ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНОЙ СФЕРЕ

Горбачев Глеб Андреевич

Академия Федеральной Службы Охраны, РФ, г. Орёл

Тезин Александр Васильевич

научный руководитель, сотрудник, Академия Федеральной Службы Охраны, РФ, г. Орёл

Кокорев Антон Владимирович

научный руководитель, сотрудник, Академия Федеральной Службы Охраны, РФ, г. Орёл

INFORMATION SECURITY IN SOCIAL SPHERE

Gleb Gorbachev

Academy of the Federal Security Service, Russia, Orel

Anton Kokorev

Scientific director, Employee, Academy of the Federal Security Service, Russia, Orel

Alexander Tezin

Scientific director, Employee, Academy of the Federal Security Service, Russia, Orel

Аннотация. В статье рассматриваются возможные угрозы информационной безопасности в социальной сфере, а также наиболее частые методы реализации этих угроз.

Abstract. The article discusses possible threats to information security in the social sphere, as well as the most frequent methods of implementation of these threats.

Ключевые слова: информационная безопасность, социальная сфера, общественная опасность, хакер, угроза.

Keywords: information security, social sphere, public danger, hacker, threat.

Введение

Согласно Доктрине информационной безопасности Российской Федерации, информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства [1]. В Доктрине

отмечено, что информационная сфера является системообразующим фактором жизни общества и активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Подчеркивается, что национальная безопасность России во многом зависит от обеспечения информационной безопасности, и в ходе современного технического прогресса эта зависимость будет постоянно возрастать.

Вопрос социальной (общественной) безопасности был и остается одним из самых важных в общественной среде. Она связана с защитой интересов государства и его граждан в социальной сфере, развитием социальных структур и отношений, системы поддержки и социализации жизни людей, образа жизни, отвечающего потребностям прогресса нынешнего и будущих поколений.

Социальное обеспечение имеет многоуровневый характер. В России сегодня она определяется наличием негативных процессов в обществе, таких как рост преступности, падение уровня жизни, рост безработицы, разрушение старой системы образования, падение престижа науки и техники, разрыв между богатыми и бедными в обществе и ухудшение отношений между людьми.

Конституция, государство, президент и другие органы государственной власти должны обеспечивать социальную безопасность народа. Основными объектами социального обеспечения являются человек и общество, социальные интересы и общественные отношения, право на получение и использование соответствующей информации с учетом информационного аспекта и системы информирования населения.

С помощью существующих и перспективных информационных инструментов, и технологий можно практически полностью контролировать и регулировать информационный обмен людей. Речь идет о таких потенциальных возможностях, как перехват телефонных разговоров (но не только), контроль коммуникаций, создание компьютерных баз данных с конфиденциальной информацией о каждом человеке и т.д.

Современные информационные технологии стремительно повысили эффективность средств воздействия на психику людей и общественное сознание, создав новые формы "негласного" ("скрытого") манипулирования индивидуальным, коллективным и общественным сознанием. Неслучайно средства массовой информации (далее СМИ) называют "четвертым институтом". Дальнейшее развитие информационных технологий значительно расширит возможности СМИ и увеличит их власть. В этом контексте возникновение и развитие нового междисциплинарного направления информационной и психозащиты вполне оправдано.

Новые медиатехнологии, сетевые технологии с доступом к разнообразной негативной информации, такой как порнография и национализм.

Угрозы общественному сознанию

При рассмотрении социальных аспектов информационной безопасности важными показателями безопасности являются: осознание социальной стратификации и групповых различий; социальные чувства, установки и стереотипы; осведомленность о законопослушном поведении и использовании информации; зашита законных интересов.

Основными понятиями информационной безопасности в современном обществе являются «социальная активность в информационном пространстве» и «социальное пространство».

Социальное пространство – это тип пространства (в дополнение к физическому пространству и т.д.), в котором функционально взаимосвязаны социальные процессы, отношения, конвенции, социальный статус и поля. Философы и социологи понимают социальное пространство как логически мыслимый конструкт, то есть специфическую среду, в которой происходят социальные отношения. Таким образом, социальное пространство является одним из аспектов информационного пространства.

В самом общем виде информационное пространство обычно понимается как совокупность результатов семантической деятельности человека. Информационное пространство также

можно описать как совокупность используемой информации, процессов и систем, в которые она вовлечена: базы данных; технологии его обслуживания и использования; информационно-коммуникационные системы, функционирующие на основе общих принципов и гарантирующие информационное взаимодействие организаций и граждан и удовлетворение их информационных потребностей.

Так вышеперечисленные системы могут быть обозначены как наиболее часто встречающиеся объекты информационной безопасности в социальном пространстве.

Субъекты информационного пространства могут быть как индивидуальными, так и групповыми. Чаще всего в их роли выступают средства массовой информации, так как они активно генерируют информационные потоки. Так же субъектами могут выступать органы государственной власти и управления, структуры, вступающие в активную связь с населением. Это могут быть представители силовых ведомств и общественно-политические объединения. Видные политики и предприниматели, лидеры мнений, блогеры, деятели науки и искусства также являются активными информационными субъектами. Их главной чертой выделяют наличие у них интересов в генерации той или иной информации, как государственных, так и собственных.

Существование вышеперечисленных субъектов является одним из образующих факторов информационного пространства, составляющего социальную сферу нашей жизни. Тем не менее влияние указанных лиц и организаций на аудиторию и ее широкий охват могут являться угрозой безопасности государства и граждан. Так летом 2019 года среди пользователей социальной сети Facebook (социальная сеть, запрещенная на территории РФ, как продукт организации Meta, признанной экстремистской – прим.ред.) распространялись шуточные призывы к штурму одного из самых закрытых военных объектов в США – зоны 51. Мероприятие приобрело шуточный характер, 75 человек из 4 тысяч присутствовавших предприняли попытки проникновения на территорию зоны, двое из них были впоследствии задержаны. В качестве еще одного примера влияния лидеров мнений на массы можно привести еще один случай, произошедший в США 5 и 6 января 2021 года, по прошествии президентских выборов в США тысячи сторонников Дональда Трампа собрались в Вашингтоне. Собравшиеся были недовольны результатами выборов, которые они считали несправедливыми и сфабрикованными. Этот митинг произошел после заявлений вице-президента, в которых он обвинял выборную комиссию в допущении нарушений и неправильном подсчете голосов. Утром 6 января Дональд Трамп, его старший сын Дональд Трамп-младший и коллега президента по партии Руди Джулиани выступили с призывом к митингующим сражаться изо всех сил и вернуть страну. После речи протестующие проследовали к Капитолию, где часть из них предприняла попытку штурма. Штурм был неудачным, однако в результате происшествия погибло 4 человека, десятки получили ранения. На территории Капитолия впоследствии было обнаружено самодельные взрывчатые устройства, Федеральное бюро расследований завело более 170 уголовных дел.

Вышеописанные события наглядно иллюстрируют опасность неконтролируемого влияния лидеров мнений и показывают возможные последствия от использования такими людьми или организациями своего влияния в корыстных целях.

Угроза конфиденциальности

Основной социальной функцией информационной безопасности является обеспечение стабильности и устойчивости социально-экономического и общественно-политического развития общества перед лицом внутренних и внешних угроз, объективно следующих существующим закономерностям и тенденциям. В свою очередь, важнейшим социальным аспектом содержания информационной безопасности является система особенностей направлений информационных потоков, институтов и функций, которые могут соответствовать или не соответствовать характеру выполнения субъектами управления своих социальных функций.

Следует отметить, что нынешний уровень защиты персональных данных явно недостаточен, особенно в отношении информации о доходах и имуществе, что на практике приводит к многочисленным преступлениям. Сегодня защита персональных данных является

практически только теоретической концепцией.

Согласно отчету Positive Technologies за первый квартал 2022 года, доля атак на организации составляет 85%, из них 45% процентов были направлены на компрометацию конфиденциальной информации. Не лучше дела обстоят с частными лицами, несмотря на тот факт, что доля атак на них составляет лишь 15%, основной угрозой является утечка персональных данных. В 55% процентах случаев злоумышленники получили к ним доступ. В 25% атак была реализована угроза финансовой безопасности частных лиц [2]. Типы украденных данных представлены на рисунках 1 и 2.

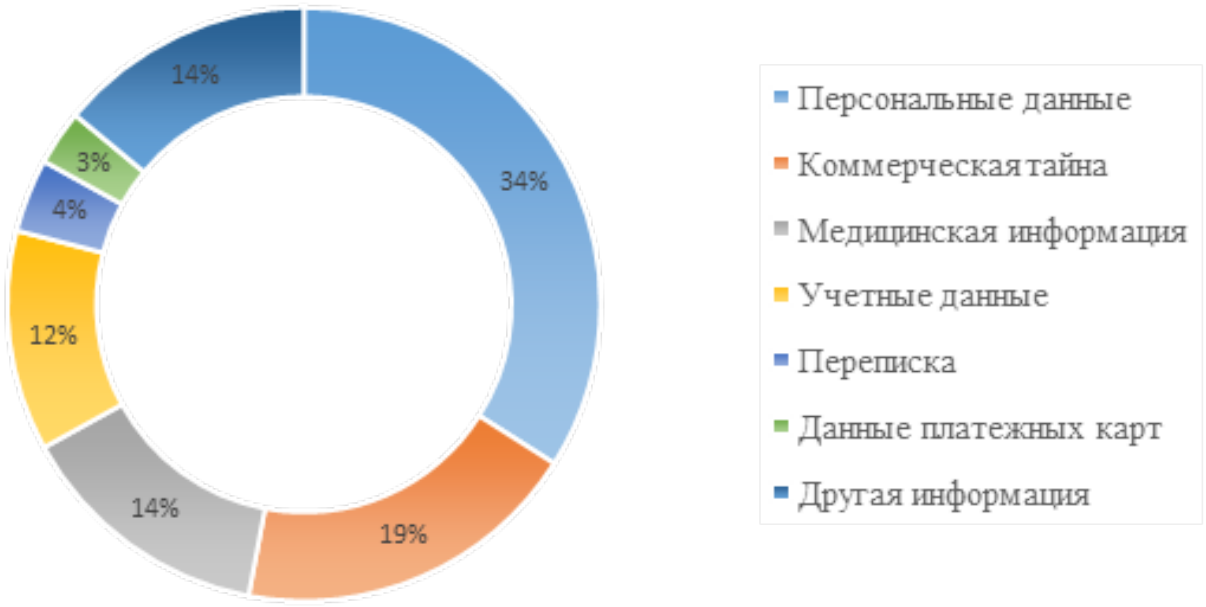

Рисунок 1. Типы украденных при атаках на организации данных

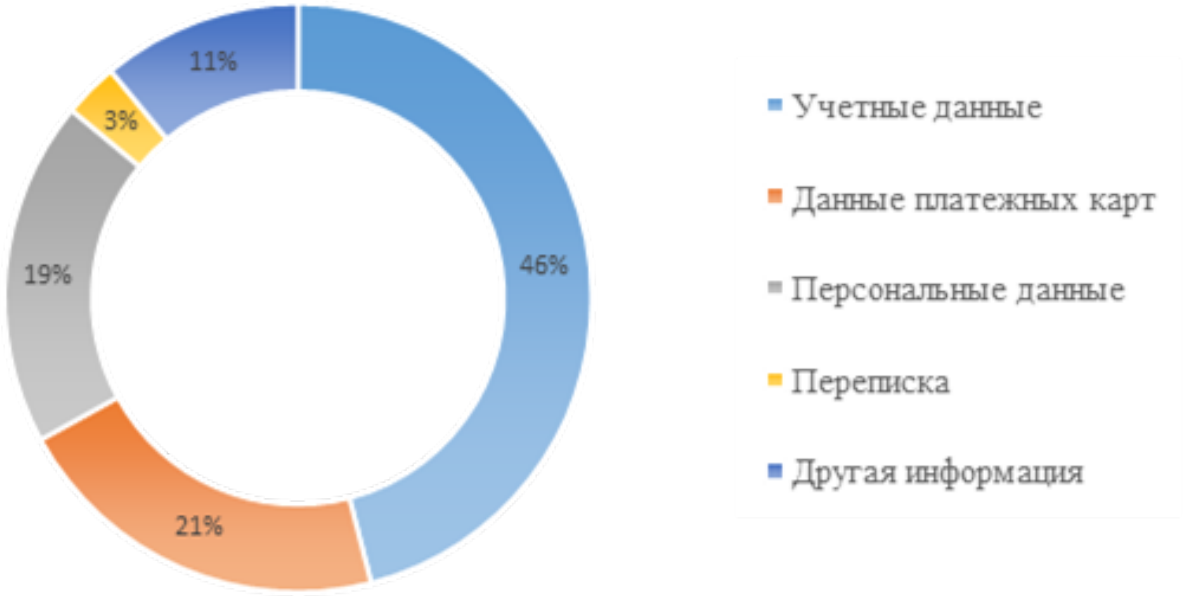

Рисунок 2. Типы украденных данных при атаках на частные лица данных

Наибольшую огласку получают атаки, направленные на крупные компании и учреждения. Можно привести несколько примеров произошедших утечек информации за минувший год. 1 марта 2022 года стало известно о факте утраты конфиденциальности информации 6,9 миллионов пользователей сервиса «Яндекс.Еда» и данные о 50 миллионах заказов. В сеть были выложены фамилии, имена, телефонные номера и адреса почты клиентов. 7 октября 2022 года Toyota Motor Corporation предупредило рассылкой уведомлений около 296 тысяч клиентов о возможном факте утечки их персональных данных из баз компании. В июле 2022 года «РИА Новости» со ссылкой на источник агентства в одной из российских спецслужб сообщило о доступе к информации тысячи сотрудников главного управления разведки министерства обороны Украины. Базы данных, в которых хранилась информация о сотрудниках, была вскрыта хакерской группировкой RaHDit.

Об основных видах атак

При рассмотрении безопасности персональных данных и другой конфиденциальной информации важным аспектом является инструмент, с помощью которого был получен доступ к информации.

Неаккуратные действия в сети «Интернет» становятся одной из наиболее частой причин нарушения конфиденциальности. Так в 2022 году интерес хакеров к веб-ресурсам возрос, доля атак на них увеличилась до 22%, по сравнению с 13%, наблюдаемыми в конце прошлого года.

Одной из распространенных методик атак на информационные системы является социальная инженерия. Ее методы используются в 90% атак на частные лица и в 41% на организации. Метод социальной инженерии подразумевает использование ошибок человека для получения доступа к информационной системе. Этим способом атаки активно пользуются как обычные мошенники, не имеющие подготовки в сфере информационной безопасности, так и опытные хакеры. Это объясняется тем фактом, что получить авторизационные данные путем манипулирования человеком гораздо проще, чем взломать систему безопасности. Об этом еще в 2001 году сообщил хакер и консультант по безопасности Кевин Митник в книге «Искусство обмана».

Социальная инженерия имеет четкую структуру, а методы обмана жертв достаточно обширны. Фишинг (от английского “fishing” – рыбалка) использует отправку жертве поддельных электронных сообщений, содержащих требования к определенным действиям. При этом рассылка производится от якобы официальной организации, а само письмо имеет деловой вид. Чаще всего такие письма содержат ссылки на поддельные интернет страницы, с которых происходит кража информации, например данных учетной записи. Кроме вышеописанного подхода к фишингу злоумышленники применяют и менее дерзкие методы обмана: письма с несуществующими лотереями, поздравлениями о победе в поддельных конкурсах или информацией о необходимости обновления средств антивирусной защиты. Не меньшей популярностью пользуется претекстинг. При проведении данной атаки злоумышленник выдает себя за другого человек, чаще всего в телефонном разговоре или в переписке по почте. Данный метод требует от преступника серьезной подготовки, ему необходимо знать как можно больше информации о человеке, чьим именем он пользуется, чтобы не вызывать подозрения у жертвы. Во избежание данных сложностей мошенник может представиться работником технического обслуживания, новым работником или сотрудником смежного подразделения организации. Кроме описанных методов социальной инженерии злоумышленник может использовать метод так называемого «дорожного яблока». Для этого ему необходимо оставить зараженные вредоносным программным обеспечением носитель информации в общественном месте, где его подберет жертва. Чтобы увеличить вероятность подключения носителя к устройству злоумышленник может оставить на нем различные подписи или примечания. Это могут быть поддельные реквизиты о регистрации внутри атакуемого учреждения или подписи, которые могут заинтересовать жертву, например «Отчет о доходах» или «Заработная плата за год» и т.п. Особо опасным подвидом социальной инженерии является обратная инженерия. Она подразумевает передачу жертвой информации по собственной инициативе. Несмотря на то, что это звучит абсурдно, но авторитетных в информационной среде коллег могут попросить о помощи при возникновении проблем. После чего «авторитету» остается лишь попросить жертву дать данные якобы необходимые для решения возникших трудностей.

Социальным инженерам особенно сложно противодействовать, поскольку они используют особенности человеческой натуры – любопытство, уважение к властям, желание помочь другу или коллеге. Но есть ряд советов о том, как обнаружить их атаки. Прежде всего необходимо задумываться, откуда могло прийти сообщение. Также необходимо убедиться, что человек, с которым вы общаетесь действительно является представившимся [3].

Ввиду напряженности в социальном и информационном пространствах атаки на государственные, правительственные учреждения и СМИ стали гораздо более распространенными. 16% процентов атак, направленных на организации, совершается на госучреждения, 5% на СМИ. Распространены атаки на сайты и порталы данных организаций, а самым простым методом реализации является реализация отказа в обслуживании (с английского “Denial of Service” – отказ в обслуживании, далее DoS-атака). DoS – это перегрузка сети паразитными запросами, таким образом, что отвечающий на них сервер теряет возможность использовать свои ресурсы для обработки запросов от пользователей. Также возможно перекрытие злоумышленником всей полосы пропускания входного маршрутизатора. Одной примечательной для хакеров чертой этих DoS-атак является тот факт, что организация атаки недельной продолжительности обычно не превышает 150 долларов, в то время как убытки в среднем составляют порядка 40 тысяч долларов в час. Данные атаки могут вестись как с одного ресурса, так и с нескольких, в таком случае речь идет о распределенной DDoS-атаке (Distributed DoS, с английского “distributed” – распределенный, далее DDoS-атака). Для генерации большого количества запросов используется сеть ботов или зомби-устройств. Зомби-устройства – устройства, зараженные вредоносным программным обеспечением, предоставляющим злоумышленнику возможность использования вычислительных ресурсов в своих нуждах.

Первая в мире DDoS-атака была зафиксирована в 1994 году. Произошла она на крупнейшего интернет-провайдера Нью-Йорка – Panix Networks. Организаторами были спамеры, недовольные запретом отправлять пользователям рекламные сообщения. Для атаки была использована уязвимость протокола TCP (Transmission Control Protocol, протокол управления передачей).

DoS-атаки подразделяются в зависимости от используемых механизмов атаки на несколько видов. Переполнение канала и использование незащищенности стека сетевых протоколов – виды DDoS-атаки, в которой используются уязвимости в протоколах сетевого взаимодействия, например в протоколах ICMP (Internet Control Message Protocol, протокол межсетевых управляющих сообщений), UDP (User Datagram Protocol, протокол пользовательских дейтаграмм), DNS (Domain Name System, система доменных имён), TCP. Такие атаки также часто называют низкоуровневыми по аналогии с уровнями модели взаимодействия открытых систем. Атака на уровне приложений происходит посредством изменения HTTP-заголовка (HyperText Transfer Protocol, протокол передачи гипертекста) в отправляемых пакетах и относится к высокоуровневым атакам. Для борьбы с DDoS-атаками применяются блокировки, особые настройки сетевых экранов, при которых минимизируется влияния устройств не из доверенного списка. Также необходимо скрыть IP-адреса сети и периодически менять их, по возможности разделить ресурсы, используемыми различными сервисами.

Таким образом можно сделать вывод, что социальная сфера является одной из важнейших сфер жизни общества, ввиду чего обеспечению ее безопасности всегда должно удаляться большое внимание. С развитием прогресса появляется все большое количество угроз, но и средства и способы защиты также не стоят на месте. Однако не все угрозы информационной безопасности могут быть решены программно-техническими средствами, поэтому необходимо проявлять бдительность, как в общественном пространстве, так и в виртуальном.

Список литературы:

1. Указ Президента РФ от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”

2. Актуальные киберугрозы: I квартал 2022 года [Электронный ресурс]: [сайт]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ - Дата обращения: 28.11.2022.

3. Социальная инженерия — защита и предотвращение [Электронный ресурс]: [сайт]. – Режим доступа: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks- Дата обращения: 28.11.2022.