УДК 338.24

ЦИФРОВАЯ ЭКОНОМИКА И КИБЕРБЕЗОПАСНОСТЬ – ПРОТИВОРЕЧИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Воинова Я.Е.
Студент 3 курса специальности «Таможенное дело»
Пермский государственный национальный исследовательский университет
Пермь, Россия
Карпович Ю.В.
к.э.н., доцент кафедры предпринимательства и экономической безопасности
Пермский государственный национальный исследовательский университет
Пермь, Россия

Аннотация: Актуальность выбранной темы обусловлена тем, что многие пользователи даже и не подозревают о том, какие риски кроются на просторах интернета. Необходимо знать, как вовремя предотвратить их и принять верное решение в случае совершения кибератаки на устройство. Даже базовые знания о кибератаках помогут минимизировать риск атаки.

Ключевые слова: кибератака, вирус, компьютер, информационная угроза, киберугроза, информационная инфраструктура, цифровая экономика.

DIGITAL ECONOMY AND CYBER SECURITY - CONTRADICTIONS AND DEVELOPMENT PROSPECTS

Voinova Ya.E.
3rd year student of the specialty "Economic Security"
Perm State National Research University
Perm, Russia

Karpovich Yu.V.
Candidate of Economic Sciences, Associate Professor of the Department of Entrepreneurship and Economic Security
Perm State National Research University
Perm, Russia

Abstract: The relevance of the chosen topic is because many users are not even aware of the risks that lie on the Internet. It is necessary to know how to prevent such attacks in time and make the right decision if a cyberattack on a device takes place. Even basic knowledge of cyberattacks can help minimize the risk of an attack.

Key words: cyberattack, virus, computer, information threat, cyber threat, information infrastructure, digital economy.

С ростом объемов цифровизации во всех сферах экономики растут и возможности преступного сообщества в части совершения преступлений по хищению денежных средств и других активов. Это вызывает необходимость постоянного мониторинга и разработки эффективных мероприятий по противодействию киберугрозам. Одной из разновидностей таких угроз являются кибератаки.

Кибератаки можно рассматривать двояко:

- в узком смысле как покушение на безопасное функционирование информационной системы компьютера,

- в широком смысле как разработка и использование механизмов контроля функционирования удаленной системы с целью ее дестабилизации [1, с. 187].

Сейчас, в мире технологий очень часто случаются происшествия с вмешательством третьих лиц, которые совершают кибератаки на устройства других людей, с целью добыть нужную информацию. Взломщики в основном

ведут себя тихо, чтобы не привлекать к себе внимания, но есть и такие кибератаки, которые поражают своими масштабами или же влиянием.

По данным статистики, ко многим кибератакам имеют отношение российские хакеры. Так, одной из самых масштабных кибератак за всю историю киберпреступности считается взлом вебсайта «Yahoo». При таком взломе, суммарно пострадало 3 миллиарда аккаунтов жителей всего мира. Изначально такие взломы совершаются для дальнейшей перепродажи базы данных людей. В связи с таким взломом, кода продавался сервер «Yahoo», американскому гиганту «Verizon» помогло хорошо сбить цену с 4,83 млрд. долларов до 4,48 млрд. долларов. К такому взлому причастны 4 человека, при чем один из них, из России.

В октябре 2019 года в Грузии была зафиксирована мощная кибератака, объектами которой стали сайты администрации президента, других органов исполнительной власти, а также коммерческих организаций. По данным МИД Грузии эта кибератака была организована в России, а также осуществлена Россией со стороны бывшего ГРУ. Такие утверждения последовали после результатов расследования грузинской стороны вместе с международными партнерами.

На данный момент, в сфере обеспечения цифровой безопасности государства специалисты отмечают непрерывное усложнение, сопровождающееся ростом масштабов компьютерных атак на объекты информационной инфраструктуры, имеющие стратегическое национальное значение. В настоящее время на долю России приходится около 10% мировых кибератак [3, с.17], что, с учетом растущей динамики, наглядно показывает всю серьезность такой угрозы.

В настоящее время в Российской Федерации на уровне соответствующих ведомств идет активная работа по разработке рекомендаций, определяющих процедуру и порядок расследований инцидентов кибербезопасности, вносятся

предложения по совершенствованию уголовного законодательства. За это направление отвечает компьютерная криминалистика.

В результате компьютерных вирусов и кибератак «страдает» информация, находящаяся на устройстве. Примером ещё одной крупной кибератаки можно рассмотреть вирус Petya, который был распространен в 2017 году. При блокировке файлов вирус вымогал уже $300 в биткоинах. Этот вирус не новый, впервые его действия были зафиксированы в 2016 году. Алгоритм проникновения вируса на компьютер подразумевает, что пользователь переходит по ссылке, которая пришла ему в спам письме, после чего открывается Windows программа для получения прав администратора. После проделанных действий, перед пользователем появляется синий экран, который сообщал о сбое работы системы. Вирус Petya запускался после перезагрузки компьютера и шифровал жесткий диск и поле этого появлялось окно с требованием оплаты расшифровки документов. Иногда встречалось и такое, что в инструкции как оплатить расшифровку документов указывалась и почта злоумышленников для связи с ними. Вирусы, как и многие вещи сейчас постоянно совершенствуются. Для примера, усовершенствованная версия вируса Petya – Misha, наделен правами администратора сразу же, в отличие от своего предшественника Petya.

Исходя из этих достаточно ярких примеров, можно наглядно просмотреть сущность уже более современных кибератак.

В связи с тем, что кибератаки делаются удаленно, это позволяет осуществлять кибератаки в крупных масштабах, что приносит максимальный ущерб пользователям. Способов совершения кибератак достаточно много, и они разнообразны: спам (письма, звонки), уязвимости, фишинг и др.

В современных условиях все чаще набирает обороты распространение вредоносных программ для проведения кибератаки. Исходя из этого, можно с уверенностью сказать, что основной инструмент у современных кибератак это вредоносное программное обеспечение. Его механизм достаточно прост:

вредоносная программа, попав на устройство и используя уязвимости в программном обеспечении, внедряет свое скопированное тело в исполняемый код других программ [2]. Из наиболее часто встречающихся «распространителей» можно выделить: письма по E-mail, флеш-накопители, а также через переход по ссылкам на какие-либо интернет-ресурсы.

Причинами для совершения кибератак и условиями для них может быть множество, именно поэтому, чтобы их предусмотреть и предотвратить, группой международных экспертов разрабатываются рекомендации для минимизации ущерба. Именно по этой же причине, в России требуется разработка системы для предупреждения, обнаружения, а также ликвидации последствий кибератак на информационные ресурсы Российской Федерации, которая включала бы в себя не только обнаружение, предупреждение и ликвидацию кибератак, но и контроль защиты информационных ресурсов.

На уровне микроэкономики современные коммерческим организациям также рекомендуется соблюдать определенные правила кибербезопасности для сохранения своих активов и баз данных. Эти правила состоят из набора криминалистических превентивных знаний, которые сформулированы на основании предшествующих современных кибератак:

- установка только лицензионного ПО с возможностью своевременного обновления. Необходимо трезво оценивать риски кибератак, так как ущерб от них совершенно несоразмерен сэкономленным денежным средствам на лицензионном программном обеспечении;

- использовать только один компьютер для работы с банком, который обслуживает организацию;

- копирование файлов на внешний носитель и использование его только на проверенных устройствах, так как в случае посягательства злоумышленников на ценные файлы, всегда будет их копия под рукой и можно будет продолжить работу уже с ними.

Соблюдение этих принципов поможет защитить активы и повысить степень информационной составляющей экономической безопасности предприятия, а также будет способствовать расследованию происходящих инцидентов. Благодаря этому появиться возможность, несмотря на огромный масштаб угроз и размер возможного ущерба от современных кибератак, им противодействовать.

Библиографический список

1. Бероева Д.М. Кибератаки как угроза информационной безопасности// Пробелы в российском законодательстве. 2018. - №2, с. 186-188.

2. Буряк В.В. Хакеры, хактивизм и проблема обеспечения кибербезопасности в условиях цифровой экономики// Бенефициар. 2018. № 27. С. 12-18.

3. Россия заняла второе место по количеству кибератак [Электронный ресурс] – Режим доступа: http://www.itsec.ru/newstext.php?news_id= 117006 (Дата обращения 02.06.2021)

Оригинальность 95%