ведение таможенной статистики осуществляется посредством внесения информации о товарах и транспортных средствах, перемещаемых на территорию Республики Беларусь, а также о лицах, их перемещающих. Существуют базы данных, где хранится информация о лицах, которые воспользовались льготами по уплате таможенных платежей и налогов; об объектах интеллектуальной собственности; реестры таможенных складов и складов временного хранения, таможенных представителей, перевозчиков. [4]

Евразийская экономическая комиссия ведет Единый реестр выданных сертификатов соответствия и зарегистрированных деклараций о соответствии, Единый реестр зарегистрированных лекарственных средств ЕАЭС, базу данных о таможенных органах, действующих на территории ЕАЭС. [5]

Таким образом, базы данных являются неотъемлемой частью деятельности государственных и негосударственных органов и учреждений, начиная с электронных журналов посещений студентов и заканчивая базами данных для ведения таможенной статистики таможенными органами Республики Беларусь. Использование баз данных значительно упрощает ведение любой деятельности, обеспечивая конфиденциальность и удобство использования хранимой информации.

Литература

1. Типы баз данных [Электронный ресурс]. – Режим доступа: https://appmaster.io/ru/blog/tipy-modelei-bazy-dannykh. – Дата доступа: 06.04.2024.

2. Базы данных Национального Банка Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.nbrb.by/today/creditregistry. – Дата доступа: 08.04.2024.

3. Базы данных МВД, ГАИ [Электронный ресурс]. – Режим доступа: https://mvd.gov.by/ru/news/5129#. – Дата доступа: 08.04.2024.

4. Базы данных в таможенном деле [Электронный ресурс]. – Режим доступа: https://www.gtk.gov.by/baza-dannykh-vvezyennogo-avtotransporta/. – Дата доступа: 08.04.2024.

5. Базы данных ЕЭК ЕАЭС [Электронный ресурс]. – Режим доступа: https://eec.eaeunion.org/comission/department/deptexreg/BD.php. – Дата доступа: 08.04.2024.

ИСТОРИЯ КИБЕРУГРОЗ И КИБЕРБЕЗОПАСНОСТИ. ОСНОВНЫЕ ЭТАПЫ

Скобля В.С.

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

Современный мир неразрывно связан с информационными технологиями, и кибербезопасность стала приоритетным направлением защиты людей и организаций. История киберугроз и кибербезопасности прошла через ряд этапов - от первых дней появления компьютеров до современных киберугроз, угрожающих информационной безопасности миллионов людей по всему миру. Изучение этих этапов поможет понять эволюцию киберугроз, а также инструменты и методы противодействия угрозам, которые со временем становятся все более сложными и изощренными.

Кибербезопасность и информационная безопасность компьютерных систем сегодня стоят на страже защиты данных от все более сложных угроз. Их задача – обеспечить конфиденциальность, целостность и доступность информации, что является основополагающим для безопасности информационных активов организаций и индивидуальных пользователей. Конфиденциальность гарантирует, что доступ к информации имеют только авторизованные пользователи; целостность защищает данные от несанкционированных изменений; доступность обеспечивает, что ресурсы доступны легитимным пользователям по требованию.

Для защиты компьютерных систем используются разнообразные технологии, включая антивирусные программы, фаерволы, а также методы обнаружения вторжений, сопровождаемые регулярными обновлениями программного обеспечения и обучением пользователей основам кибергигиены. Это сводит к минимуму риск кибератак, таких как фишинг и социальная инжинерия.

Существуют определённые исторические этапы возникновения киберугроз и решений в виде кибербезопасности:

Возникновение первых ЭВМ (1959 г.)

Именно в этот период началась разработка первого в Беларуси компьютера первого поколения "Минск-1" и его программного обеспечения. В то время еще не было Интернета и компьютерных сетей, а значит, не существовало и киберугроз.

Создание «Телефонного фрикинга» (1950-х годах)

Попытки использовать протоколы, применяемые в телефонных системах, чтобы совершать бесплатные звонки. Данный вид мошенничества не всегда можно было предотвратить.

«Хакинг» для компьютерный систем (1965 г.)

Период заинтересованности в исследовании новейшего компьютера. Люди, которые имели доступ к дорогостоящей машине, осуществляли взлом.

Рождение кибербезопасности (1970 г.)

В 1972-1974 годах стали возникать вопросы о компьютерной безопасности. Государственные ведомства ESD и ARPA в сотрудничестве с ВВС США и другими организациями разработали ядро безопасности для компьютерных систем Honeywell. Компания Multics (HIS Level 68) создала одну из первых систем компьютерной безопасности. [1]

Компьютерные вирусы и «кибершпионаж» (1980 г.)

Значительно возросла угроза вмешательства государств в дела друг друга.

Переход к интернету (начало 2000-х г.)

Интернет развивается семимильными шагами, а персональные компьютеры становятся все более распространенными на работе и дома. Повсеместное использование персональных компьютеров повысило производительность труда, но в то же время создало риски безопасности для многих пользователей. [2]

Переход в онлайн (2010-х г.)

Киберпреступники обнаружили множество уязвимостей в программном обеспечении и протоколах компьютерных сетей. Ежегодно эти уязвимости наносят ущерб на миллионы долларов частным лицам и на миллиарды долларов крупным компаниям.

Новое поколение (2020-х г.)

Период возможности взломать все, что заблагорассудится. Несколько специализированных сайтов предлагают услуги автоматизированных приложений и инструментов для взлома. Своевременные и эффективные кибератаки могут принести компаниям огромные убытки, а организаторам - огромную прибыль. В связи с этим крупные компании и правительства все чаще инвестируют в кибербезопасность.

В эпоху цифровизации и увеличения объемов обмениваемых данных, значимость кибербезопасности неуклонно растет. Преступники и хакеры постоянно ищут способы проникновения в системы для доступа к чувствительной информации, требуя от организаций комплексного подхода к обеспечению безопасности на всех уровнях – от технических до организационных и правовых.

Защита персональных данных подчиняется строгим регуляциям, например GDPR в ЕС, что обязывает организации принимать меры по обеспечению безопасности данных. В современном цифровом мире кибербезопасность требует постоянного внимания и адаптации к новым угрозам, чтобы эффективно защищать информацию, ставшую важнейшим активом.

В настоящее время НЦЭУ, являясь инфраструктурным оператором электронного правительства, работает в нескольких направлениях. Одной из основных обязанностей является обеспечение надлежащего уровня

электронной безопасности. В настоящее время НЦЭУ находится в процессе создания Центра кибербезопасности и реагирования на киберинциденты. Ожидается,

Исходя из выше сказанного, можно сделать вывод, что с каждым новым этапом появлялись новые виды угроз, требующие новых подходов к обеспечению кибербезопасности. Это подчеркивает необходимость постоянного совершенствования технологий и стратегий безопасности для защиты информационных систем и личных данных.

Важным аспектом является также осознание роли каждого участника в обеспечении кибербезопасности, будь то отдельный пользователь, предприятие или государственная организация. Подход к безопасности должен быть комплексным и включать как технические меры защиты, так и образовательные программы для повышения осведомленности об угрозах и методах их предотвращения.

Несмотря на все усилия, современная кибербезопасность остается постоянным вызовом, и необходимость в непрерывном развитии и совершенствовании методов защиты информации никогда не прекращается. История киберугроз и кибербезопасности напоминает нам о важности постоянного внимания к этой проблеме и необходимости сотрудничества на всех уровнях для обеспечения безопасности в цифровом мире.

Литература

1. История киберзащиты: от 40-х годов до наших дней // Avast [Электронный ресурс]. — Режим доступа: https://blog.avast.com/ru/history-of-cybersecurity-avast/ — Дата доступа: 09.04.2024.

2. Center For Internet Security: The Mirai Botnet–Threats and Mitigations [Электронный ресурс]. — Режим доступа: https://www.cisecurity.org/blog/the-mirai-botnet-threats-and-mitigations/. — Дата доступа: 09.04.2024.

3. Центр обеспечения кибербезопасности появится в Беларуси // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. — Режим доступа: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2023/december/76302. — Дата доступа: 09.04.2024.