор данных передается или безопасно отправляется другому человеку без какой-либо утечки информации ? Ответ кроется в кибербезопасности. Сегодня Интернет — это самая быстрорастущая инфраструктура в повседневной жизни. В современной технической среде многие новейшие технологии меняют облик человека. Но из-за этих новых технологий мы не можем в достаточной мере защитить нашу личную информацию, и, следовательно, в наши дни киберпреступность растет каждый день. Сегодня более 60 процентов от общего числа коммерческих транзакций совершаются в Интернете, поэтому эта область требует высокого качества безопасности для прозрачных и лучших транзакций. Следовательно, кибербезопасность стала последней проблемой. Сфера кибербезопасности не ограничивается защитой информации только в ИТ-индустрии, но также распространяется и на другие области, таких как киберпространство и т.д.

Даже новейшие технологии, такие как облачные вычисления, мобильные вычисления, электронная коммерция, интернет-банкинг и другие также требуют высокого уровня безопасности. Поскольку эти технологии содержат важную информацию о человеке, их безопасность является обязательной. Повышение кибербезопасности и защита критически важных информационных инфраструктур имеют важное значение для безопасности и экономического благополучия каждой страны. Повышение безопасности Интернета (и защита пользователей Интернета) стало неотъемлемой частью разработки новых услуг, а также государственной политики[1]. Борьба с киберпреступностью требует

комплексного и более безопасного подхода. Учитывая, что одни только технические меры не могут предотвратить преступления, крайне важно, чтобы правоохранительные органы имели возможность эффективно расследовать киберпреступления и преследовать их в судебном порядке. Сегодня многие страны и правительства вводят строгие законы о кибербезопасности, чтобы предотвратить потерю некоторой важной информации. Каждый человек также должен быть обучен этой кибербезопасности и спастись от этих растущих киберпреступлений.

Киберпреступления.

Киберпреступность — это термин, обозначающий любую незаконную деятельность, при которой компьютер используется в качестве основного средства совершения или кражи[1]. Министерство юстиции США расширяет определение киберпреступности, включив в него любую незаконную деятельность, в которой для хранения доказательств используется компьютер. Растущий список киберпреступлений включает преступления, которые стали возможными благодаря компьютерам, такие как вторжения в сеть и распространение компьютерных вирусов, а также компьютерные разновидности существующих преступлений, такие как кража личных данных, преследование, запугивание и терроризм, которые имеют стать серьезной проблемой для людей и народов[1]. Обычно на простом человеческом языке киберпреступность может быть определена как преступление, совершенное с использованием компьютера и Интернета с целью присвоения личности человека, продажи контрабанды или преследования жертв или срыва операций с помощью злонамеренных программ.

Кибербезопасность.

Конфиденциальность и безопасность данных всегда будут главными мерами безопасности, о которых заботится любая организация. В настоящее время мы живем в мире, где вся информация хранится в

цифровой или кибер-форме. Сайты социальных сетей предоставляют пространство, где пользователи чувствуют себя в безопасности, общаясь с друзьями и семьей. В случае домашних пользователей киберпреступники продолжат атаковать сайты социальных сетей для кражи личных данных. Не только в социальных сетях, но и во время банковских операций человек должен принимать все необходимые меры безопасности.

Тенденции, изменяющие кибербезопасность.

Ниже приведены некоторые из технологий, оказывающих огромное влияние на кибербезопасность.

Веб-серверы.

Угроза атак на веб-приложения с целью извлечения данных или распространения вредоносного кода сохраняется. Киберпреступники распространяют свой вредоносный код через взломанные веб-серверы. Но атаки с кражей данных, многие из которых привлекают внимание СМИ, также представляют собой большую угрозу. Теперь нам нужно больше внимания уделять защите веб-серверов и веб-приложений. Веб-серверы - особенно лучшая платформа для киберпреступников, чтобы украсть данные. Следовательно, всегда нужно использовать более безопасный браузер, особенно во время важных транзакций, чтобы не стать жертвой этих преступлений[2].

Облачные вычисления и их услуги.

В наши дни все малые, средние и крупные компании постепенно переходят на облачные сервисы. Другими словами, мир медленно движется к облакам. Эта последняя тенденция представляет собой серьезную проблему для кибербезопасности, поскольку трафик может обходить традиционные точки проверки. Кроме того, по мере роста числа приложений, доступных в облаке, элементы управления политиками для веб-приложений и облачных сервисов также должны будут развиваться, чтобы предотвратить потерю ценной информации. Хотя облачные сервисы

разрабатывают свои собственные модели, возникает множество проблем с их безопасностью. Облако может предоставить огромные возможности, но всегда следует учитывать, что по мере развития облака его проблемы с безопасностью возрастают[3].

APT и целевые атаки.

APT (Advanced Persistent Threat) — это совершенно новый уровень кибератак[4]. В течение многих лет возможности сетевой безопасности, такие как веб-фильтрация или IPS, играли ключевую роль в выявлении таких целевых атак (в основном после первоначального взлома). По мере того, как злоумышленники становятся все смелее и используют более расплывчатые методы, сетевая безопасность должна интегрироваться с другими службами безопасности для обнаружения атак. Следовательно, необходимо улучшить наши методы безопасности, чтобы предотвратить появление новых угроз в будущем.

Мобильные сети.

Сегодня мы можем связаться с кем угодно в любой части мира. Но для этих мобильных сетей безопасность - очень большая проблема. В наши дни брандмауэры и другие меры безопасности становятся все более уязвимыми, поскольку люди используют такие устройства, как планшеты, телефоны, ПК и т.д.. И все они снова требуют дополнительных мер безопасности, помимо тех, которые присутствуют в используемых приложениях. Мы всегда должны думать о проблемах безопасности этих мобильных сетей. Другие мобильные сети очень подвержены этим киберпреступлениям, поэтому необходимо проявлять большую осторожность в случае возникновения проблем с их безопасностью.

IPv6: новый интернет-протокол.

IPv6 — это новый интернет-протокол, который заменяет IPv4 (старую версию), который был основой наших сетей в целом и Интернета в целом. Защита IPv6 — это не просто вопрос переноса возможностей IPv4.

Хотя IPv6 представляет собой полную замену в предоставлении большего количества IP-адресов, в протокол внесены некоторые очень фундаментальные изменения, которые необходимо учитывать в политике безопасности. Следовательно, всегда лучше перейти на IPv6 как можно скорее, чтобы снизить риски, связанные с киберпреступностью.

Шифрование кода.

Шифрование — это процесс кодирования сообщений (или информации) таким образом, чтобы перехватчики или хакеры не могли их прочитать[5]. В схеме шифрования сообщение или информация шифруются с использованием алгоритма шифрования, превращая его в нечитаемый зашифрованный текст. Обычно это делается с использованием ключа шифрования, который определяет способ кодирования сообщения. Шифрование на самом начальном уровне защищает конфиденциальность и целостность данных. Но более широкое использование шифрования создает дополнительные проблемы для кибербезопасности. Шифрование также используется для защиты данных при передаче, например данных, передаваемых через сети (например, Интернет, электронная торговля), мобильные телефоны, беспроводные микрофоны, беспроводные домофоны и т.д. Следовательно, зашифровав код, можно узнать, есть ли утечка информации[5].

Методы обеспечения кибербезопасности.

Контроль доступа и защита паролем.

Концепция имени пользователя и пароля была фундаментальным способом защиты вашей информации[5]. Это может быть одна из первых мер в отношении кибербезопасности.

Аутентификация данных.

Документы, которые мы получаем, всегда должны быть аутентифицированы перед загрузкой, то есть следует проверять, исходят ли они из надежного и надежного источника и не изменяются ли они[5].

Аутентификация этих документов обычно выполняется антивирусным программным обеспечением, установленным на устройствах. Таким образом, хорошее антивирусное программное обеспечение также необходимо для защиты устройств от вирусов.

Сканеры вредоносных программ.

Это программное обеспечение, которое обычно сканирует все файлы и документы, присутствующие в системе, на наличие вредоносного кода или вредоносных вирусов. Вирусы, черви и троянские кони являются примерами вредоносных программ, которые часто группируются вместе и называются вредоносными программами.

Брандмауэры.

Брандмауэр — это программа или аппаратное обеспечение, которое помогает отсеивать хакеров, вирусы и червей, которые пытаются проникнуть на ваш компьютер через Интернет[5]. Все сообщения, входящие или выходящие из Интернета, проходят через имеющийся брандмауэр, который проверяет каждое сообщение и блокирует те, которые не соответствуют указанным критериям безопасности. Следовательно, брандмауэры играют важную роль в обнаружении вредоносного ПО.

Антивирусное программное обеспечение.

Антивирусное программное обеспечение — это компьютерная программа, которая обнаруживает, предотвращает и предпринимает действия по обезвреживанию или удалению вредоносных программ, таких как вирусы и черви. Большинство антивирусных программ включают функцию автоматического обновления, которая позволяет программе загружать профили новых вирусов, чтобы она могла проверять наличие новых вирусов, как только они обнаруживаются. Антивирусное программное обеспечение является обязательной и базовой необходимостью для каждой системы.

Заключение.

Компьютерная безопасность - обширная тема, которая становится все более важной, потому что мир становится все более взаимосвязанным, а сети используются для выполнения критических транзакций. Киберпреступность продолжает расходиться разными путями с каждым новым годом, как и безопасность информации. Новейшие и революционные технологии, а также новые кибер-инструменты и угрозы, которые обнаруживаются каждый день, ставят перед организациями задачу не только в том, как они защищают свою инфраструктуру, но и в том, как им для этого требуются новые платформы и интеллектуальные возможности. Не существует идеального решения для киберпреступлений, но мы должны стараться изо всех сил минимизировать их, чтобы иметь безопасное и надежное будущее в киберпространстве.

Использованные источники:

1. Cybercrime [Электронный ресурс] // URL: https://en.wikipedia.org/wiki/Cybercrime (дата обращения 8.06.2021).
2. Web Server and its Types of Attacks [Электронный ресурс] // URL: https://www.greycampus.com/opencampus/ethical-hacking/web-server-and-its-types-of-attacks (дата обращения 8.06.2021).
3. The NIST Definition of Cloud Computing [Электронный ресурс] // URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (дата обращения 10.06.2021).
4. Advanced persistent threat [Электронный ресурс] // URL: https://en.wikipedia.org/wiki/Advanced_persistent_threat (дата обращения 12.06.2021).
5. Stallings W. Cryptography and Network Security: Principles and Practice, 7th Edition / W. Stallings. – London: Pearson plc, Cop. 2017. – 766 c.