внедрение новых способов автоматизации, а также переход таможенной документации в электронный формат несет в себе и другие преимущества. К примеру, использование технологий электронного декларирования вместо оформления «бумажных» деклараций и сопутствующих документов обеспечивает следующие преимущества:

– ликвидация ряда избыточных операций, связанных с проверкой документов в бумажном виде, сверки электронных и бумажных копий документов;

– высокая надёжность и низкая трудоёмкость проверки подлинности электронных документов и подписей [2, с. 78].

Таким образом, можно с уверенностью сделать вывод о том, что в современных реалиях невозможно умалить роль информационных технологий, применяемых в таможенных органах при совершении идентификации и таможенного контроля. Только в случае проведения непрерывного мониторинга соответствия программных продуктов современным тенденциям в сфере таможенного оформления и контроля, позволит таможенным органам эффективно решать поставленные перед ними задачи.

Литература

1. Аксенов, И.А. Информационные технологии в таможенной деятельности: учеб.-практ. пособие / И.А. Аксенов – Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых, 2018. – 131 с.

2. Хахаев, И.А. Информационные таможенные технологии: учеб. Пособие / И.А. Хахаев – СПб: НИУ ИТМО, 2014. – 122 с.

УДК 004.056(09)

ИСТОРИЯ КИБЕРУГРОЗ И КИБЕРБЕЗОПАСНОСТИ: ОСНОВНЫЕ ЭТАПЫ

Мойсюк А.В., Мойсюк М.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Человек живёт в мире постоянного совершенствования, и на протяжении всего своего развития сталкивается с большим количеством информации, которая накапливается и передаётся. С поступлением новой информации человечество развивается и упрощает свою жизнь, однако, с приходом чего-то нового возникает необходимость защиты тех данных, которые должны быть скрыты от других людей.

С развитием технологий информационных систем связанных с электронными платежами, электронным документооборотом и другими формами информации, при незащищённости этих данных может произойти несанкционированный взлом, который приведёт к утечке важной информации и соответственно к колоссальным убыткам. [1]

В настоящее время существуют такие понятия, как *кибербезопасность* и *киберугроза*. Если говорить о том, что такое киберугроза, то возникает такое определение как проникновение в виртуальное пространство незаконным путём с целью получения какой-либо конфиденциальной информации. Во избежание такой угрозы необходимы определённые средства кибербезопасности. [2]

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

Возникновение цифрового компьютера (1943 г.).

После создания такой электронной машины никаких киберугроз не возникало, так как доступ к данным был ограничен, а соединения компьютеров в сеть ещё не было.

Появление «Телефонного фрикинга» (1950 г.).

Возникли объединения людей, которые были заинтересованы в работе телефона. Они нашли способ осуществлять звонки на дальние расстояния, уклоняясь от уплаты. Данная практика сошла на нет в конце 1980 года.

Появление интереса во взломе компьютера, по причине любопытства (1960 г.)

В 1960 г. компьютеры представляли собой огромные мэйнфреймы, защищённые в помещениях определённой температуры. Эти устройства были дорогостоящими, поэтому доступ был ограничен, однако те, кто имел доступ, пытались осуществить взлом только из любопытства, без коммерческой и политической цели.

Рождение кибербезопасности (1970 г.).

Боб Томас разработал программу, называвшуюся Creeper. Программа курсировала по сети, оставляя после себя цепочку навигации и запись «I'm the creeper, catch me if you can». В ответ на эту программу Рэй Томлинсон написал свою программу под названием Reaper, которая смогла удалить программу Creaper. Таким образом, программа Рэя Томлинсона стала первой антивирусной базой.

В 1972–1974 гг. начали появляться вопросы, касающиеся обеспечения безопасности компьютеров. Государственные ведомства ESD и ARPA совместно с ВВС США и другими организациями, которые работали над разработкой проекта ядра безопасности для компьютерной системы Honeywell Multics (HIS level 68), создали одну из первых систем компьютерной безопасности. [3]

Переход к интернету (1980 г.).

Немецкий хакер Маркус Хесс в 1986 году с помощью интернет-шлюза в городе Беркли подключился к ARPANET. Ему удалось взломать 400 военных компьютеров, а также мэйнфреймы в Пентагоне, с целью продажи данной информации КГБ.

К теме безопасности данных стали относиться более критично. Этот образ мыслей отразился в реализации мер по кибербезопасности и внезапное снижение свободной памяти остаётся признаком атаки до сих пор.

Появление киберзащиты (1987 г.).

Первая коммерческая антивирусная программа появилась в 1987 году. Андреас Люнин и Кай Фэгге выпустили первую антивирусную продукцию для ATARI ST. Для этой же платформы вышел антивирус UltimateVirus Killer UVK. Трое чешских граждан создали первые версии антивируса NOD. А в США Джон Макафи основал компанию McAfee и затем выпустил антивирусную программу VirusScan. [4]

Переход в онлайн (1990 г.).

Произошли следующие события:

Был изобретён первый полиморфный вирус, исходный код которого постоянно мутировал, чтобы его невозможно было обнаружить.

В британском компьютерном журнале PC Today вышел диск с вирусом Disk Killer, заражающий десятки тысяч компьютеров.

Был создан Европейский институт компьютерных антивирусных исследований – EICAR.

Новое поколение (2010 г.).

В интернете хакер из Саудовской Аравии OXOMAP разместил данные о более чем 400 тысяч кредитных карт. Экс-сотрудник ЦРУ Эдвард Сноуден, работавший на правительство США, копировал и публиковал конфиденциальные данные Агентства национальной безопасности. Неизвестные киберпреступники взломали Yahoo, использовав учётные записи 3-х миллиардов пользователей, вследствие чего компания Yahoo была оштрафована на 35 миллионов долларов за сокрытие этой информации.

Исходя из всего вышесказанного, можно сделать вывод, что постепенное развитие киберпреступлений во многом связано с политическими и экономическими аспектами. Учитывая данные обстоятельства необходимы средства вмешательства в виде киберзащиты с целью сохранности конфиденциальных данных. [5]

Литература

1. Ковалькова, И. А. Киберугрозы, с которыми сталкиваются пользователи сети. // Информационные технологии в политических, социально-

экономических и технических системах [Электронный ресурс] : материалы научно-практической конференции, 22 апреля 2022 года / Белорусский национальный технический университет, Факультет технологий управления и гуманитаризации ; редкол.: Г. М. Бровка (пред. редкол.) [и др.] ; сост. А. В. Садовская. – Минск : БНТУ, 2022. – С. 267-270.

2. Бровка, Г. М. Информационная безопасность в таможенных органах : учебно-методическое пособие для студентов специальности 1-96 01 01 «Таможенное дело» / Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель ; Белорусский национальный технический университет, Кафедра "Таможенное дело". – Минск : БНТУ, 2019. – 118 с.

3. Avast. // [Электронный ресурс]. Режим доступа: https://blog.avast.com/ru/history-of-cybersecurity-avast/ Дата доступа: 19.03.2023.

4. История и современность. // [Электронный ресурс]. Режим доступа: chrome-extension://mhjfbmdgcfjbbpaeojofohoefgiehjai/index.html/ Дата доступа: 19.03.2023.

5. Виртуальный компьютерный музей. // [Электронный ресурс]. Режим-доступа: https://computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/ Дата доступа: 19.03.2023.

УДК 339

ТАМОЖЕННАЯ ПРОЦЕДУРА ЭКСПОРТА: КЛЮЧЕВЫЕ ПОЛОЖЕНИЯ И ОСОБЕННОСТИ ПРИМЕНЕНИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ.

Мойсюк А.В., Мойсюк М.В.
Научный руководитель: преподаватель Жевлакова А.Ю.
Белорусский национальный технический университет

Деятельность, относящаяся к внешнеэкономической сфере в Республике Беларусь, быстрыми темпами приобретает существенное значение и во многих аспектах определяет характер развития хозяйственного комплекса. Развитие экспортного потенциала на сегодняшний день является важным условием экономического роста. Внешнеэкономическая связь в сфере её расширения и роста эффективности представляется важным направлением национальной экономической политики.

Порядок, применяемый к товарам Союза, вывозимым с территории Союза для нахождения за пределами территории Союза, называется таможенной процедурой экспорта.