УДК 004.77

Шарыпова Т.Н.,
кандидат экономических наук
доцент кафедры информационных технологий и защиты информации
Ростовский государственный экономический университет «РИНХ»
Россия, г. Ростов-на-Дону
Калюжная А.Н.,
студентка 1 курса, юридический факультет
Ростовский государственный экономический университет «РИНХ»
Россия, г. Ростов-на-Дону

ПРОБЛЕМА ОПРЕДЕЛЕНИЯ УЩЕРБА В РЕЗУЛЬТАТЕ КИБЕРАТАКИ

Аннотация: *в статье рассматриваются вопросы, связанные с обеспечением информационной безопасности хозяйствующих субъектов. Часто информация становится объектом кибератак. Потеря информации для субъектов предпринимательства грозит наступлением материального ущерба. На практике возникают сложности при определении ущерба, нанесенного несанкционированным доступом к информации или ее хищении.*

Ключевые слова: и*нформация, кибератака, хозяйствующий субъект, обмен информации, убытки, вред.*

Annotation: *The article deals with issues related to information security of economic entities. Often information becomes the object of cyber attacks. Data loss for businesses is threatened by the onset of material damage. In practice, it is difficult to determine the damage caused by unauthorized access to or theft of information.*

Key words: *Information, cyber attack, economic entity, information exchange, losses, harm.*

Большинство хозяйствующих субъектов, осуществляя предпринимательскую деятельность, обязательно участвуют в электронном

обмене информацией, а также в ее распространении. Неотъемлемой частью бизнес-процессов являются механизмы обмена информацией. Технологии обмена обеспечивают как внутренние механизмы взаимодействия между структурами организации или ее сотрудниками, так и взаимодействие организаций во внешней информационной среде со своими контрагентами, клиентами или потенциальной целевой аудиторией.

Однако в процессе обмена информацией, электронные носители и сама информация, являясь ценностью, могут подвергаться угрозам в виде утечки, модификации, уничтожения. Такие угрозы именуются угрозами безопасности и могут быть как внутренними, так и внешними.

Таким образом, объектом кибератаки является не только информация, но и нарушение механизмов передачи и получения информации. В соответствии со статей 1064 ГК РФ [1], основанием возникновения обязательства возмещения вреда служит гражданское правонарушение, выразившееся в причинении вреда другому лицу. Для наступления ответственности за причинение вреда в общем случае необходимы четыре условия: наличие вреда, противоправное поведение (действие, бездействие) причинителя вреда, причинная связь между противоправным поведением и наступившим вредом, вина причинителя вреда.

В статье 15 ГК РФ законодатель разграничил понятия «убытки», «ущерб» и «вред», определил режим их правового применения в зависимости от нарушения объектов гражданских прав. Это обусловлено тем, что термином «убытки», как правило, обозначаются последствия нарушения имущественных прав граждан и юридических лиц [3].

В ст. 12 ГК РФ одним из способов защиты приводится такой способ защиты гражданских прав, как возмещение убытков. В этой же статье законодатель называет и такой способ защиты, как «компенсация морального вреда», разграничивая тем самым понятия «вред», «убытки». «Возмещение вреда» как самостоятельный способ защиты гражданских прав в Кодексе не предусмотрен.

При определении ущерба, причиненного кибератакой, то есть в результате осуществления неправомерного доступа к информации или нарушения права на доступ к информации тех или иных лиц, то для оценки ущерба следует разграничить понятия, описывающие этот объект и дающие легальное его толкование. Так, согласно статье 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Информация - сведения (сообщения, данные), независимо от формы их представления; доступ к информации - возможность получения информации и ее использования; распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц; предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц [2].

Процессы, осуществляемые при помощи информационных систем и баз данных, являющиеся объектом кибератак, могут быть описаны с точки зрения закона как процессы, обеспечивающие распространение, предоставление и получение информации. Ущерб, причиненный кибератакой, должен оцениваться с точки зрения прав на получение, предоставление и распространение информации, которые были нарушены. При этом ущерб может быть причинен как обладателю информации, обладающему правом на распространение и предоставление информации в своих интересах, так и кругу лиц, обладающих правом на получение этой информации. Отдельно стоит выделить исключительные права на информацию как на объект авторского права [4].

Осуществляя фиксацию общего ущерба, причиненного кибератакой, и при дальнейшем его доказывании возникает ряд проблем, связанных с разграничением различных правоотношений, затронутых или нарушенных неправомерными действиями. Когда,кибератака нарушает работоспособность информационных сервисов осуществляющих процессы приема и передачи информации на какое-то время без утраты этой самой информации, доказывание ущерба сводится к тому, что при помощи технических данных, фиксирующих

работоспособность оборудования, обеспечивающего работу информационных сервисов, устанавливается длительность нарушения работоспособности сервиса и оценивается его средняя производительность по тем же данным за аналогичные временные отрезки [5].

Объектом современных кибератак являются персональные данные пользователей атакуемых сервисов, а целью атаки является получение доступа к этим данным. В случаях возникновения таких инцидентов возникает проблема в доказывании ущерба, причиненного субъекту персональных данных, поскольку эти данные не оцениваются в каком-либо количественно-качественном выражении, могут дублироваться другими сервисами, и в случае утечки источник этой утечки почти не подлежит идентификации. В целях доказывания ущерба, причиненного кибератакой с неправомерным доступом к данным, целесообразным было бы использование цифровых отпечатков, позволяющих отслеживать те или иные экземпляры файлов и источники их получения.

Большинство организаций не имеют возможности самостоятельно провести оперативное расследование обстоятельств осуществления злоумышленниками кибератаки в отношении их, поэтому рекомендуется незамедлительно обратиться в правоохранительные органы после выявления возникшей угрозы информационной безопасности. Также надлежит незамедлительно уведомить об инциденте безопасности провайдера, организующего доступ к сети, посредством которой осуществляется атака на сервер.

Необходимо осуществлять фиксацию продолжительности атак, изменений характера атак, которые происходят, как правило, в качестве реакции на противодействие атаке. Злоумышленники поочередно могут использовать различные уязвимости систем безопасности, и если при блокировании угроз злоумышленники меняют характер атаки, используя другие уязвимости для продолжения атаки, то это дополняет субъективную сторону состава правонарушения.

Обязательно необходимо фиксировать IP-адреса, участвовавших в компьютерной атаке на информационный ресурс или на сервер. Данные действия существенно повысят вероятность установления организатора атаки и механизма ее организации. При появлении подозрений о совершении атаки надлежит осуществить временное блокирование счетов, доступ к которым возможен посредством сети Интернет. Поскольку злоумышленник, имеющий целью хищение денежных средств, с помощью полученной информации, постарается совершить хищение незамедлительно. А также необходимо проводить регулярные инструктажи по информационной безопасности и исполнению кризисных протоколов среди сотрудников вашей организации.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 29.07.2018) // Собрание законодательства РФ. 1996. № 5. Ст. 410.
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.12.2018) «Об информации, информационных технологиях и о защите информации» // Российская газета. № 165. 29.07.2006.
3. Пешкова О.А. Соотношение понятий «вред», «убытки», «ущерб» // Мировой судья. 2010. № 7. С. 7-11.
4. Ландик С.А., Шарыпова Т.Н. Компьютерные преступления и мероприятия по защите электронных данных. В сборнике: наука сегодня: вызовы и решения, материалы международной научно-практической конференции: в 2 частях. 2018. С. 68-70.
5. Тищенко Е.Н., Шарыпова Т.Н. Формализация выбора различных вариантов системы защиты информации от несанкционированного доступа в среде электронного документооборота. Вестник Ростовского государственного экономического университета (РИНХ). 2010. № 3 (32). С. 226-233.