УДК 343.988

Модели реализации виктимности в цифровой среде

Дмитрий Витальевич Жмуров
Байкальский государственный университет, Иркутск, Россия
кандидат юридических наук, доцент
zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X

Аннотация. Проанализированы ключевые паттерны (модели) процесса кибервиктимизации. В данном случае речь идет о схемах взаимодействия жертвы и преступника в цифровом пространстве, объединенных сходством внутренних особенностей и стереотипий поведения сторон. Автором описаны 9 основных паттернов кибервиктимизации, которые отличаются друг от друга числом и спецификой участников, инициативой сторон, особенностями их ролевого поведения и проч. Описаны основные свойства вышеназванных поведенческих моделей.

Ключевые слова: кибервиктимология, кибержертва, кибервиктимность, кибервиктимизация, паттерны кибервиктимизации

Для цитирования: Жмуров Д. В. Модели реализации виктимности в цифровой среде // Защита жертв преступлений в современном обществе (PVCMS 2023) : материалы VI Международной научно-практической интернет-конференции (Челябинск, 21–22 февраля 2023 г.) / отв. ред. А. В. Майоров. Челябинск : Эскуэла, 2023. С. 88–93. URL: https://victimolog.ru/index.php/PVCMS/article/view/532

Models of Implementation of Victimization in the Digital Environment

Dmitrij V. Zhmurov
Baikal State University, Irkutsk, Russia
Candidate of Law Science, Associate Professor
zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X

Abstract. Key patterns (models) of the process of cyber-victimization are analyzed. In this case it is about schemes of interaction between victim and offender in the digital

space, united by similarity of internal features and stereotypes of behavior. The author describes 9 basic patterns of cyber-victimization, which differ from each other by the number and specificity of participants, the initiative of the parties, the characteristics of their role-behavior, etc. Described the main features of the above behavioral patterns.

Keywords: cybervictimology, cybervictimization, cybervictimization, cybervictimization patterns

For citation: Zhmurov D. V. Models of victimhood implementation in the digital environment // Protection of victims of crime in modern society (PVCMS 2023) : materials of the VI International Scientific-Practical Internet-Conference (Chelyabinsk, February 21-22, 2023). ed. by A. V. Mayorov. Chelyabinsk : Escuela, 2023. Pp. 88-93. (In Russ.) URL: https://victimolog.ru/index.php/PVCMS/article/view/532

Для начала следует определить исходную терминологию. Что обозначают понятия «модель реализации виктимности в цифровой среде» или «паттерн кибервиктимизации»? В данной статье они будут употребляться как тождественные термины. Итак, паттерном в психологии зачастую называют поведенческую реакцию или шаблонное действие индивида. Кибервиктимизация охватывает процесс и результат становления жертвы правонарушения в виртуальном пространстве. Следовательно, паттерн кибервиктимизации — это типовой случай или умозрительная модель того, как человек становится кибержертвой, т. е. пострадавшим в сети интернет [1; 2].

Иными словами, имеются ввиду базовые образцы взаимодействия сторон интернет-правонарушения, обладающие некоторыми важными свойствами:

— поведенческая ситуация описывается наличием *двух антагонистических сторон* — правонарушителя и жертвы (причинителя и потерпевшего);

— их виртуальное взаимодействие характеризуется двух-, трех- или многосторонним форматом, когда каждая из сторон связана с другой в техническом, социальном, информационном или экономическом плане;

— взаимодействие сторон виртуального акта не сводится исключительно к коммуникации живых лиц и не обязательно отражается в индивидуальной психике одной из сторон. Порой, субъекты коммуникации лично не знакомы; случается, что один из них не догадывается о личности корреспондента или обманывается в ней; не исключены инциденты, когда взаимодействие пострадавшего происходит с небиологическим субъектом, созданным причиняющей стороной (вирусом, червем, бот-нетом) или происходит по отношению к неодушевленной жертве (самоорганизующемуся блокчейн-проекту, FOSS-ресурсу, ИИ) и проч.;

— результатом взаимодействия сторон криминального акта является виктимизация одной из них (реже — обеих).

Таким образом, *паттерн кибервиктимизации — это схема взаимодействия жертвы и преступника в виртуальном пространстве*. В ходе анализа научной и публицистической литературы удалось выявить и описать не менее девяти таких паттернов. Естественно, это далеко не исчерпывающий перечень. Отметим некоторые из них:

1. **Билатеральное взаимодействие**, когда оба участника виктимологической ситуации — живые люди, использующие глобальную сеть. При этом один из них причиняет вред (выступая правонарушителем), а другой является объектом негативного воздействия (потерпевшим). Возможны различные варианты подобной ситуации:

1.1. *Характеризуемая инициативностью жертвы*, ее активными действиями по вступлению в отношения с правонарушителем (добровольное вхождение в хайп-проект или финансовую пирамиду в интернете; использование сомнительных инвестиционных схем для быстрого заработка; некритичные знакомства в чатах; некорректное поведение на форумах, провоцирующее кибербуллинг или сталкинг и проч.).

1.2. *Характеризуемая инициативностью правонарушителя,* когда активные действия по поиску и отбору жертвы предпринимаются причиняющей стороной. Большинство случаев киберпреступного поведения реализуются в рамках данной схемы. Она предполагает организацию мошеннических проектов в интернете и целенаправленную вербовку (обработку) потенциальных потерпевших, отправку писем фишингового содержания, иные способы активного выслеживания жертв и вступления с ними в контакт.

1.3. *Характеризуемая инверсивным взаимодействием сторон,* когда в ходе акта причинения вреда преступник и жертва могут меняться местами. Инициация межличностного взаимодействия в одинаковой степени возможна с обеих сторон. Например, это могут быть случаи ответных действий на кибербуллинг еще более интенсивной агрессией; попытки отомстить обидчику (скомпрометировав его аккаунт, распространяя клевету о его личности, заражая вредоносным ПО гаджеты); встречные DDOS-атаки (взломы системы), направленные на подозреваемых в недружественных действиях.

1.4. *Характеризуемая коллективным взаимодействием сторон,* происходящим как по отношению к правонарушителю (групповые киберпреступления), так и жертве (случаи массовой виктимизации). Это могут быть разнообразные формы группового преследования (остракизма); виктимизациииндивида со стороны коллективного субъекта (преступной группы, организовавшей мошеннические проекты и т. п.).

2. **Монотеральное взаимодействие,** в котором одной из сторон выступает одушевленное лицо (личность), а другой — опасный для нее интеллектуальный продукт, который в достаточной степени автономизирован

(вирусная программа, червь, лжеантивирус). Обозначим его как автономный цифровой продукт или автономную цифровую сущность, если последняя несет в себе признаки машинного интеллекта (способность к обучению, самоизменяемость, некоторая степень адаптивности к среде). Данный вид взаимодействия предполагает ряд возможных модальностей, среди которых:

2.1. *Характеризуемая инициативностью жертвы* происходит в случае, если потерпевший, минуя коммуникативную составляющую (межличностный компонент) самостоятельно устанавливает вредоносные программы на свой компьютер, выдает им административные права, находясь под влиянием обмана и заблуждения (фейковые обновления; вредоносные патчи, замаскированные под полезные апгрейды и т. п.).

2.2. *Характеризуемая инициативностью вредоносного цифрового продукта*, когда принятие решения о виктимизации пользователя заложено программно и не требует вмешательства со стороны разработчика. Такие продукты именуются «сетевыми червями». Они демонстрируют признаки аутоpепликации и автономного проникновения на компьютеры жертв. Эксплуатируя несовершенство сетевого программного обеспечения, эти цифровые организмы способны осуществлять подбор паролей, дальнейшую саморассылку по адресной книге и поиск новых жертв.

2.3. *Характеризуемая взаимодействием программы и индивида, которое причиняет вред третьим одушевленным лицам.* Это происходит, когда вредоносная программа, воздействуя на одно лицо, использует его в качестве посредника для виктимизации другого. Такое возможно, например, когда на компьютер пользователя (по его воле или помимо нее) устанавливаются программы типа бэкдор. Это дефекты алгоритма, позволяющие злоумышленнику получить несанкционированный доступ к данным или управлению цифровым устройством другого человека. Точно так бэкдор заражает сотни и тысячи машин, формируя из них единую сеть, которая используется, как правило, в преступных целях (атаки на сайты, скрытый майнинг, проведение вычислений за счет ресурсов других людей и т. п.). При этом хозяин единичного компьютера, как правило, не предполагает, что является в этой ситуации потерпевшим, поскольку явных дискриминирующих действий по отношению к нему не осуществляется.

3. **Процедурное (техническое) взаимодействие**, в котором участвуют автономные цифровые продукты (сущности), приводящее, в конечном итоге, к виктимизации живых лиц. Укажем несколько типов подобного контактирования:

3.1. *Характеризуемое интеркомпьютерным взаимодействием и причиняющее вред живым лицам.* Для него свойственна антагонистическая

связь двух цифровых систем (компрометирующей и дискредитируемой), а в качестве одного из возможных последствий — наступающий вред для реальных людей, каким-либо образом зависящих от работы дискредитируемого субъекта. Например, атаки вредоносного ПО на систему контроля дорожного движения или воздушной логистики; роботизированные производственные циклы; систему распределения электрической энергии и проч. Указанные действия в ряду прочих последствий могут повлечь неблагоприятные результаты для неопределенного круга лиц (участников дорожного движения, рабочих на предприятии, потребителей электроэнергии).

3.2. *Характеризуемое интеркомпьютерным взаимодействием и причиняющее вред неорганическим сетевым структурам* (цифровым организмам, экосистеме интернета, узлам сети, целостности блокчейна и т. п.). Как правило, подобный тип атак выделяется с некоторой долей условности, поскольку за неорганическими сетевыми структурами, в конечном итоге, стоят люди со своими интересами и ценностями. Гипотетически такая ситуация вполне возможна в ходе интернет-блэкаут, когда происходит тотальное нарастающее отключение компонентов информационно-коммуникационной сети.

Таким образом, понимание паттернов кибервиктимизации позволяет исследователю не заблудиться в разнообразии и сложностях сетевых хитросплетений, приводящих одну сторону к ущербу, охватить общим взглядом максимально возможное число моделей виктимизации, упорядочить их, выстроить на этой основе систему и тактику противодействия киберпреступности. Безусловно, изучаемый вопрос является чрезвычайно актуальным и требует дальнейших поисков.

Список источников

1. Жмуров Д. В. Кибервиктимность как новая категория виктимологии постмодерна // Азиатско-тихоокеанск ий регион: экономика, политика, право. 2021. Т. 23, № 2. С. 113–122. DOI: https://doi.org/10.24866/1813-3274/2021-2/113-122

2. Жмуров Д. В. Кибервиктимизация. Исследовательская матрица // Пролог: журнал о праве. 2021. № 3 (31). С. 109–121. DOI: https://doi.org/10.21639/2313-6715.2021.3.11

References

1. Zhmurov D. V. Kiberviktimnost’ kak novaya kategoriya viktimologii postmoderna // Aziatsko-tihookeanskij region: ekonomika, politika, pravo. 2021. T. 23, № 2. S. 113–122. DOI: https://doi.org/10.24866/1813-3274/2021-2/113-122

2. Zhmurov D. V. Kiberviktimizaciya. Issledovatel'skaya matrica // Prolog: zhurnal o prave. 2021. № 3 (31). S. 109–121. DOI: https://doi.org/10.21639/2313-6715.2021.3.11

Дата поступления / Received: 07.02.2023.
Дата публикации / Accepted: 03.04.2023.