УДК 340(082) **DOI: 10.14529/iimj180214**

ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИХ ВЛИЯНИЕ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЙ

НОРИН В.Г., ФЕДОРЕНКО Е.А.
Хабаровский государственный университет экономики и права, г. Хабаровск, Россия

Аннотация. Цель работы – определить, каким образом IT-преступления могут влиять на экономическую безопасность предприятий. Соответственно, предметом исследования является влияние IT-преступлений на экономическую безопасность организаций. В статье рассмотрена сущность отдельных видов киберпреступлений, их мотивы и влияние на работу организаций. Проанализированы статистические данные по произошедшим кибератакам на глобальном уровне, а также в разрезе отдельных стран и компаний. Сделаны выводы о влиянии IT-преступлений на экономическую безопасность организаций, даны рекомендации по повышению киберзащиты на предприятиях. Выяснено, что киберпреступления, хоть и косвенно, но в значительной степени могут снизить экономическую безопасность фирм, в особенности малого бизнеса. Полученные результаты могут быть применены в условиях принятия решений о разработке стратегии киберзащиты на предприятиях.

Выяснено, что инновационный малый бизнес является одним из главных инструментов национальной безопасности. Полученные результаты могут быть применены при реализации Стратегии экономической безопасности Российской Федерации.

Ключевые слова: экономическая безопасность, информационные технологии, киберпреступления, финансовые услуги, информация, коммуникации

На постиндустриальном этапе развития общества невозможно умалять роли информационных технологий в формировании стабильно функционирующих предприятий, обеспечении их конкурентоспособности, защите от внешних угроз. Не случайно высший этап постиндустриальной экономики называют «экономикой знаний», а информация на сегодняшний день является ключевым фактором развития организаций, отдельных стран и мира в целом.

Однако стремительное развитие информационных технологий влечет за собой и новые угрозы, ранее не известные обществу. Информация, являющаяся ценным товаром (особенно в контексте бизнеса и инноваций), обретает ряд уязвимостей и часто становится объектом преступлений. На микроэкономическом уровне хозяйствования это может повлиять на ключевые индикаторы экономической безопасности, подрывая стабильность работы предприятий, снижая ее эффективность. В связи с этим, исследование является актуальным.

Преступления в сфере информационных технологий, или киберпреступления, вовлекают компьютеры и сети в противоправные действия по отношению к индивидуумам, организациям и целым странам. Наиболее частым инструментом киберпреступлений являются DoS- и DDoS-атаки – традиционная (DoS) либо распределенная (DDoS) атака типа «отказ в обслуживании». Первая используется для преступлений против небольших организаций, вторая – хорошо защищенных крупных компаний. Механизм таких атак представлен следующим образом. Злоумышленник рассылает на множество

случайных компьютеров вредоносное программное обеспечение. Чаще всего это происходит с помощью электронных писем, в которых содержатся вложения – файлы, прикрепленные к письму. Для того, чтобы заставить пользователей открыть файлы, преступник может замаскировать адрес отправителя, текст и вложения как отправленные от родственников и друзей или содержащие выгодное и заманчивое предложение. Как только пользователь, открывает файл, его компьютер считается зараженным.

Если злоумышленник отправил подобные электронные письма, к примеру, на 200 тысяч адресов, и 10% пользователей запустили вредоносное ПО на своих компьютерах, значит, в его распоряжении оказались 20 тысяч зараженных компьютеров, объединенных в сеть под названием «ботнет». Всеми этими устройствами преступник теперь может управлять удаленно, используя их в качестве инструмента атаки.

Если происходит команда совершить «ping-флуд» (дословно – «наводнение запросами»), тысячи компьютеров почти одновременно пытаются посетить вебсайт организации, причем пользователи атакующих устройств остаются в неведении, так как посещение сайта визуально не отображается. Серверы компаний, не адаптированные к настолько нагруженному трафику, не в состоянии обработать такое большое количество запросов, в связи с чем происходит отказ некоторых элементов системы [15].

Такие атаки парализуют работу компьютерной сети организации, лишая клиентов возможности воспользоваться ее услугами. В дальнейшем злоумышленники могут получить доступ к системе и похитить информацию. На уровне предприятий основными мотивами IT-преступлений могут являться похищение финансовых средств и обеспечение финансовых потерь, кража интеллектуальной собственности и корпоративных конфиденциальных данных, нанесение ущерба репутации компании [26]. Стоит рассмотреть каждый из мотивов более подробно.

Похищение финансовых средств – это наиболее частый мотив киберпреступлений, в частности, в финансовом секторе – его называют «магнитом для киберпреступности». Количество кибератак на организации этой отрасли в 2016 году выросло на 29% по сравнению с 2015 годом, что неудивительно – из компьютерных систем таких компаний можно добыть данные клиентов, предоставляющие доступ к большим объемам финансовых средств (данный вид преступлений называется «фишинг») [1]. Финансовые потери от киберпреступлений, в свою очередь, несут любые предприятия, независимо от отрасли. Неспособность компьютерной системы своевременно получать, обрабатывать и отправлять информацию ведет к нарушению функционирования предприятия, снижению его продуктивности, что сказывается на объемах продаж товаров, работ и услуг.

Кража интеллектуальной собственности происходит в результате доступа преступников к компьютерной сети организации. В то время как похищение данных клиентов влечет за собой ощутимые расходы в настоящем, украденные технологии и секреты фирмы оказывают значительное влияние на будущее компании. Инициаторами таких преступлений могут являться не только конкуренты, но и злоумышленники, заинтересованные в продаже полученных данных. Кроме того, узнав о бизнес-стратегиях той или иной компании, можно использовать эту информацию для правильного поведения на бирже или инвестиций, получая абсолютно легальный доход [11]. Отраслями с

высоким риском похищения интеллектуальной собственности являются фармацевтика, биотехнологии, IT и химическая промышленность [6].

Согласно статистике, около 80% активов компаний содержатся в цифровом виде [25]. Это означает, что восприятие компании рынком непосредственно связано с тем, насколько успешно в ней устроена система компьютерной защиты. Инвесторы и акционеры заинтересованы в сохранности собственных вложенных в компанию средств, клиенты – в конфиденциальности своих личных данных. Утечка того или другого провоцирует недоверие общественности, что не только лишает организацию существующих инвесторов и покупателей, но и не дает возможности обзавестись новыми, что подрывает репутацию.

Необходимо проанализировать, как произошедшие за последние несколько лет киберпреступления повлияли на бизнес в целом, некоторые отрасли и отдельные компании. Это станет базой для определения основных направлений влияния таких преступлений на экономическую безопасность предприятий.

Согласно Отчету о кибербезопасности, подготовленному компанией Cisco Systems, влияние IT-преступлений на определенные функции компаний распределяется следующим образом:

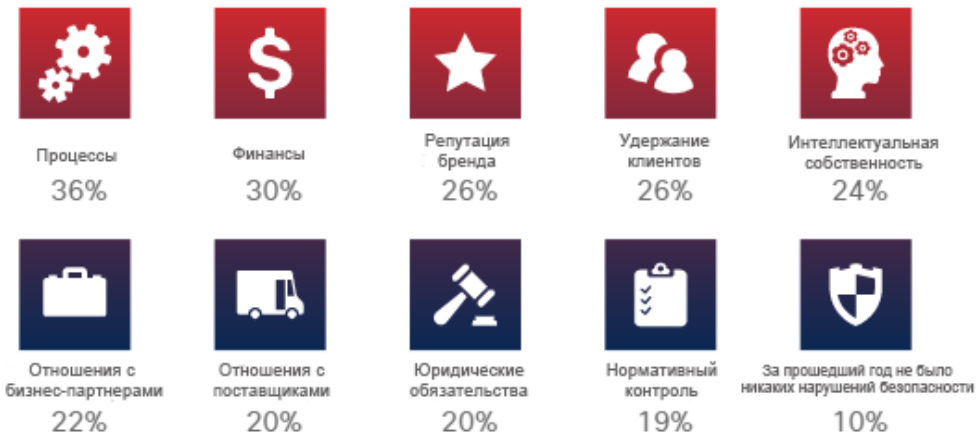

Рисунок. 1. Влияние киберпреступлений на функции компаний [3]

В каких же показателях наиболее явно прослеживалось негативное влияние таких преступлений? Глобально, 29% компаний потеряли прибыль из-за IT-преступлений, пятая часть из этих компаний потеряла от 20% до 40% прибыли. 23% организаций испытали так называемые «упущенные возможности», то есть потерю доходов от более выгодных альтернативных возможностей при принятии решений. 22% не смогли удержать клиентов, причем пятая часть таких компаний существенно сократила клиентскую базу, потеряв от 20% до 40% потребителей. В 90% исследуемых компаний посягательство на их компьютерную систему заставило пересмотреть технологии, политику и процедуры защиты от угроз. Безусловно, все это потребовало крупных финансовых вложений [3].

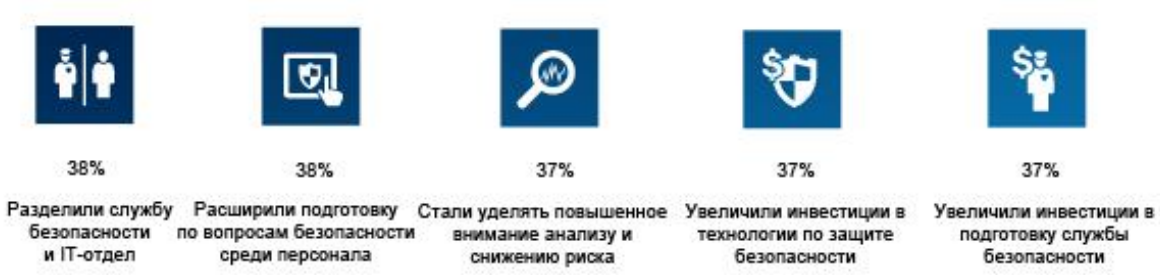

Рисунок. 2. Изменения в компаниях после киберпреступлений [3]

По прогнозам, в 2019 году издержки по избавлению от последствий киберпреступлений будут равняться 2,1 трлн. долларов, увеличившись почти в 4 раза по сравнению с 2015 годом. Сейчас средний объем издержек одной компании на избавление от уязвимости составляет 3,8 млн долларов [4]. Незамедлительно на заявления о киберпреступлении реагирует цена акций компании. Согласно исследованию, сразу же после того, как информация об утечке данных компании становится общедоступной, цена акции снижается в среднем на 0,43%. Кроме того, темпы роста цены после решения проблем с безопасностью существенно снижаются: если за три года до утечки данных цена акции в среднем выросла на 45,6%, то за три года после – всего на 14,8% [2].

Наиболее подвержены кибератакам следующие отрасли: финансовые услуги, информация и коммуникации, производство, розничная торговля и здравоохранение [13]. Что касается финансового сектора, IT-преступления в этой отрасли стали более частыми, масштабными и изощренными, чем раньше. США, будучи крупнейшим финансовым центром мира благодаря Нью-Йорку, являются наиболее привлекательной страной для финансовых киберпреступников. Согласно Forbes, только четыре крупные американские финансовые организации – J.P. Morgan, Bank of America, Citibank и Wells Fargo – в 2015 году потратили на борьбу с киберпреступностью более 1,5 млрд долларов [21].

Говоря о характере киберпреступлений, следует заметить, что отрасль здравоохранения лидирует по доле атак, совершенных злонамеренным инсайдером – то есть, сотрудником компании. Даже в более уязвимых отраслях доля таких атак не превышает 5%.

Таблица 1

Лидирующие отрасли по количеству киберпреступлений, с указанием характера атак [13]

Ранг	Отрасль	Злонамеренных инсайдерских атак, %	Непреднамеренных, по неосторожности работников, %	Посторонними, %
1	Финансовые услуги	5	53	42
2	Инф. и комм.	1	3	96
3	Производство	4	5	91
4	Розница	2	7	91
5	Здравоохранение	25	46	29

Издержки на избавление от последствий киберпреступлений в здравоохранении составляют около 200 долларов на пациента. Напротив, стоимость предотвращения таких преступлений – всего около 8 долларов на пациента. В 2016 году около 63% организаций этой отрасли планировали потратить на обеспечение кибербезопасности более 1 млн долларов каждая [16]. В 2015 году 3 из 7 крупнейших утечек информации произошли в отрасли здравоохранения, самой значительной из которых стала утечка данных более 18 тысяч клиентов и работников медицинской страховой компании Anthem. Для урегулирования всех исков, предъявленных теми, чьи данные были украдены, компании пришлось заплатить 115 млн долларов. По оценкам юристов, это крупнейшая в мире компенсация за утечку данных [19].

Другим говорящим случаем стала атака на веб-сайт британского провайдера TalkTalk, откуда были украдены личные данные 157 тысяч клиентов, включая имена, адреса, даты рождения, номера телефонов и адреса электронной почты. Согласно расследованию, провайдер не обеспечил должного уровня безопасности, что позволило посторонним лицам с легкостью получить доступ к конфиденциальным данным. На компанию был наложен штраф в размере 400 тысяч фунтов стерлингов [12]. Однако наиболее негативные последствия выражались в испорченной репутации. Крупнейшие СМИ, включая Reuters, The Times и Financial Times, критиковали компанию за нанесение ущерба потребителям, называя ее «безответственной». Акции провайдера упали на 11%. Жалобы клиентов на долгое ожидание компенсаций распространялись в социальных сетях, провоцируя создание негативного имиджа [22]. После инцидента компания потеряла 230 тысяч (5%) клиентов [9].

Еще одним примером снижения репутации является Yahoo, которая за последние несколько лет трижды стала жертвой кибератак, что в совокупности привело к компрометации почти 2 млрд. аккаунтов. В 2017 году произошло поглощение компании конгломератом Verizon. Скорее всего, именно ситуации с киберпреступлениями против Yahoo привели к тому, что Verizon заплатила за поглощение на 350 млн. долларов меньше, чем объявляла годом ранее [7].

В последнее время глобальное распространение получил отдельный блок кибератак – внедрение в компьютерные системы организаций вирусов-вымогателей. Заражение таким вирусом происходит по схеме, аналогичной DDoS-атаке. Однако, в отличие от нее, он не преследует цель перегрузить серверы компании с помощью зараженного компьютера. Посредством изощренных механизмов он парализует работу самого компьютера, оповещая пользователя о том, что доступ к своим данным он получит только после перечисления определенной суммы на анонимный кошелек. Кроме того, попав на компьютер пользователя, он осуществляет рассылку аналогичных вредоносных писем всем контактам, находящимся в почтовом клиенте компьютера [10].

В 2017 году организации по всему миру поразили два таких вируса: «Petya» и «WannaCry». В мае WannaCry распространился на более чем 400 тысяч компьютеров. Несмотря на то, что только 0,07% жертв перечислили средства для получения доступа к данным, преступники обогатились на более чем 120 тысяч долларов (по курсу на май 2017 года) [5]. Если учесть увеличившийся за это время курс биткоина к доллару и возможность того, что злоумышленники не выводили средства, сумма доходов от распространения вируса может достигать 560 тысяч долларов. Сильнее всего WannaCry поразил

российские предприятия: банки, телекоммуникационных провайдеров, ОАО РЖД и другие [23]. По оценкам, затраты на избавление от его последствий составили около 4 млрд долларов [14].

27 июня 2017 года компании по всему миру атаковал другой вирус-вымогатель под названием «Petya». Пострадали от него такие компании, как Роснефть, A.P. Moller-Maersk, WPP, украинские и российские банки и другие [20]. Издержки датской судоходной компании Maersk составили около 300 млн. долларов [18]. Другие компании практически не раскрывают информацию о потерях за счет вируса, однако стоит предположить, что они достаточно велики.

Еще одним заметным случаем считается заражение похожим вирусом-вымогателем южнокорейской фирмы Nayana, занимающейся веб-хостингом. Требования злоумышленников в обмен на сохранность корпоративных данных были настолько высоки, что компании пришлось перечислить на анонимный кошелек 1 млн долларов. Это считается крупнейшим зафиксированным перечислением средств вирусу-вымогателю за все время. Как только об этом стало известно широкой публике, акции компании незамедлительно упали более чем на 3% [17].

Теперь, после анализа основных мотивов, проявлений и последствий IT-преступлений, важно обобщить результаты и определить, как такие преступления могут влиять на экономическую безопасность предприятий. В целом, все издержки, которые фирма может понести по причине кибератак, можно выделить в следующий перечень:

1. Явные: уведомление клиентов об утечке данных; защита клиентов после утечки; выплата штрафов за необеспечение надлежащей сохранности данных клиентов; PR/Кризисные коммуникации; затраты на адвокатов и судебные разбирательства; улучшение кибербезопасности; техническое расследование.

2. Менее явные: увеличение страховых премий; увеличение стоимости привлечения долга; ликвидация операционных сбоев; снижение ценности взаимоотношений с клиентом; упущенная выгода по контрактам; обесценение торговой марки; потеря интеллектуальной собственности [24].

Все эти затраты, несомненно, подрывают стабильное функционирование предприятия. Они относятся к внереализационным расходам, то есть, не связаны с продажей продукции или оказанием услуг клиентам. Они не сопряжены с наращиванием продаж или клиентской базы, а значит, не предполагают генерирование прибыли. Таким образом, при прочих равных условиях, объем расходов в краткосрочном периоде вырастет, а доходы – нет. Это снизит чистую прибыль предприятия, что, в свою очередь, снизит показатели рентабельности.

Кроме того, появление новых затрат вынуждает привлекать больше заемных средств. Это особенно справедливо для малого бизнеса, где нет достаточных ресурсов для обеспечения надежных киберзащитных механизмов, а стоимость избавления от последствий кибератак несоизмеримо высока. Увеличение заемных средств провоцирует снижение ликвидности предприятия, делая его все более зависимым от внешнего финансирования. Это представляет прямую угрозу экономической безопасности.

Помимо этого, многие менее явные издержки угрожают стабильности в долгосрочном периоде – прежде всего, это обесценение нематериальных активов и потеря репутации. Украденные секреты фирмы могут лишить компанию конкурентного преимущества, что снизит буду-

щие денежные потоки, а кража еще не реализованных инновационных технологий не позволит «снять сливки» после внедрения, обеспечив тем самым высокую прибыль. Наконец, подрыв репутации может лишить предприятие инвестиций и клиентов, снизить его доходность и платежеспособность.

Выводы о влиянии кибератак на деятельность предприятий прямо указывают на то, что предотвращение таких преступлений требует гораздо меньших затрат, чем избавление от их последствий. В связи с этим, компаниям необходимо разработать стратегию повышения корпоративной кибербезопасности. Она может включать следующие решения:

1. Обучение персонала по вопросам киберзащиты. Как известно, многие атаки совершаются за счет неосторожности работников, запускающих вредоносное программное обеспечение через e-mail. Важно предостерегать персонал от открытия нежелательной корреспонденции, рассказать об основных способах распознавания мошеннических писем.

2. Пригласить стороннюю аккредитованную организацию для оценки уровня кибербезопасности и кибер-осведомленности на предприятии, которая сможет разработать план повышения защиты в случае выявления недостатков.

3. Убедиться в том, что существует иерархия доступа к корпоративным данным, согласно которой новые работники, а также занимающие должности низового звена и должности с высокой текучкой кадров имеют наименьший доступ к данным о компании.

4. Аккаунт каждого работника должен обладать надежным паролем, включающим не менее 10 символов, чередовать буквы верхнего и нижнего регистров, а также обязательно иметь цифры и символы.

5. Обеспечить высокую емкость сервера, которая может справиться с высокой нагрузкой и большим количеством запросов.

6. Установить технологию мониторинга данных сети, которая позволит дать представление об индикаторах нормальной работы корпоративных компьютеров. Значительное изменение каких-либо показателей поможет незамедлительно определить надвигающуюся атаку и вовремя ее предотвратить.

7. Программное обеспечение защиты данных должно быть лицензионным и постоянно обновляться.

8. Сотрудники IT-отдела должны быть высококвалифицированными, их подбор должен осуществляться профессионалом в IT-области [8].

Таким образом, преступления в сфере информационных технологий оказывают довольно значительное влияние на экономическую безопасность предприятия с помощью косвенных факторов. Они снижают платежеспособность, ликвидность, доходность и рентабельность предприятия, повышают его зависимость от заемных средств. Крупные компании зачастую способны самостоятельно избавиться от последствий кибератак, в то время как малый бизнес достаточно уязвим, и может находиться под угрозой снижения экономической безопасности. Для предотвращения IT-преступлений предприятия обязаны разработать актуальную стратегию киберзащиты и неукоснительно ее соблюдать.

Литература:

1. Alvarez M. A Magnet for Cybercrime: Financial Services Sector. 2017. Режим доступа: https://securityintelligence.com/a-magnet-for-cybercrime-financial-services-sector/ (дата обращения: 14.01.2018)

2. Bischoff P. Analysis: How data breaches affect stock market share prices. 2017. Режим доступа: https://www.comparitech.com/blog/information-security/data-breach-share-price/ (дата обращения: 18.01.2018)

3. Cisco 2017. Annual Cybersecurity Report. Режим доступа: https://engage2demand.cisco.com/en-us-annual-cybersecurity-report-2017 (дата обращения: 17.01.2018)

4. Cook S. Cybercrime stats & facts for 2016-2017. 2017. Режим доступа: https://www.comparitech.com/vpn/cybercrime-statistics-2016-2017/ (дата обращения: 18.01.2018)

5. Crowe J. WannaCry Ransomware Statistics: The Numbers Behind the Outbreak. 2017. Режим доступа: https://blog.barkly.com/wannacry-ransomware-statistics-2017 (дата обращения: 27.01.2018)

6. Dempsey M. Cyber crime: Biggest danger to intellectual property comes from within. 2013. Режим доступа: https://www.ft.com/content/856b17e8-a760-11e2-9fbe-00144feabdc0 (дата обращения: 15.01.2018)

7. Eubanks N. The True Cost Of Cybercrime For Businesses. 2017. Режим доступа: https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#5cd191c74947 (дата обращения: 15.01.2018)

8. Featherstone E. Protecting your business from cybercrime – what the experts say. 2016. Режим доступа: https://www.theguardian.com/small-business-network/2016/dec/05/how-to-protect-business-cybercrime-advice-experts (дата обращения: 27.01.2018)

9. Fildes N. TalkTalk warns of profit fall in 2017-18 under new strategy. 2017. Режим доступа: https://www.ft.com/content/7e43df6a-354e-11e7-bce4-9023f8c0fd2e (дата обращения: 18.01.2018)

10. Fruhlinger J. What is ransomware? How it works and how to remove it. 2017. Режим доступа: https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html (дата обращения: 27.01.2018)

11. Hackers are after your intellectual property, not only your money. Panda Security. 2017. Режим доступа: https://www.pandasecurity.com/mediacenter/security/hackers-intellectual-property/ (дата обращения: 14.01.2018)

12. Hern A. TalkTalk hit with record £400k fine over cyber-attack. 2016. Режим доступа: https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack (дата обращения: 18.01.2018)

13. IBM X-Force Threat Intelligence Index 2017. Режим доступа: https://www.ibm.com/security/data-breach/threat-intelligence (дата обращения: 18.01.2018)

14. Lehnis M. Total WannaCry losses pegged at $4 billion. 2017. Режим доступа: https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/ (дата обращения: 27.01.2018)

15. Mercer C. What is a DDoS attack? What happens during a DDoS attack? 2017. Режим доступа: https://www.techworld.com/security/how-does-ddos-attack-work-3659197/ (дата обращения: 27.01.2018)

16. Morgan S. Top 5 Industries At Risk Of Cyber-Attacks. 2016. Режим доступа: https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#32d9c174715e (дата обращения: 18.01.2018)

17. O'Brien D. Internet Security Threat Report. 2017. Режим доступа: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf (дата обращения: 27.01.2018)

18. Palmer D. Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk. 2017. Режим доступа: http://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/ (дата обращения: 27.01.2018)

19. Pierson B. Anthem to pay record $115 million to settle U.S. lawsuits over data breach. 2017. Режим доступа: https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML (дата обращения: 18.01.2018)

20. Reuters Staff. Factbox: Companies hit by global ransomware attack on June 27. 20170. Режим доступа: https://www.reuters.com/article/us-cyber-attack-factbox/factbox-companies-hit-by-global-ransomware-attack-on-june-27-idUSKBN19I29O (дата обращения: 27.01.2018)

21. Roohparvar R. 5 Industries That Top the Hit List of Cyber Criminals in 2017. Режим доступа: http://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/ (дата обращения: 27.01.2018)

22. The reputational risk of cybersecurity attacks: TalkTalk case study. Alva. 2015. Режим доступа: http://www.alva-group.com/en/the-reputational-risk-of-cyber-attacks-talktalk-case-study/ (дата обращения: 18.01.2018)

23. Vigliarolo B. Gallery: 10 major organizations affected by the WannaCry ransomware attack. 2017. Режим доступа: https://www.techrepublic.com/pictures/gallery-10-major-organizations-affected-by-the-wannacry-ransomware-attack (дата обращения: 27.01.2018)

24. Weldon D. How much does a data breach cost? Here's where the money goes. 2016. Режим доступа: https://www.csoonline.com/article/3110756/data-breach/a-deeper-look-at-business-impact-of-a-cyberattack.html?upd=1516273351459 (дата обращения: 18.01.2018)

25. Westby J. Caution: Active Response to Cyber Attacks Has High Risk. 2012. Режим доступа: https://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#77f777236d71 (дата обращения: 17.01.2018)

26. Westervelt R. Top 5 Cybercriminal Motives in 2013 Attacks. 2013. Режим доступа: http://www.crn.com/slide-shows/security/240164580/top-5-cybercriminal-motives-in-2013-attacks.htm/pgno/0/3 (дата обращения: 14.01.2018)

Норин В.Г., кандидат экономических наук, доцент, Хабаровский государственный университет экономики и права, г. Хабаровск, norin58@mail.ru

Федоренко Е.А., магистрант, Хабаровский государственный университет экономики и права, г. Хабаровск, Urf1@mail.ru

Дата поступления 29 января 2018 г.

DOI: 10.14529/iimj180214

CRIMES IN THE SPHERE OF INFORMATION TECHNOLOGIES AND THEIR IMPACT ON THE ECONOMIC SECURITY OF ENTERPRISES

NORIN V.G., FEDORENKO E.A.
Khabarovsk state university of economics and law, Khabarovsk, Russia

Abstract. The purpose of the research is to determine how IT crimes may affect economic security of enterprises. Accordingly, the subject of the study is the impact of IT crimes on the economic security of enterprises. The article considers the essence of certain types of cybercrimes, the motives and their impact on the performance of enterprises. Statistical data on cyber attacks occurred globally, across certain countries and companies were analyzed. Conclusions were drawn about the impact of IT crimes on the economic security of enterprises, recommendations were made on increasing cyber security in enterprises. It was found that cybercrimes, though indirectly, but may significantly reduce economic security of firms, especially of those in small business. The results may be applied to decision-making processes of developing cyber security strategies in enterprises.

Keywords: economic security, cybercrime, information technology, financial services, information and communications

References

1. Alvarez M. A. Magnet for Cybercrime: Financial Services Sector. 2017. Режим доступа: https://securityintelligence.com/a-magnet-for-cybercrime-financial-services-sector/ (дата обращения: 14.01.2018)

2. Bischoff P. Analysis: How data breaches affect stock market share prices. 2017. Режим доступа: https://www.comparitech.com/blog/information-security/data-breach-share-price/ (дата обращения: 18.01.2018)

3. Cisco 2017. Annual Cybersecurity Report. Режим доступа: https://engage2demand.cisco.com/en-us-annual-cybersecurity-report-2017 (дата обращения: 17.01.2018)

4. Cook S. Cybercrime stats & facts for 2016-2017. 2017. Режим доступа: https://www.comparitech.com/vpn/cybercrime-statistics-2016-2017/ (дата обращения: 18.01.2018)

5. Crowe J. WannaCry Ransomware Statistics: The Numbers Behind the Outbreak. 2017. Режим доступа: https://blog.barkly.com/wannacry-ransomware-statistics-2017 (дата обращения: 27.01.2018)

6. Dempsey M. Cyber crime: Biggest danger to intellectual property comes from within. 2013. Режим доступа: https://www.ft.com/content/856b17e8-a760-11e2-9fbe-00144feabdc0 (дата обращения: 15.01.2018)

7. Eubanks N. The True Cost Of Cybercrime For Businesses. 2017. Режим доступа: https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#5cd191c74947 (дата обращения: 15.01.2018)

8. Featherstone E. Protecting your business from cybercrime – what the experts say. 2016. Режим доступа: https://www.theguardian.com/small-business-network/2016/dec/05/how-to-protect-business-cybercrime-advice-experts (дата обращения: 27.01.2018)

9. Fildes N. TalkTalk warns of profit fall in 2017-18 under new strategy. 2017. Режим доступа: https://www.ft.com/content/7e43df6a-354e-11e7-bce4-9023f8c0fd2e (дата обращения: 18.01.2018)

10. Fruhlinger J. What is ransomware? How it works and how to remove it. 2017. Режим доступа: https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html (дата обращения: 27.01.2018)

11. Hackers are after your intellectual property, not only your money. Panda Security. 2017. Режим доступа: https://www.pandasecurity.com/mediacenter/security/hackers-intellectual-property/ (дата обращения: 14.01.2018)

12. Hern A. TalkTalk hit with record £400k fine over cyber-attack. 2016. Режим доступа: https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack (дата обращения: 18.01.2018)

13. IBM X-Force Threat Intelligence Index 2017. Режим доступа: https://www.ibm.com/security/data-breach/threat-intelligence (дата обращения: 18.01.2018)

14. Lehnis M. Total WannaCry losses pegged at $4 billion. 2017. Режим доступа: https://www.reinsurancene.ws/total-wannacry-losses-pegged-4-billion/ (дата обращения: 27.01.2018)

15. Mercer C. What is a DDoS attack? What happens during a DDoS attack? 2017. Режим доступа: https://www.techworld.com/security/how-does-ddos-attack-work-3659197/ (дата обращения: 27.01.2018)

16. Morgan S. Top 5 Industries At Risk Of Cyber-Attacks. 2016. Режим доступа: https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#32d9c174715e (дата обращения: 18.01.2018)

17. O'Brien D. Internet Security Threat Report. 2017. Режим доступа: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf (дата обращения: 27.01.2018)

18. Palmer D. Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk. 2017. Режим доступа: http://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/ (дата обращения: 27.01.2018)

19. Pierson B. Anthem to pay record $115 million to settle U.S. lawsuits over data breach. 2017. Режим доступа: https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML (дата обращения: 18.01.2018)

20. Reuters Staff. Factbox: Companies hit by global ransomware attack on June 27. 20170. Режим доступа: https://www.reuters.com/article/us-cyber-attack-factbox/factbox-companies-hit-by-global-ransomware-attack-on-june-27-idUSKBN19I29O (дата обращения: 27.01.2018)

21. Roohparvar R. 5 Industries That Top the Hit List of Cyber Criminals in 2017. Режим доступа: http://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/ (дата обращения: 27.01.2018)

22. The reputational risk of cybersecurity attacks: TalkTalk case study. Alva. 2015. Режим доступа: http://www.alva-group.com/en/the-reputational-risk-of-cyber-attacks-talktalk-case-study/ (дата обращения: 18.01.2018)

23. Vigliarolo B. Gallery: 10 major organizations affected by the WannaCry ransomware attack. 2017. Режим доступа: https://www.techrepublic.com/pictures/gallery-10-major-organizations-affected-by-the-wannacry-ransomware-attack (дата обращения: 27.01.2018)

24. Weldon D. How much does a data breach cost? Here's where the money goes. 2016. Режим доступа: https://www.csoonline.com/article/3110756/data-breach/a-deeper-look-at-business-impact-of-a-cyberattack.html?upd=1516273351459 (дата обращения: 18.01.2018)

25. Westby J. Caution: Active Response to Cyber Attacks Has High Risk. 2012. Режим доступа: https://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/#77f777236d71 (дата обращения: 17.01.2018)

26. Westervelt R. Top 5 Cybercriminal Motives in 2013 Attacks. 2013. Режим доступа: http://www.crn.com/slide-shows/security/240164580/top-5-cybercriminal-motives-in-2013-attacks.htm/pgno/0/3 (дата обращения: 14.01.2018)

Norin V.G., PhD, associate professor, Khabarovsk state university of economics and law, Khabarovsk, norin58@mail.ru

Fedorenko E.A., undergraduate, Khabarovsk state university of economics and law, Khabarovsk, Urf1@mail.ru

Received 29 January 2018

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Норин, В.Г. Преступления в сфере информационных технологий и их влияние на экономическую безопасность предприятий / В.Г. Норин, Е.А. Федоренко // *Журнал управление инвестициями и инновациями.* – 2018. – №2. – Стр. 88–99. DOI: 10.14529/iimj180214

FOR CITATION

Norin V.G., Fedorenko E.A. Crimes in the Sphere of Information Technologies and Their Impact on the Economic Security of Enterprises. *Investment and innovation management journal.* – 2018. – No. 2. – Pp. 88–99. DOI: 10.14529/iimj180214