УДК 33

БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Маркарьян Ю.А.

Кандидат технических наук, доцент кафедры «Экономика»

Донской государственный технический университет

Россия, г. Ростов-на-Дону

Михайличенко К.И.

Ассистент кафедры «Экономика»

Магистрант 1 курса, направление «Торговое дело(коммерция)»

Донской государственный технический университет,

Россия, г. Ростов-на-Дону

Андренко Е.В.

Студент

4 курс, факультет «Информационно-экономические системы»

Донской государственный технический университет,

Россия, г. Ростов-на-Дону

Аннотация: в статье рассмотрены аспекты безопасности электронной коммерции, статистика кибератак на различные организации, способы защиты от кибермошенников, определены угрозы экономической безопасности в сфере электронной коммерции.

Ключевые слова: безопасность, кибермошенник, кибератака, личные данные, преступление.

SECURITY OF E-COMMERCE SYSTEMS

Markaryan Yu.A.

Candidate of Technical Sciences, Associate Professor of the Department "Economics"
Don State Technical University
Russia, Rostov-on-Don
Mikhailichenko K.I.
Assistant of the Department "Economics"
Master Course 1 course, the direction of "Trading (Commerce)"
Don State Technical University,
Russia, Rostov-on-Don
Andrenko E.V.
Student
4 course, faculty "Information and Economic Systems"
Don State Technical University,
Russia, Rostov-on-Don

Annotation: the article deals with aspects of e-Commerce security, statistics of cyber attacks on various organizations, ways to protect against cyber criminals, identified threats to economic security in the field of e-Commerce.

Keywords: security, cyber-fraud, cyber-attack, personal data, crime.

Обеспечение безопасности необходимо для любых организаций, независимо от форм их собственности, начиная от государственных организаций и заканчивая маленькой палаткой, занимающейся розничной торговлей. Отличия будут состоять только в том, какие средства и методы и в каком объеме требуются.

В последнее время интерес злоумышленников к персональным данным растёт. Чаще всего они пытаются взломать страницы при помощи фишинга или используя уязвимости в смартфонах и компьютерах пользователя (рис. 1).

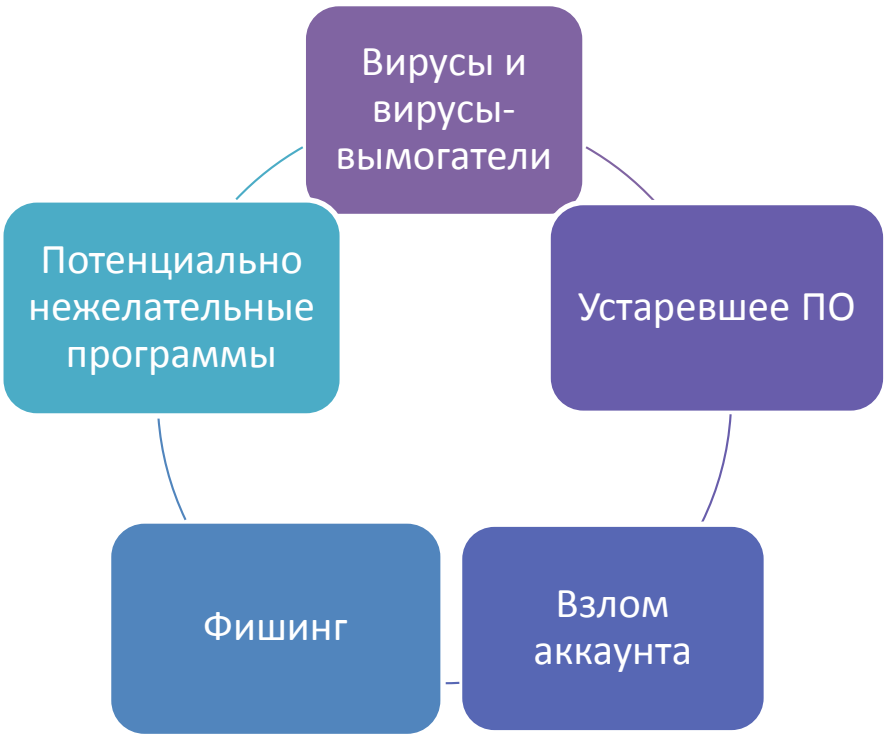

Рис. 1 – Самые распространенные виды хакерских атак.

Эксперты в области информационной безопасности указывают на перемены в поведении киберпреступников. Начиная с прошлого года, целью большинства нападений является не кража денег, а получение доступа к личным данным — логинам, паролям для доступа к сервисам и системам, в том числе к почте (рис. 2).

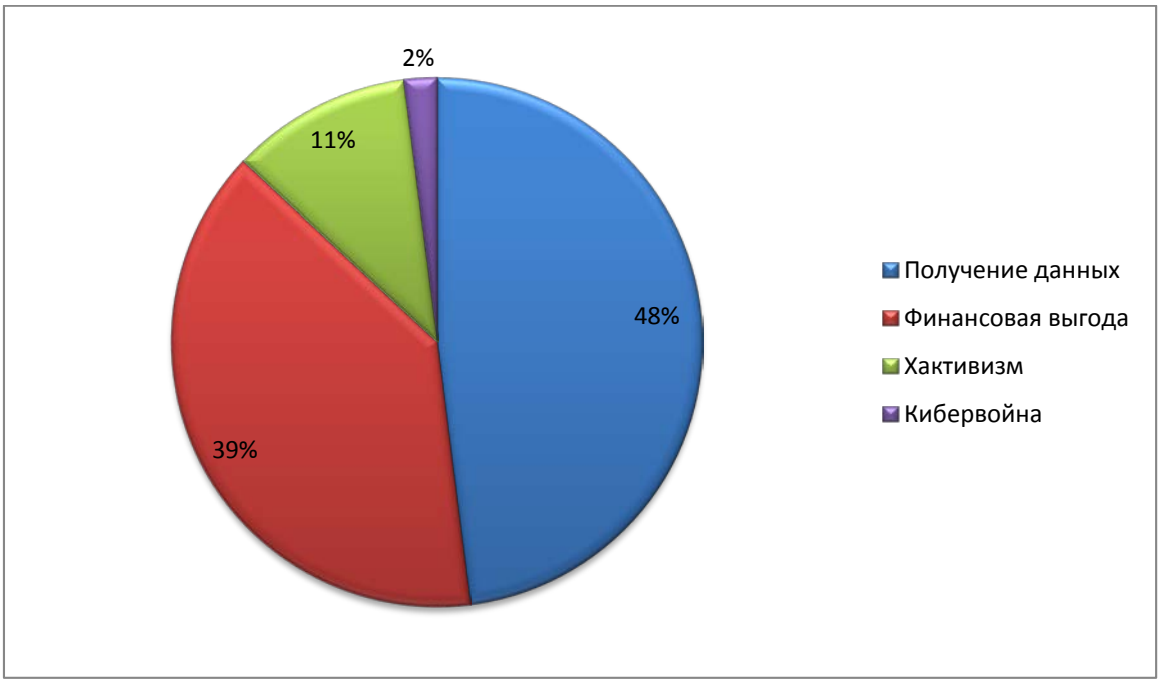

Рис. 2. – Цель кибератак.

Кража личных данных стала приоритетной целью среди преступников лишь во II квартале 2018 года — на ее долю пришлось 40% кибератак. Тогда злоумышленники были заинтересованы в личных и учетных данных, а также в данных банковских карт. Их воровали в основном с помощью создания двойников различных онлайн-площадок: интернет-магазинов, сервисов для продажи билетов, бронирования отелей и т.д. В 4 квартале 2018 года кража учетных данных была целью 48% кибератак.

В последнем квартале 2018 года количество уникальных киберинцидентов на 11% превысило данные аналогичного периода 2017 года и на 7% — показатели 3 квартала 2018 года. По данным аналитиков, число кибератак росло весь прошлый год. По их мнению, предпосылок для уменьшения динамики нет. Это связано как с повышением количества устройств, подключенных к интернету, так и с повышением числа данных в сети. Объектом атаки могут стать не только мобильные устройства, корпоративные сети и банкоматы, рабочие станции, но и принтеры, камеры, устройства интернета вещей и «умных» домов.

По данным «Лаборатории Касперского» в 2018 году замечено 1,9 млрд попыток онлайн-заражений устройств, а в 2017 году - 1 млрд. Что касается вредоносного программного обеспечения, то в 2018 году ежедневно появлялось около 360 тыс. его новых образцов, в 2017 году - 320 тыс. В основном речь идет о массовых, а не целевых атаках.

До последнего времени наиболее частыми целями для мошенников были финансовые учреждения, тем не менее ситуация начала меняться. Все чаще жертвами кибермошенников становятся государственные учреждения — их атакуют в 16% случаев. Государственные органы все чаще используют цифровые технологии, переводят свои услуги в интернет, однако защищают информацию менее эффективно, чем это делает частный бизнес. Устойчиво высокой остается доля атак на медицинские и образовательные учреждения.

В основном, киберпреступники отправляют письма на электронную почту сотрудников с целью заражения рабочих компьютеров вредоносным кодом и проведения целевых атак. Основной целью мошенников является проникновение внутрь корпоративной сети. Например, банк «Открытие» зафиксировал и нейтрализовал сотни рассылок с вредоносным кодом, успешных атак на банк не было, поэтому убытки отсутствуют.

Как бы то ни было, защитить компанию от кибермошенников получается далеко не всегда. Опираясь на данные опроса 192 компаний, можно сделать вывод, что в 2018 году 82% компаний-респондентов столкнулись с атаками, в 47% опрошенных компаний кибератаки оказались успешными, а 32% компаний понесли прямые финансовые потери в размере от 500 тыс. до 20 млн руб.

Организации, которые вынуждена защищаться от кибератак, всегда стоят перед сложным выбором: затраты на защиту не должны превышать ценность охраняемой информации. Согласно опросу, проведенному «Лабораторией Касперского» в 2018 году, в России цена устранения последствий от одного киберинцидента повысилась и в среднем составляла 74 тыс. долл. для малого и среднего бизнеса и 246 тыс. долл. для крупного бизнеса (рис. 3). В эту

стоимость включаются расходы на усовершенствование программного обеспечения и инфраструктуры, подготовку сотрудников, наём новых экспертов, компенсации, штрафы и т.д. Исходя из этого исследования можно сделать вывод, что в среднем в России на информационную безопасность выделяется около 20% бюджета на информационные технологии.

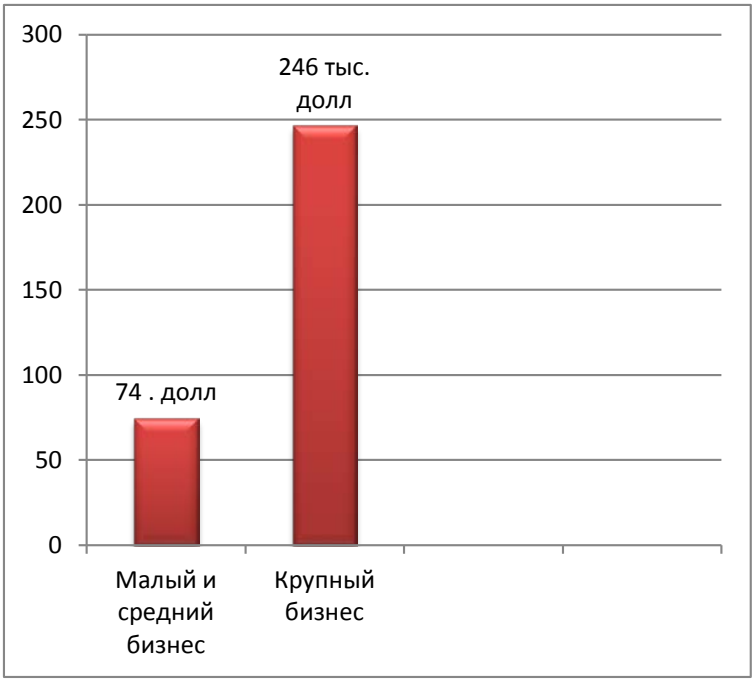

Рис. 3 – Затраты на устранение последствий кибератак в 2018 году.

При всем при этом, и такие расходы могут оказаться нецелесообразными. Если говорить о должном уровне информационной безопасности, то нужно отталкиваться от того, на что этот бюджет тратится. Можно закупить дорогостоящие программы для обеспечения безопасности и выявления атак, однако при этом не иметь в штате сотрудников высокого уровня подготовки, чтобы эти системы продуктивно применять. В этом случае даже бюджет в сотни миллионов рублей не поможет защититься от хакеров. Организации тратят на информационную безопасность примерно 10% от бюджета на информационные технологии, но этот подход не всегда результативен, ведь успешные атаки разного уровня продолжают случаться.

Например, в социальной сети «ВКонтакте» своей задачей видят

своевременное предотвращение взлома аккаунтов, для этого компания использует специальные механизмы на базе искусственного интеллекта. «Но стратегически очень важно повышать общую компьютерную грамотность пользователей интернета. Мы рекомендуем не устанавливать нелицензионный софт, не использовать непроверенные бесплатные VPN-сервисы и прокси-серверы, не переходить по подозрительным ссылкам и не отправлять персональную информацию незнакомцам», — говорит Сергей Кубасов. О важности работы с конечным пользователем напоминают и в «Лаборатории Касперского»: «Очень большого количества инцидентов можно избежать, если установить защитные решения на компьютеры, а также провести обучение сотрудников основам киберграмотности».

В 2018 году аналитики антивирусной компании McAfee подсчитали, что в 2017 году мировой ущерб от киберпреступлений составил около $600 млрд или 0,8% от мирового ВВП, увеличившись примерно на 35% по сравнению с оценкой за 2014 год в $445 млрд. Среди факторов, обусловивших рост, специалисты перечислили все более изощренные хакерские атаки, расширение рынка киберкриминальных услуг и распространение криптовалют.

Вот несколько примеров крупнейших хакерских атак за последнее время:

1.В январе 2012 года был закрыт сайт MegaUpload. В знак протеста Anonymous провела крупнейшую в истории DDoS-атаку с применением LOIC. На несколько часов были выведены из строя сайты ФБР, Белого дома, Министерства юстиции, холдинга звукозаписи Universal Music Group, Американской ассоциации звукозаписывающих компаний, Американской ассоциации кинокомпаний, Американского управления авторского права. В апреле 2013 года Anonymous атаковали более 100 тысяч израильских сайтов. Общий ущерб от атаки сами хакеры оценили в $3 млрд. Акция стала ответом на операцию «Облачный столп», прошедшую в ноябре 2012 года. Также

хактивисты во время украинского кризиса в марте подвергли мощной атаке правительственные сайты РФ и сайты российских СМИ.

2. 300 тысяч компьютеров и 150 стран мира — такова статистика по пострадавшим от этого вируса-шифровальщика. В 2017 году в разных концах света он проник в персональные компьютеры с операционной системой Windows (воспользовавшись тем, что они не имели на тот момент ряда необходимых обновлений), перекрыл владельцам доступ к содержимому жёсткого диска, но пообещал вернуть его за плату в 300 долларов. Те, кто отказался платить выкуп, лишились всей захваченной информации. Ущерб от WannaCry оценивается в 1 мдрд долларов. Авторство его до сих пор неизвестно, считается, что к созданию вируса приложили руку разработчики из КНДР.

Делая вывод, можно сказать, что в нашем обществе все больше внимания уделяется вопросам безопасности, причем как на высшем уровне, так и на уровне отдельных организаций и институтов. Предполагается, что, в конечном счете, это приведет к заметному улучшению состояния национальной экономической безопасности.

Библиографический список:

1. Богданов И.А. Экономическая безопасность России: теория и практика. - М.: ИСПИРАН, 2009.

2. Богомолов В.А., Эриашвшш Н.Д. Экономическая безопасность. ЮНИТИ-ДАНА. 2010.

3. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. М., 2004.

4. Сенчагова В.К. «Экономическая безопасность России» Дело. 2010.

5. [Электронный ресурс]/ /URL: https://www.rbc.ru/politics (03/03/2019)

Оригинальность 90%