СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В РОССИИ

Кан Ен Дя, *старший преподаватель*
К.А. Стародуб, *студент*
Сахалинский государственный университет
(Россия, г. Южно-Сахалинск)

Аннотация. *Информатизация общества и экономики поднимает вопрос сохранности данных и необходимости поиска механизмов и технологий защиты информации, как от внешних, так и от внутренних угроз. Поэтому в наши дни предпринимателям крайне необходимо иметь представление об имеющихся решениях в вопросах сохранения конфиденциальных данных и степени их развития, чтобы выбрать поддерживаемую компаниями-разработчиками систему, которая будет отвечать постоянно развивающимся типам угроз. В данной статье представлена оценка места и роли информационных технологий по защите конфиденциальных данных в Российской Федерации. Приведены результаты анализа структуры утечек информации. Также приведены фактические данные развития российского рынка DLP систем. Рассмотрены преимущества и недостатки DLP систем и технологии Blockchain. В результате исследования были выявлены проблемы внедрения, характерные не только для рассматриваемых технологий, но и для всего сегмента рынка в целом.*

Ключевые слова: *Блокчейн, DLP, информационные технологии, экономика, безопасность данных.*

Активное развитие информационных технологий, в совокупности с современными достижениями в области высоких технологий, компьютеров оказывают существенное влияние на все сферы человеческой деятельности. Процесс цифровизации общества связан с ростом информационных угроз, которые непосредственно могут нанести серьезный вред организации. Поэтому предпринимателям крайне необходимо иметь представление о популярных и перспективных технологиях защиты информации и развитии рынка в целом, чтобы выбрать решение, которое будет поддерживаться и развиваться за счет конкуренции присутствующих на рынке компаний.

Под информационными технологиями понимаются процессы, а также методы поиска, сбора, хранения, обработки, предоставления и распространения информации, включая способы осуществления таких процессов и методов. [1]

Большинство разрабатываемых программ направленны на решение существующих экономических и социальных проблем, тем самым оказывая значительное влияние на развитие этих сфер деятельности человека.

Развитие информационных систем по сбору, обработке и хранению персональных данных пользователей позволило, с одной стороны, значительно упростить идентификацию пользователей, получить возможность более точечно доносить информацию до целевой аудитории с помощью таргетированной рекламы, получать информацию о потенциальных заемщиках и т.д., но в то же время, с появлением новых информационных технологий растут и уязвимости, результатом которых может являться утечка информации.

Под утечкой информации понимают нелегитимный переход конфиденциальной информации, включая персональные данные и объекты коммерческой или государственной тайны в открыты доступ или к конкурентам. В качестве последствий от утечек для организации могут выступать штрафные санкции, потеря своей деловой репутации, перехода клиентов к конкурентам и судебных исков.

Кроме этого, утечки в любом случае наносят серьезный ущерб. Так, случившаяся осенью 2015 года утечка с сайта "Кинопоиск" привела к публикации планов о развитии компании, структуре сервиса и другой конфиденциальной информации, что повлияло на конкурентные позиции компании на рынке и привело к многомиллионным потерям [2].

Другой пример, скандал из-за утечки персональных данных 50 млн пользователей, что привело не только к уходу клиентов, но и к падению акций компании на 6.26 процента, что отразилось на рыночной капитализации компании, которая упала примерно на 23,8 миллиарда долларов [3].

Согласно исследованию аналитического центра InfoWatch: по итогам 2016 года эксперты насчитали в России около 213 случаев утечек информации, что в сто раз больше, чем в 2015 году, в результате которых было скомпрометировано 128 млн записей конфиденциальных данных, в том числе относящихся к банковским картам и счетам.

Число утечек постоянно растет, и по их количеству Россия уже несколько лет подряд уверенно занимает вторую строчку в рейтинге. Утечки информации можно разделить по векторам атаки, их соотношение изображено на Рисунке 1.

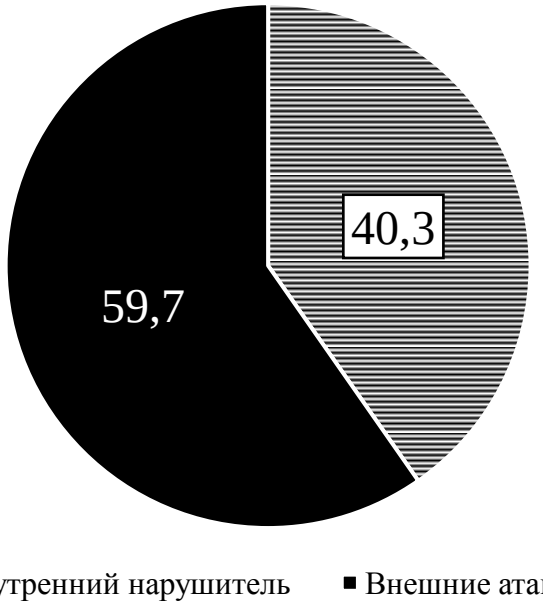

Рис. 1. Распределение утечек по векторам атаки в 2016 году

Таким образом, исходя из Рисунка 1, можно сделать вывод о том, что в 2016 году, несмотря на преобладание внешних атак, внутренние занимают значительную долю.

Исходя из данных Рисунка 2, можно сделать вывод о том, что около двух третей утечек в России составляют так называемые неквалифицированные утечки. Под неквалифицированными утечками понимают те, которые не связанны с мошенничеством или злоупотреблением. Примером может являться невнимательность сотрудников или же халатное отношение к конфиденциальной информации.

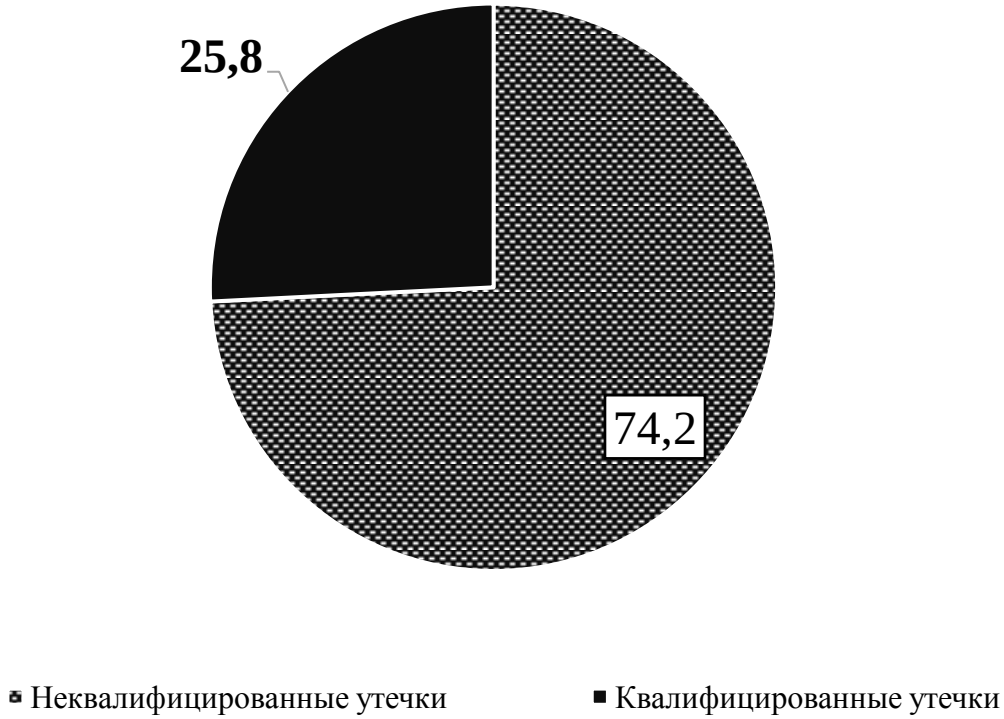

Рис. 2. Распределение утечек по типу инцидентов в 2016 г.

Потери от утечек в среднем составили $820 тыс. [2].

Для решения проблем неквалифицированных издержек была разработана система DLP – Data Leak prevention. Она включает в себя совокупность организационных, консультационных мероприятий и информационно- технических мер защиты и расследования утечек. Данная технология развертывается в три этапа:

На первом, выбор объектов защиты, подготовка базы классификации информации для дальнейшего полуавтоматического отслеживания конфиденциальных данных в компании. На этом этапе важно подготовить такую классификацию, чтобы у системы в процессе работы не возникало ни сомнений, ни ложных срабатываний. На втором, происходит развертывание софта и программного обеспечения. На третьем, происходит расследование утечек информации. При соблюдении в компании ряда процедур данные системы могут использоваться в качестве доказательства в суде (в случае преследования нарушителя за несоблюдение режима коммерческой тайны, например). [2]. Также существует деление по типам разворачиваемых систем:

Border DLP – определение секретности документа по имени файла либо по сигнатуре. Когда документ пытается покинуть пределы организации каким-либо путем – по сети, через USB-диск (флешку), по почте и так далее, определяется его сигнатура и сравнивается с базой защищаемых документов. Если сигнатура в базе найдена, операция блокируется, а ИТ-безопасность уведомляется. Положительной стороной является доступность и простота системы. Минусами – конфликтность даже с однотипными системами и при изменении документа, меняется сигнатура, а значит система не сработает.

Agent DLP – На каждый компьютер устанавливается специальная программа, отслеживающая любые попытки работы с документом. При каждой такой попытке вычисляется сигнатура документа и сравнивается с базой. Если документ защищен, определяется пользователь, пытающийся с ним работать. Если права есть, операция выполняется,

если нет, блокируется и уведомляется служба безопасности. Плюсы – невозможно работать с документом без права доступа. Минусы – снижение производительности компьютера и сети, при слабых мощностях ПК могут происходить задержки между запуском и выполнением операции, а также высокая стоимость установки и необходимость установки на каждый компьютер.

DRM – встраивание механизмов шифрования и дешифрации в стандартные программы для редактирования документов. Клиентская часть при попытке открытия документа обращается с информацией о документе и открывающем его пользователе к серверу ключей, который хранит сведения о правах различных пользователей на доступ к различным документам. Если право на доступ есть, отправляется ключ, с помощью которого клиент незаметно для пользователя расшифровывает документ и дает возможность выполнить разрешенные операции. Из положительных сторон – высокая степень защищенности, меньшая нагрузка на компьютер нежели ADLP. Минусы заключаются в том, что для данной системы требуется программное обеспечение одной версии и от одного производителя.

Лидирующие шесть позиций на рынке по итогам 2016 года занимают российские производители, чья совокупная доля рынка составляет уже более 91%. В тройку ведущих компаний входят Infowatch (30.7%); SolarSecurity (0.17%); Инфосистемы джет (14,9%). В целом объем рынка составляет 4,73 млрд. [4]

Среди российских компаний разворачивается жесткая конкуренция в сегменте крупного бизнеса и госсекторе, что способствует постепенному снижению цены, росту качества и функциональности отечественных DLP-систем. Значительное влияние на DLP оказывает высокий уровень неопределенности в российской экономике. При сильном ухудшении экономической ситуации, бизнес ограничивает экономические вложения, в совокупности с зависимостью от иностранного оборудования, вспомогательного софта, баз данных и сервисов, это ставит российский рынок DLP в крайне затруднительное положение.

Другой важной технологией, которая может быть направлена на решение проблем в области безопасности, является блокчейн. Блокчейн – постоянно растущая цепочка взаимосвязанных, криптографически защищенных блоков, а также процесс передачи данных в одноранговой децентрализованной сети с применением шифрования. Централизованная сеть предполагает наличие посредника. Эти посредники занимаются построением и обслуживанием всей рыночной деятельности, от определения подлинности и установления личности людей до удаления, создания документов и делопроизводства. [5]

Но есть ряд проблем, связанных с ними: они уязвимы для хакерских атак, тормозят экономические процессы, берут комиссию за услуги, занимаются сбором личных данных, коммерциализируя их, тем самым нанося ущерб личному пространству людей.

В децентрализованных или пиринговых сетях роль посредников либо сведена к минимуму, либо исключена вовсе, что является одним из ключевых преимуществ для криптовалюты – проекта Сатоши Накамото, где доверие позиционировалось не на авторитете посредников, а на доверительном протоколе.

В децентрализованных или пиринговых сетях роль посредников либо сведена к минимуму, либо в случае исключена вовсе, что является одним из ключевых преимуществ для криптовалюты – проекта Сатоши Накамото, где доверие позиционировалось не на авторитете посредников, а на доверительном протоколе. На Рисунке 3 изображен процесс записи нового блока на примере криптовалютной транзакции.

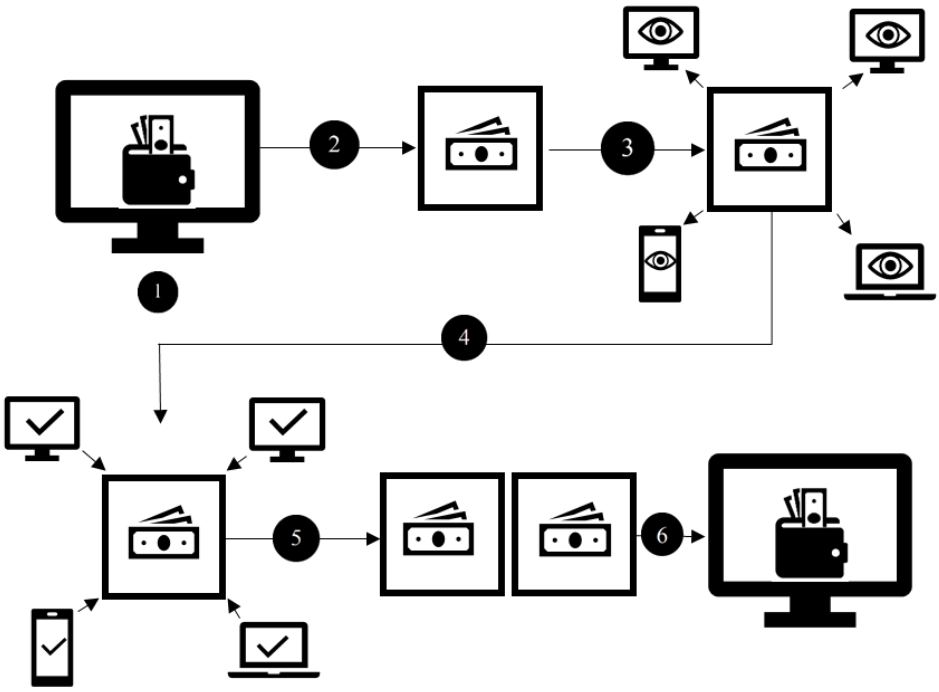

Рис. 3. Принцип работы технологии «блокчейн»

Процесс создания нового блока в блокчейне разбит на несколько этапов:

1. Формирование исходных данных для транзакции на компьютере–отправителе;

2. Транзакции передаются в сеть, где затем собираются в блок, при этом каждый блок имеет номер и хеш-сумму предыдущего блока. Хэш-сумма – это уникальный идентификатор, в данном случае блока, высчитываемый путем ряда математических преобразований. Фиксируя информацию в создаваемом блоке, её крайне сложно становится изменить.

3. Блоки рассылаются всем участникам для проверки;

4. Затем, при отсутствии ошибок, каждый участник сети записывает блок в свой экземпляр базы данных;

5. Блок добавляется к цепочке, которая содержит информацию обо всех предыдущих транзакциях;

6. Непосредственно перевод денег.

Таким образом, можно выделить следующие ключевые особенности блокчейн [6]:

- Отсутствие финансовых посредников;
- Снижение транзакционных издержек;
- Открытость внесенной информации;
- Крайняя сложность изменения единожды внесенных в систему данных.

К негативным сторонам можно отнести:

- Избыточное хранение данных – вся информация дублируется на большом числе носителей;
- Необходимость обеспечения высокой пропускной способности;
- Отсутствие стандартов и законодательной базы;

Несмотря на недостатки все вышеперечисленное создает обширную область использования блокчейна. К примеру, фиксация прав собственности. При поддержке государства созданную систему невозможно будет взломать. Это создаёт условия благосостояния для миллиардов людей. В России блокчейн находится на начальной стадии развития, только начала формироваться законодательная база и стандарты. По данным ЕГРЮЛ на 10 января 2018 года в России зарегистрировано 50 юридических лиц, так или иначе связывающих свою деятельность с технологией блокчейн. Объем рынка блокчейн в России в 2017 году оценивается в 1 млрд долларов. Основными оригинальными сферами

деятельности в России блокчейн-компании указывают обработку данных, использование вычислительной техники, разработку компьютерного программного обеспечения, правовую деятельность, консультирование в области компьютерных технологий. Однако, есть и компании, деятельность которых также связана с оптовой непрофильной торговлей и производством. Также по прогнозам, в 2018 году можно ожидать запуска и успешной реализации еще минимум 10 проектов в сфере блокчейна, связанных с государственным сектором [6].

В целом, для технологий перечисленных выше можно выделить следующие общие проблемы:

- В РФ наблюдается недостаток кадров непосредственно связанных с ИТ технологиями в том числе и в области защиты информации, особенно связанных с технологией блокчейн [6];
- Также наблюдается серьезная зависимость от иностранных электронных комплектующих – в России, практически отсутствуют высокопроизводительные персональные и коммерческие решения, а также вспомогательный софт;
- Также данные технологии зависят от волатильности рынка – при нестабильной экономической ситуации, многие компании предпочитают направлять имеющийся капитал для более насущных проблем;

В долгосрочной перспективе эти проблемы можно решить следующим образом:

- Создать благоприятную налоговую политику в отношении компаний, занимающихся производством электронных компонентов;
- Создать базу для подготовки и переподготовки кадров осуществлять на основе российских ИТ- компаний;

Таким образом, рынок по защите информации в России находится в начальной стадии развития, и несмотря на медленные темпы, а также наличия таких сдерживающих факторов как нехватка кадров, зависимость от иностранных компонентов и ПО и нестабильных экономических условий, постепенно развивается. Российским компаниям удалось вытеснить иностранные и занять главенствующее положение на рынке. Обилие компаний и путей применения данных технологий создает конкурентоспособную среду, в которой данные технологии будут поддерживаться и развиваться, постепенно совершенствуясь в вопросах защиты информации организаций.

Библиографический список

1. *«Об информации*, информационных технологиях и о защите информации» [Электронный ресурс]: Федеральный закон № 149-ФЗ от 27 июля 2006 года. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 19.04.2018).

2. *Технологии предотвращения* утечек конфиденциальной информации из информационной системы вовне [Электронный ресурс] // Консультационно- информационный портал Tadviser. URL: http://www.tadviser.ru/ ИБ_-_Предотвращения_утечек_информации (дата обращения: 20.04.2018).

3. *Утечка данных* обошлась Facebook в миллиарды долларов [Электронный ресурс] // Lenta.Ru (Лента.Ру): интернет-издание. URL: https://lenta.ru/news/2018/03/19/facebook_down/ (дата обращения: 20.04.2018).

4. *Рынок DLP*- решений (Россия) [Электронный ресурс] // Консультационно- информационный портал Tadviser. URL: http://www.tadviser.ru/index.php (дата обращения: 21.04.2018).

5. *Bitcoin:* A Peer-to-Peer Electronic Cash System [Электронный ресурс] // Сайт сообщества системы Bitcoin.URL: https://bitcoin.org (дата обращения: 20.04.2018).

6. *Дон Тапскотт.* Как блокчейн трансформирует бизнес и денежную систему [Электронный ресурс] // Официальный сайт конференций TED URL: https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business (дата обращения: 21.04.2018).

MODERN INFORMATION TECHNOLOGIES OF CONFIDENTIAL DATA PROTECTION IN RUSSIA

Kahn Yen Dya, *senior lecturer*
K.A. Starodub, *student*
Sakhalin state university
(Russia, Yuzhno-Sakhalinsk)

Abstract. *Informatization of society and economy raises the issue of data security and the need to search for mechanisms and technologies that allow information protecting both from external and internal threats. Therefore, it is extremely necessary to have an idea of the available solutions in terms of preserving confidential data and the level of their development for select a system supported by the developer companies that will meet constantly evolving types of threats nowadays. This article analyzes and assesses the place and role of information technology for protecting sensitive data in the Russian Federation. There are the results of the analysis of data leak cases' structure. In addition, the actual data on the development of the Russian market of DLP systems are given. Advantages and disadvantages of DLP systems and Blockchain technology are considered. As a result, the study identified implementation problems that are typical not only for presented technologies, but also for the entire market segment.*

Keywords*: Blockchain, DLP, informational technologies, economics, data protection.*