Известия Гомельского государственного университета
имени Ф. Скорины, № 2 (143), 2024

УДК 343.3/.7 EDN: SACGOW

К вопросу о кибершпионаже как инструменте совершения преступлений, связанных со шпионажем

О.Г. Шляхтова, С.Л. Емельянов

В статье анализируется кибершпионаж как средство коммерческого шпионажа. Кибершпионаж – обход систем компьютерной безопасности и получение несанкционированного доступа к защищённой информации в различных целях.
Ключевые слова: кибершпионаж, коммерческий шпионаж, национальная безопасность, цифровизация, информационные технологии, корпоративные сети, утечка информации.

The article analyzes cyber espionage as a means of commercial espionage. Cyber espionage is the bypassing of computer security systems and gaining unauthorized access to protected information for various purposes.
Keywords: cyber espionage, commercial espionage, national security, digitalization, information technologies, corporate networks, information leakage.

Введение. Глобальная компьютеризация (цифровизация) общества позволяет компьютерным технологиям быстрыми темпами проникать во все сферы жизни граждан. Во-первых, это открывает перед гражданами и обществом в целом новые возможности. Во-вторых, стремительное развитие технологий, рост количества электронных и мобильных гаджетов, увеличение числа сервисов и интернет-услуг приводит к возникновению рисков и угроз, что в свою очередь послужило основанием к увеличению количества киберпреступлений, у которых в настоящее время нет конкретной трактовки.

С развитием информационных технологий появились средства шпионажа, использующие специальное оборудование и программное обеспечение.

Основная часть. Определения термина «кибершпионаж» на законодательном уровне нет, поэтому в теоретическом аспекте под кибершпионажем можно понимать несанкционированный доступ к защищенной информации (данным), информационным системам государственных или коммерческих организаций, а также физических лиц с различными целями. Выполняется такой доступ путем обхода системы безопасности компьютера, используя для этого специальные шпионские программы и трояны. Взлом осуществляется путем физического доступа, посредством сети Интернет или локальных сетей.

Кибершпионаж подразумевает использование информационно-коммуникационных технологий (далее – ИКТ) отдельными лицами, группами лиц или компаниями для получения экономической или личной выгоды.

Кибершпионаж также может осуществляться правительственными организациями, финансируемыми или контролируемыми государством или лицами, действующими от имени государства, для получения несанкционированного доступа к системам и данным и сбора информации об интересующих их объектах в целях укрепления национальной безопасности, экономической конкурентоспособности и (или) военной мощи страны.

Сам по себе шпионаж не является новым противоправным деянием, однако, появление ИКТ не только позволило другим странам осуществлять неправомерную деятельность по сбору данных с беспрецедентной скоростью, частотой, интенсивностью и в невероятных масштабах, но и снизило риски, связанные с деятельностью по шпионажу (например, риск быть обнаруженным в странах, на которые направлена деятельность по сбору данных).

Цели кибершпионажа могу иметь политическое, экономическое и военное направления. С возникновением нового программного обеспечения, повышением значения гаджетов способы осуществления кибершпионажа регулярно совершенствуются. К основным методам можно отнести:

– целевые атаки (APT), обладающие высокой эффективностью. APT – это совокупность киберпреступлений, совершаемых против конкретных компаний и организаций;

– распространение вредоносных и шпионских программ. Вредоносные программы используются для совершения атак на компьютерные системы и сбора информации в системах-мишенях. Шпионскими программами заражают жесткие диски для сбора данных о сетевых соединениях и процессах из других систем. Вся полученная информация отправляется на серверы, подконтрольные лицам, которые использовали такие программы;

– социальная инженерия – злоумышленник обманом заставляет свою цель раскрыть информацию или совершить иное действие [1]. Примером может служить целевой фишинг, когда осуществляется отправка электронных писем с зараженными вложениями или ссылками, чтобы заставить получателя открыть письмо и перейти по ссылке;

– «атаки на водопое» (watering hole) – атаки, при которых киберпреступники отслеживают сайты, наиболее часто посещаемые членами определенной организации или группы, а затем заражают эти сайты вредоносными программами в попытке получить доступ к их сети.

Инструменты осуществления кибершпионажа также разнообразны и включают в себя эксплойты (например, поиск и обнаружение ранее неизвестных уязвимостей систем, которые в дальнейшем используются для кибепреступлений) и импланты (например, программный код, разрешающий получать доступ к компьютерной системе).

Необходимо отметить, что кибершпионаж является одним из инструментов, которые могут использоваться в рамках коммерческого шпионажа, когда государства или частные акторы направляют свои киберспособности на сбор конфиденциальной информации у конкурентов или других коммерческих организаций.

Согласно Уголовному кодексу Республики Беларусь (далее – УК) под коммерческим шпионажем подразумевается «похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну, с целью их разглашения либо незаконного использования» [2, ст. 254].

Объектом посягательства данного преступления является информационная безопасность субъектов экономической деятельности от внешних и внутренних угроз сведений, составляющих их коммерческую или банковскую тайну, которые являются в свою очередь предметом преступления [3, с. 571].

Сбор и похищение сведений, составляющих коммерческую или банковскую тайну, могут быть тайными (кража) и осуществляться путем грабежа, разбоя, вымогательства, мошенничества, злоупотребления служебными полномочиями, присвоения, растраты или модификации компьютерной информации. Помимо этого могут использоваться сетевые атаки, устанавливаться прослушивающие устройства, взламываться корпоративные сети.

Чаще всего целью кибершпионов являются большие объемы информации, хранящейся в автоматизированных государственных системах и базах данных. Данная цель преследуется по причине того, что такой массив информации содержит в себе большой объем персональных данных или коммерчески значимой информации.

Кибершпионаж представляет серьезный риск для государственной безопасности. Конкретные последствия коммерческого кибершпионажа могут быть разнообразными и зависят от целей и масштаба атаки:

1) Утечка конфиденциальной информации. Получение доступа к государственным секретам, планам развития, политическим стратегиям и другой конфиденциальной информации может привести к серьезным последствиям для национальной безопасности интересов государства (например, ослабление обороноспособности). Согласно данным Экспертно-аналитического центра InfoWatch в 2019–2020 гг. почти 60 % инцидентов связаны с компрометаций персональных данных, а примерно каждая пятая утечка в Республике Беларусь – это случай потери или кражи данных, относящихся к категории «коммерческая тайна» (рисунок 1) [4, с. 14–15].

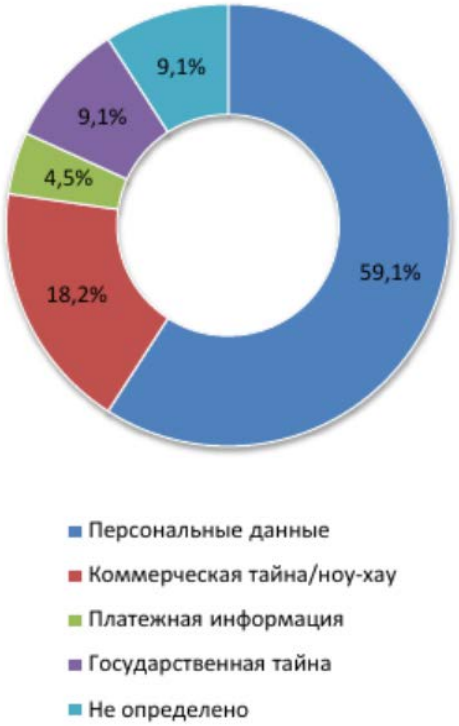

Рисунок 1 – Схема распределения утечки информации по виновным лицам [4, с. 15]

Зарегистрированные утечки связывают с накалившейся политической обстановкой после оглашения предварительных итогов президентских выборов (09.08.2020 г.), когда компрометация данных использовалась оппозицией как средство борьбы с действующей властью. В стране начались массовые акции протеста. Противостояние властей и оппозиции вылилось в подавление ряда митингов. В результате протестующие, используя свои каналы, начали «сливать» в сеть Интернет данные силовиков.

В 2022 г. примерами значимых утечек персональных данных стали факты распространения сведений о клиентах торговых сетей «Соседи» (более 630 тысяч), «Остров чистоты и вкуса» (более 140 тысяч), оператора доставки еды «Just-eat» (более 230 тысяч), баз данных РУП «Национальный центр маркетинга и конъюнктуры цен» (более 55 тысяч), Белгазпромбанка (около 42 тысяч) [5].

Значительно возросла активность вымогателей в первом квартале 2023 г., когда доля использования шифровальщиков в атаках на организации с использованием вредоносного программного обеспечения составила 53 %, что на 9 п.п. больше показателя прошлого квартала, а число инцидентов выросло на 77 % относительно начала 2022 г. Особенно напряженная обстановка наблюдается в секторе науки и образования – на него пришлись 19 % атак вымогателей [6].

Новшества продемонстрировали вымогатели BlackCat и HardBit. Первые начали выкладывать похищенные данные на сайты с адресами, похожими на домен скомпрометированной организации, чтобы факт утечки мог стать известен широкому кругу клиентов или партнеров компании. Вторые пытались убедить жертву раскрыть детали киберстрахования, чтобы скорректировать требования выкупа и гарантированно получить выплату от страховщика.

Модификация (изменение) компьютерной информации может способствовать ее утечке несколькими способами:

– несанкционированный доступ. Если злоумышленник имеет доступ к системе, в которой хранится информация, он может внести изменения в эту информацию, чтобы получить доступ к конфиденциальным данным. Например, злоумышленник может изменить пароль пользователя, чтобы получить доступ к его учетной записи;

– ошибки в программном обеспечении могут привести к тому, что информация будет изменена или раскрыта без ведома пользователя. Например, ошибка в алгоритме шифрования может привести к тому, что зашифрованные данные будут дешифрованы без ключа;

– вредоносное программное обеспечение, которое может быть специально разработано для модификации или раскрытия информации. Например, троян может быть использован для изменения файла конфигурации сервера, чтобы разрешить доступ к конфиденциальным данным.

2) Подрыв доверия и деловой репутации. Кибершпионаж может привести к нарушению доверия клиентов, партнеров и общественности. Утечка конфиденциальной информации или нарушение безопасности данных может нанести непоправимый ущерб репутации компании, что может отразиться на ее финансовых показателях и отношениях с клиентами.

3) Экономические потери. Украденная интеллектуальная собственность может быть использована конкурентами для создания аналогичных продуктов или услуг, что может снизить спрос на оригинальные продукты и привести к убыткам компании. Кибершпионы могут использовать собранную информацию для составления стратегий по захвату рыночной доли у конкурентов. С помощью украденных данных о ценах, планах продаж и маркетинговых стратегиях они могут установить более конкурентоспособные цены, предложить лучшие условия или создать продукты, которые будут привлекательными для клиентов конкурентов. Кроме того, восстановление после кибератаки может потребовать значительных финансовых ресурсов.

4) Распространение киберугроз. Злоумышленники, обладая передовыми киберспособностями, могут использовать их не только для осуществления шпионажа, но и для совершения других преступлений, таких как кибератаки на другие организации, мошенничество, вымогательство и т. д., что создает общую угрозу для бизнес-сообщества и общества в целом.

5) Шпионаж как услуга (EaaS). Появление EaaS сделало коммерческий кибершпионаж более доступным для более широкого круга субъектов угроз. Под EaaS подразумевается предоставление возможностей и инструментов кибершпионажа как услуги, позволяющей отдельным лицам или группам с ограниченными техническими навыками участвовать в шпионской деятельности. Предложения EaaS могут включать инструменты взлома, доступ к скомпрометированным сетям и даже специализированное обучение проведению шпионских операций.

Противодействие кибершпионажу требует комплексного подхода. Организации должны уделять особое внимание кибербезопасности и применять соответствующие меры защиты, такие как использование надежных паролей, многофакторной аутентификации, шифрования данных, регулярное обновление программного обеспечения и установку защитного программного обеспечения.

Непрерывные исследования и разработки в области технологий, программы обучения специалистов вопросам кибербезопасности и повышение осведомленности сотрудников и широкой общественности о киберугрозах также являются важными компонентами комплексной стратегии по борьбе с кибершпионажем.

Сотрудничество с кибербезопасными компаниями, правоохранительными органами и государственными учреждениями также может быть полезным. Такие организации могут предоставить экспертную помощь в обнаружении и расследовании кибератак, а также в разработке стратегий защиты от кибершпионажа.

Организациям следует инвестировать в надежные меры кибербезопасности, включая регулярные оценки уязвимостей, мониторинг сети и возможности реагирования на инциденты. Сотрудничество между государственным и частным секторами имеет решающее значение для обмена информацией об угрозах, координации усилий по реагированию на инциденты и разработки общих стандартов кибербезопасности.

Также необходимо дальнейшее усиление международного сотрудничества и обмен информацией о киберугрозах между государствами, что поможет предотвратить и пресечь киберпреступления в сфере коммерции.

Заключение. В целом кибершпионаж представляет значительную угрозу для организаций, экономики и национальной безопасности. Эффективная кибербезопасность, информи-

рованность и сотрудничество с ведущими организациями в области кибербезопасности являются ключевыми элементами противодействия этой угрозе.

Чтобы снизить риск утечки информации в результате ее модификации, необходимо принимать следующие меры:

– обеспечить надлежащий контроль доступа к системе. Только авторизованные пользователи должны иметь доступ к системе, в которой хранится информация;

– регулярно проводить аудит безопасности системы, что позволит выявить ошибки в программном обеспечении и другие потенциальные уязвимости;

– использовать надежные методы шифрования для защиты компьютерной информации от несанкционированного доступа;

– обновлять программное обеспечение до последней версии. Обновления программного обеспечения часто содержат исправления ошибок, которые могут привести к утечке информации.

Программисты также могут внести свой вклад в снижение риска утечки информации, разрабатывая программное обеспечение с учетом безопасности. При разработке такого программного обеспечения необходимо учитывать следующие факторы:

– безопасность должна быть одним из основных приоритетов;

– все функции программного обеспечения должны быть тщательно протестированы на предмет безопасности;

– необходимо использовать надежные методы шифрования;

– программное обеспечение должно регулярно обновляться.

Для повышения эффективности правового регулирования и раскрытия противоправных деяний такого рода считаем целесообразным внести следующие дополнения в ст. 254 и 358 УК:

1) ч. 1 ст. 254 УК после слова «способом» дополнить словами «, в том числе с использованием глобальной компьютерной сети Интернет либо иной информационной сети,»;

2) ст. 358 УК после слова «хранение» дополнить словами «, в том числе с использованием глобальной компьютерной сети Интернет либо иной информационной сети,».

Литература

1. Кибершпионаж [Электронный ресурс] / Управление Организации Объединенных наций по наркотикам и преступности. – Режим доступа : https://www.unodc.org/e4j/ru/cybercrime/module-14/key-issues/cyberespionage.html. – Дата доступа : 07.07.2023.

2. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 4 июня 1999 г. : одобрен Советом Республики 24 июня 1999 г. : в ред. Закона Республики Беларусь от 09.03.2023 г., № 256-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

3. Уголовный кодекс Республики Беларусь : научно-практический комментарий / Т. П. Афонченко [и др.] ; под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. – Минск : НЦПИ РБ, 2019. – 1000 с.

4. Утечки информации в Республике Беларусь. 2019–2020 годы / Экспертно-аналитический центр InfoWatch. – М., 2020. – 24 с.

5. В Национальном центре защиты персональных данных назвали компании, допустившие утечки данных в 2022 году [Электронный ресурс] // Беларусь Сегодня. – Режим доступа : https://www.sb.by/articles/sosedi-ostrov-chistoty-i-vkusa-i-drugie-v-ntszpd-rasskazali-o-samykh-bolshikh-utechkakh-dannykh-belo.html. – Дата доступа : 25.10.2023.

6. Актуальные киберугрозы : I квартал 2023 года [Электронный ресурс]. – Режим доступа : https://myfin.by/stati/view/aktualnye-kiberugrozy-i-kvartal-2023-goda. – Дата доступа : 25.10.2023.

Гомельский государственный
университет имени Франциска Скорины

Поступила в редакцию 27.04.2023