Данная таксонометрическая классификация социальных детерминант присуща различным половозрастным категориям. Как показывают проведенные исследования, молодежь объективно обладает большими потенциальными возможностями по участию в инновационной деятельности. Молодежи присущи большая креативность мышления, инновационная восприимчивость и активность, способность творчески относиться к выполнению своих функциональных обязанностей. Молодежь, как органическая часть общества, обладает потенциальными возможностями, характерными для ее возраста, образования и ценностных ориентаций. Ей присуща более высокая социально-профессиональная мобильность и восприимчивость к новшествам, способность разрабатывать и реализовывать социально значимые и экономически эффективные проекты. В связи с этим представляется возможным выделить особенности социальных детерминант инновационной активности присущей именно данной группе. Анализ общей динамики социально-демографического развития показывает увеличение доли молодежи в высокотехнологичных и наукоемких отраслях экономики. Соответственно и готовность молодежи в реализации своих потенциальных возможностей будет возрастать. Для этого необходима разработка соответствующих механизмов и инструментов активного участия молодежи в модернизации и цифровизации экономики и общества, в реализации социально-значимых проектов и программ.

УДК 004.056

КИБЕРУГРОЗЫ, С КОТОРЫМИ СТАЛКИВАЮТСЯ ПОЛЬЗОВАТЕЛИ СЕТИ

Ковалькова И.А., Лабкович О.Н.
Белорусский национальный технический университет

Киберугроза – это угроза вредоносного проникновения или незаконное проникновение в информационное пространство для достижения политических, социальных или иных целей. Реализованная киберугроза обычно поражает носители данных, предназначенные для их хранения, обработки и передачи личной информации пользователя.

Как правило, киберугрозы исходят от компьютерных злоумышленников (хакеров) – высококвалифицированных специалистов, понимающих тонкости работы программ на ЭВМ, способных взламывать серверы и таким незаконным путём получать из них нужную информацию.

Киберугрозы разделяют на внешние и внутренние.

Источники внешних угроз находятся вне компьютеров пользователей, как правило, в глобальной сети. К ним относят вредоносное программное обеспечение, спам, удалённый взлом компьютеров, фишинг, DoS/DDoS-атаки, хищение мобильных устройств и другое.

Внутренние угрозы зависят от используемого программного обеспечения (ПО) и оборудования. Большую опасность представляют уязвимости программного обеспечения, связанные с недоработками и ошибками в популярных программах, которые выявляются хакерами и которые потом ложатся в основу большинства вирусов, троянских программ, червей, проникающих через эти лазейки на компьютеры. [1]

Основные цели кибератак – взлом доступа к закрытой информации, её изменение или уничтожение, вымогательство денег у пользователей или владельцев сайтов, причинение вреда бизнес-процессам и их управлению.

Атаки хакеров на информационные ресурсы с каждым годом становятся всё более изощрёнными и для их осуществления они используют различные инструменты и приёмы.

Вредоносное ПО. Часто распространяется под видом безобидных файлов или почтовых вложений. Наиболее распространёнными видами вредоносного ПО являются:

- *Вирусы* – программы, которые заражают файлы вредоносным кодом, распространяясь внутри компьютерной системы и копируя самих себя.
- *Троянцы* – вредоносные программы, которые прячутся под маской легального ПО. Киберпреступники обманным путём вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
- *Программы-вымогатели (шифраторы)* – вредоносные программы, которые шифруют файлы всех распространённых типов (doc, xls, jpeg и т.д.) на заражённом устройстве и даже на внешних носителях, а потом выводят на экран требование денежного выкупа за ключ расшифровки. Как правило, распространяются через спам-письма, торренты или заражённые сайты.
- *Шпионское ПО* – шпионские программы (или spyware), которые втайне следят за действиями пользователя и собирают всю доступную о нём информацию (например, данные кредитных карт, список посещённых веб-сайтов, адресные книги, даже набираемый на клавиатуре текст), которую киберпреступники затем могут использовать в своих целях. [1]
- *Рекламное ПО* – программы рекламного характера (или adware), которые навязчиво демонстрируют рекламу на устройстве, мешая нормальной работе и с помощью которых может распространяться вредоносное ПО. Пользователь заражённого устройства видит всплывающие окна, баннеры, текстовые ссылки, автоматический запуск

видеороликов, т.е. всё, кроме нужной ему информации. И пока жертва пытается избавиться от подобных назойливых объявлений, разработчики adware зарабатывают на показе рекламы. [2]

• *Ботнеты* – сети компьютеров, с запущенными бот-программами, которые скрыто устанавливаются на ПК пользователя и открывают злоумышленнику удалённый доступ к устройству. Ботнеты используются для рассылки спама, хищения личных данных или DDoS-атак. Как и большая часть вредоносного ПО, бот-программа проникает на устройство вместе с любым контентом, который скачивается на непроверенных сайтах.

Спам. Массовые неадресные рассылки (или «мусор») со всевозможным сомнительным содержанием и рекламой, которые распространяются через электронную почту. Такие рассылки могут являться каналом для внедрения вирусных программ, способных разрушать операционную систему, блокировать и уничтожать файлы на компьютере пользователя.

Фишинг. Внедрение фальшивых почтовых и других сообщений, которые выглядят убедительными и официальными, и с помощью которых можно украсть личную информацию пользователей (например, номера кредитных карт, пин-коды доступа к картам и учётным данным). Существуют фальшивые сайты мобильных банков, пользуясь которыми можно потерять деньги, и дать доступ к другим пользователям-контактам. Фишинг обычно распространяется вместе со спамом.

DoS/DDoS-атаки (или «отказ в обслуживании»). Это атаки в виде целенаправленных многочисленных запросов, создающих избыточную нагрузку на сети и серверы объекта атаки, нарушающие и блокирующие его работу (например, определённого сайта интернет-магазина или почтового сервера). Такие атаки разрушают алгоритм работы и приводят к приостановке деятельности, что сказывается на работе и прибыли. Подобными атаками обычно пользуются конкуренты. [3]

Атаки Man-in-the-Middle («человек посередине»). Это атаки, в ходе которых киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Подвергнуться такой атаке можно, если, например, подключитесь к незащищённой сети Wi-Fi.

SQL-инъекция. Этот вид кибератак используется для кражи информации из баз данных, когда используются уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL). [1]

Руткит (Rootkit). Программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов,

сервисов, ключей реестра, открытых портов, соединений и пр.) посредством обхода механизмов системы.

Литература

1. Киберугрозы и информационная безопасность. // [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security.

2. Основы интернет-безопасности. // [Электронный ресурс]. Режим доступа: https://academy.esetnod32.ru/course/course4/lesson1082/

3. Какие бывают киберугрозы. // [Электронный ресурс]. Режим доступа: https://temowind.ru/bezopasnost-windows-7/kakie-byvayut-kiberugrozy/.