Инструменты реализации информационной безопасности цифровой экономики России на примере ЗАО "КРОК"

Круглов Вадим Игоревич,
Институт цифровой экономики и информационных технологий
РЭУ имени Г.В. Плеханова
117997, Москва, Стремянный переулок, д.36

В данной научной работе исследуются инструменты реализации информационной безопасности цифровой экономики в России. Анализируются методы и способы нарушения конфиденциальности внутрикорпоративной информации, а также возможности защиты и противодействия. Целью работы является выявление наиболее актуальных механизмов обеспечения информационной безопасности в России на примере деятельности IT-компании ЗАО «Крок». Автором объективно оценивается текущее состояние рынка услуг информационной безопасности, государственное регулирование, инструментарий информационной защиты с учетом вектора развития цифровой экономики.

Ключевые слова: *цифровая экономика, информационная безопасность, развитие цифровых технологий России, конфиденциальность информации.*

JEL коды: *D51, G14, L86, M15.*

Tools for ensuring information security in the framework of the development of the digital economy of Russia

Kruglov Vadim Igorevich,
Institute of digital economics and information technologies,
Plekhanov Russian University of Economics
117997, Moscow, Stremyanny Lane, 36

This research paper explores the tools for implementing the information security of the digital economy in Russia. It analyzes the methods and tools of violating the confidentiality of internal corporate information, as well as the possibilities of protection and counteraction. The aim of the work is to identify the most relevant mechanisms for ensuring information security in Russia using the example of the activities of the IT company CJSC Krok. The current state of the information security services market, government regulation, information protection tools taking into account the development vector of the digital economy are also objectively assessed.

Key words: *digital economy, information security, development of digital technologies in Russia, confidentiality of information.*

Введение

Информационная безопасность является одним из ключевых направлений защиты как всего государства, так и отдельных отраслей его промышленности, в частности. С развитием частной собственности и появлением конкуренции, защита информации, коммерческой тайны, технологий и изобретений стала особым направлением деятельности предприятий [8, 9].

В СССР информационная безопасность реализовывалась преимущественно на уровне государства, с целью защиты интеллектуальной собственности страны. Первые серьезные изменения последовали после 1991 года, с преобразованием плановой экономики в рыночную. Возникшая частная собственность была слабо защищена, так как государственный аппарат более не мог обеспечивать коллективную информационную безопасность, а слаборазвитая нормативно-правовая система и неконтролируемое насыщение рынка современными технологиями не обеспечивали должной защиты юридических лиц.

Тем не менее, вопрос информационной безопасности с каждым годом актуализировался и часть данных функций взяли на себя коммерческие структуры, разрабатывающие ряд технологий, обеспечивающих должную протекцию внутреннего документооборота и прочих видов передачи внутрикорпоративной информации [2].

Основная часть

В 21 веке развитие телекоммуникационных и IT-технологий продвинуло систему функционирования предприятий на качественно новый уровень. Стала развиваться среда цифровой экономики и индустрии 4.0. Согласно всероссийскому энциклопедическому словарю, термин цифровая экономика, введенный в 1995 г., обозначает экономическую деятельность, базирующуюся на

электронно-цифровых технологиях, т.е. обеспечение работы предприятия возможно только в рамках цифровой среды [6].

Термин индустрия 4.0 появился уже в 21 веке и является характеристикой технологического развития предприятий. Данный термин предполагает не только использование цифровых технологий, но и выводит их возможности на качественно новый уровень. Синтез двух понятий определяет вектор развития современных предприятий – рациональное использование наиболее продвинутых технологий с целью обеспечения функционирования всех систем компании [5].

Так как данное функционирование происходит в информационной среде, с каждым внедрением нового технологического решения возникает угроза утечки информации, которая проходит через данную систему, а также заражения вредоносным ПО.

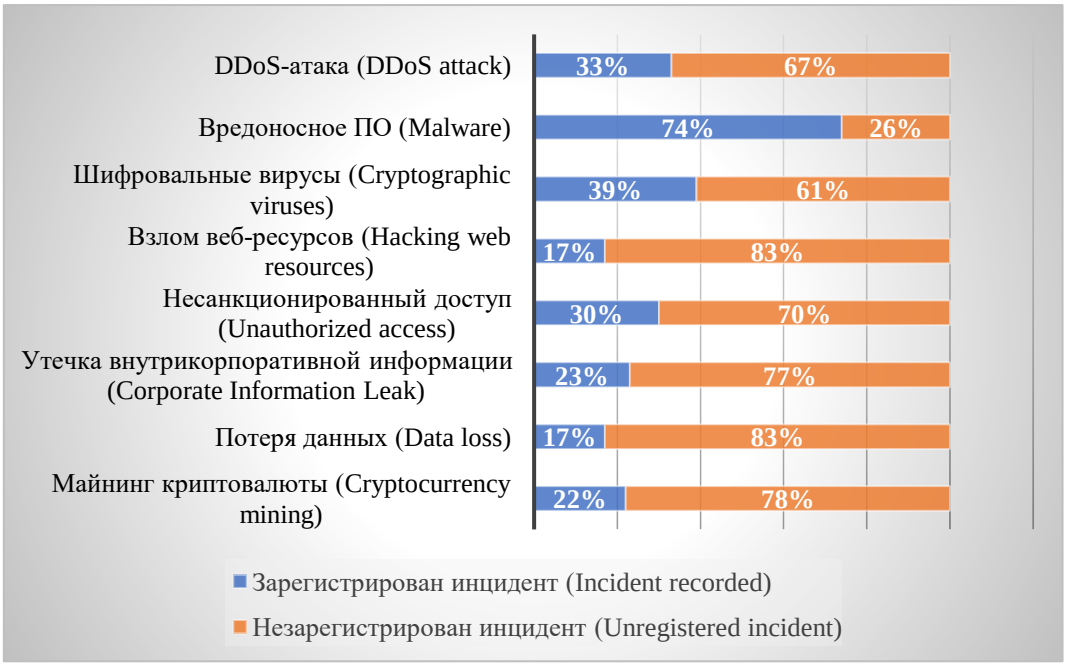

Рис. 1. Обращение к услугам компаний сферы информационной безопасности в России в 2018 г., до и после зафиксированного инцидента.
Fig. 1. The call to the services of information security companies in Russia in 2018, before and after the recorded incident.

Источник: составлено по данным [3].

Source: Compiled from [3].

На рис. 1. можно наблюдать виды зарегистрированных инцидентов по российским компаниям за 2018 год. Наибольшее количество компаний обращается к услугам предприятий информационной безопасности при заражении техники вредоносным программным обеспечением (далее – ПО). Также в 2018 г. отмечено повышенное количество инцидентов майнинга криптовалюты и шифрование данных пользователей внутрикорпоративных сетей [2].

Для продвижения технологий информационной безопасности, развития информационной грамотности и исполнения ряда государственных задач в сфере развития цифровой экономики, 15 мая 2018 г. в РФ было основано Министерство цифрового развития, связи и массовых коммуникаций. Согласно отчетности Министерства за 2018 г., было зарегистрировано более 150 млн. обращений от юридических лиц и индивидуальных предпринимательств об инцидентах, связанных с нарушением информационной безопасности [4].

Согласно исследованиям компании «Anti-Malware», только 47% случаев нарушения защиты возможно предотвратить внутренними силами организации, остальная часть вынуждена обращаться к сторонним компаниям. Также согласно данному исследованию, существует более 3000 актуальных видов нарушения информационной безопасности предприятий России на данный момент.

Следует отметить, что и технологическая база инструментов обеспечения информационной безопасности современных компаний России обширна, поэтому для наиболее объективного анализа можно рассмотреть пример компании, функционирующей на данном рынке продолжительное время. Одной из таких компаний является ЗАО «Крок» [1].

История компании берет отсчет еще до появления цифровой экономики, в 1992 году. В начале своей деятельности компания специализируется на продвижении информационных технологий: поставки технического оборудования, периферийное оборудования, сетевые коммуникационные технологии и услуги поддержки и обновления ПО.

С массовым распространением технологий появляется все больше способов нарушить информационную безопасность фирмы, поэтому множество IT-компаний внедряют услуги по защите конфиденциальности внутрикорпоративного документооборота, с применением ПО и специализированного технического оборудования.

В 21 веке набор предоставляемых услуг заметно расширился, поэтому на базе анализируемой компании можно обозначить актуальный спрос на ряд технологических решений и услуг, наиболее востребованных на рынке в текущий момент времени. «Крок» предоставляет 35 видов технологических решений и услуг в рамках развития цифровой индустрии, среди которых 17 видов относятся к обеспечению информационной безопасности [3].

Ключевыми для корпоративной защиты можно выделить: межсетевые экраны, антивирусную защиту, системы мониторинга доступа и запросов, контроль доступа и защиту внутренней информации.

Межсетевые экраны обеспечивают дифференциацию сетей и доступа к ним, что предотвращает попытки незаконного доступа к другим персональным аккаунтам. Межсетевые экраны способствуют построению иерархичной модели управления и доступа к информации даже в рамках одного устройства. Помимо персональных компьютеров, данные системы можно использовать для доступа к оборудованию или системам управления предприятия. Так, к примеру, рабочие могут лишь приводить оборудование в действие, а операторы и инженеры получать доступ к архивам выполненных работ и удаленному доступу к устройству, в том числе возможность проводить работы с программным обеспечением.

Данный вид защиты может реализовываться как программным обеспечением, так и аппаратным. Также возможна комбинация данных методов в более сложную, но структурированную сеть доступа к данным. Недостатком данной сети можно выделить возможность получения удаленного доступа более высоким по иерархии доступа аккаунтом, а также получение

идентификационных данных других аккаунтов с целью использования полномочий и возможностей без ведома данного пользователя.

Следующим распространенным и эффективным методом протекции данных является антивирусная защита. Компания «Крок» использует в своем ассортименте продукцию сторонних сервисов антивирусной защиты, однако обладает возможностью более «тонкой» детальной настройки спецификаций системы под любого потребителя. Основными типами специализированных настроек является почтовые шлюзы, прокси-сервера, ограничение доступа на ряд сайтов, индивидуальные возможности каждого сотрудника компании и др.

Также можно выделить системы обнаружения атак (далее – СОА). Данная система функционируют по превентивным методам, т.е. предотвращает не саму атаку, а возможности ее осуществления и анализирует изъяны системы. Современные СОА обладают набором интеллектуальной логики, которая может обучаться на сторонних примерах и проводить ряд защитных мер еще до того, как данный изъян будет замечен злоумышленником.

Немаловажным фактором защиты является внутренняя безопасность. Для обеспечения контроля всех внутренних пользователей может формироваться отдельный дата-центр с записями всех зарегистрированных попыток доступа к данным, создание общей консоли управления. Также внутренняя передача данных может быть перехвачена сторонним устройством, подключаемым к корпоративной сети. Для минимизации рисков передача информации между устройствами шифруется, также возможно применение систем блокчейн, которые обеспечивают все персональные устройства информацией обо всех передачах данных.

Однако, к вышеприведенным мерам безопасности прибегают не все компании, функционирующие на рынке. Многие из юридических лиц ограничиваются антивирусными мерами защиты, остальные инструменты внедряются в систему после инцидента (рис. 1).

Так, по данным компании, в 2018 г. было зафиксировано практически на 1/3 заказов больше, чем за аналогичный прошлый период. Также в совокупной

выручке увеличились и доли направлений, объединенных в портфель digital-услуг: разработки в области виртуальной и дополненной реальности, проекты по робототехнике, облачные сервисы, аудиовизуальные комплексы и промышленные решения Индустрии 4.0. Суммарно эти динамично растущие направления принесли компании 2592,4 млн руб., составив долю 8,5% в общей структуре выручки. Также меняются и подходы к осуществлению механизмов безопасности внутренних процессов. (Рис. 2.)

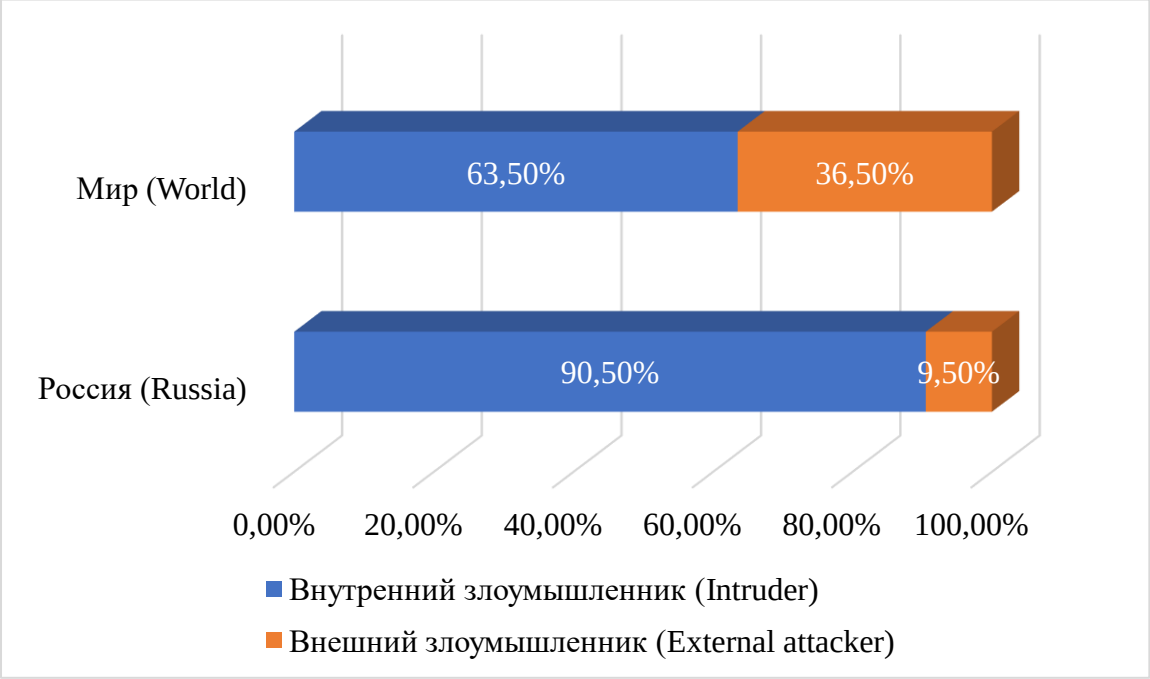

Рис. 2. Распределение утечек информации по вектору воздействия в 2018 г.

Fig. 2. Distribution of information leaks by impact vector in 2018.

Источник: составлено автором по данным [7].

Source: Compiled from [7].

Согласно информации на рис. 2., 90,5% инцидентов нарушения безопасности происходит из-за действий сотрудников, в то время как в среднем по миру данный показатель не превышает 63,5%. Соответственно политика проведения мер информационной защиты в российских компаниях должна быть направлена, в первую очередь, на внутренние службы и повышение информационной грамотности сотрудников.

Заключение

В заключение работы следует выделить, что более 86% компаний России подвергается угрозе нарушения информационной безопасности не менее 1 раза в год. Наибольшее количество из них сталкивается с попыткой/частичным/полным заражением программного обеспечения вредоносными объектами. Более 15% компаний, имеющих собственные дата-центры, подвергались атакам с кражей или утерей данных. А 30% из зарегистрированных случаев фиксировалось более чем через 1 календарный месяц и позже. Не менее редки и случаи заражения производственных мощностей, что может поставить под угрозу не только информационную безопасность, но и безопасность сотрудников организации, взаимодействующих с зараженным оборудованием [3].

Эффективными инструментами защиты внутрикорпоративной информации выделяются:

- установка защитного ПО;
- повышение компьютерной грамотности сотрудников;
- мониторинг персонального доступа к корпоративной информации;
- физическое ограничение доступа к дата-банкам и серверам;
- использование искусственного интеллекта для мониторинга потенциальных угроз;
- проверка коммуникаций на внешнее отслеживание информации;
- разработка систем закрытого типа (в т.ч. без возможности выхода в интернет, с технологией защиты Блокчейн) и др.

В век цифровизации количество «умных» устройств будет ежегодно расти, каждое из них может быть подвергнуться заражению, что напрямую или косвенно пагубно повлияет на всю систему организации. Поэтому необходимо заранее обеспечить внутренние технологические устройства должными мерами защиты.

Список литературы

1. ЗАО «Крок» [Электронный ресурс]. URL: https://www.croc.ru/ (дата обращения: 03.11.2019).
2. Информационная безопасность в России [Электронный ресурс]. URL: https://www.infowatch.ru/company/presscenter/news/15706 (дата обращения: 14.11.2019).
3. Информационная безопасность российских компаний [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/ (дата обращения: 07.11.2019).
4. Министерство цифрового развития, связи и массовых коммуникаций России [Электронный ресурс]. URL: https://digital.gov.ru/ru/activity/(дата обращения: 08.11.2019).
5. Терминологический словарь. Понятие Индустрия 4.0 [Электронный ресурс]. URL: https://bspu.ru/files/39366 (дата обращения: 03.11.2019).
6. Терминологический словарь. Понятие цифровая экономика [Электронный ресурс]. URL: https://dic.academic.ru/ (дата обращения: 03.11.2019).
7. Федеральная Служба Государственной Статистики России [Электронный ресурс]. URL: https://www.gks.ru/ (дата обращения: 14.11.2019).
8. Черняев М.В., Нежникова Е.В., Папельнюк О.В., Кореневская А.В. Экономика качества: Учебник для бакалавров. – М., 2018.
9. Черняев М.В. Инновационные стратегии и их реализация в организации // Теория и практика развития предпринимательства: современные концепции, цифровые технологии и эффективная система: Материалы VI Международного научного конгресса, 2018. - С. 88-94.

References

1. ZAO «Krok» [CJSC Krok]. Available at: https://www.croc.ru/ (accessed 3 November 2019).
2. Informacionnaja bezopasnost' v Rossii [Information security in Russia]. Available at: https://www.infowatch.ru/company/presscenter/news/15706 (accessed 14 November 2019).
3. Informacionnaja bezopasnost' rossijskih kompanij [Information security of Russian companies]. Available at: https://www.anti-malware.ru/analytics/ (accessed 7 November 2019).
4. Ministerstvo cifrovogo razvitija, svjazi i massovyh kommunikacij Rossii [The Ministry of Digital Development, Telecommunications and Mass Media of Russia]. Available at: https://digital.gov.ru/ru/activity/(accessed 8 November 2019).
5. Terminologicheskij slovar'. Ponjatie Industrija 4.0 [The terminological dictionary. Concept Industry 4.0]. Available at: https://bspu.ru/files/39366 (accessed 3 November 2019).
6. Terminologicheskij slovar'. Ponjatie cifrovaja jekonomika [Terminological dictionary. The concept of digital economy]. Available at: https://dic.academic.ru/ (accessed 3 November 2019).
7. Federal'naja Sluzhba Gosudarstvennoj Statistiki Rossii [Federal State Statistics Service of Russia]. Available at: https://www.gks.ru/ (accessed 14 November 2019).
8. Chernyaev M., Nezhnikova E., Papelnuk O., Korenevskaya A. Economika kachestva: Textbook for Bachelors [Quality Economics]. Moscow, 2018.
9. Chernjaev M. Innovacionnye strategii i ih realizacija v organizacii // Teoriya i praktika razvitiya predprinimatel'stva: sovremennye koncepcii, cifrovye tehnologii i effektivnaya sistema: Materialy VI Mezhdunarodnogo nauchnogo kongressa [Theory and practice of entrepreneurship development: modern concepts, digital technologies and an effective system], 2018, pp. 88-94.