Содержание

Введение

В настоящее время всё большее распространение получают различные мобильные устройства и, как следствие, операционные системы, установленные на данные устройства. В связи с этим востребован перенос каких-либо программ на эти устройства и, как следствие, экономически выгодно разрабатывать приложения на мобильные платформы. Но также, учитывая современные тенденции рынка, не менее востребованной является разработка инновационных приложений сразу на мобильной платформе.

Благодаря применению мобильных приложений во много раз упрощается проблема доступа пользователя к определённым информационным ресурсам и, также, могут быть доступны ресурсы, которые не могут быть доступны через обыкновенное Web-приложение.

Одним из главных факторов, оказывающих влияние на ведение преуспевающего бизнеса, является обладание ценной информацией и особенно это становится заметно с развитием информационных технологий. Одновременно с этим все более актуальной становится защиты информации и средства, помогающие в этом. Исключением не стала и такая активно развивающаяся отрасль как мобильные приложения и мобильные устройства. В связи с этим разработка средств защиты на данный тип устройств приобретает всё большую актуальность.

Таким образом:

Проблема, которой посвящена работа, является информационная безопасность приложения.

Цель и задача - разработка инновационных методов улучшения информационной безопасности данных приложений.

Объект и предмет исследования - текущие приложения

Степень разработанности - данная тема является широко разрабатываемой в данное время.

Место и значение в науке и практике – данная тема является важной как с точки зрения практики, так и научных знаний.

1.Глава актуальность работы

1.1. Актуальность разработки мобильных приложений.

Мобильное приложение — программное обеспечение, предназначенное для работы на смартфонах, планшетах и других мобильных устройствах.

Изначально мобильное приложение применялось для более быстрой проверки электронной почты, но высокий интерес к ним привёл к тому, что их применение стало расширяться и в другие области, к примеру, такие как пользование интернетом, общение, игры для мобильных устройств, просмотр видео и GPS.

На сегодняшней день мобильные приложения на рынке хорошо распространены и продолжают распространятся.

Данный термин приобрёл большую популярность в 2007 году и в 2010 году Американское диалектическое общество внесло его в список «Слова года».

Мобильное приложение — это программное обеспечение, специально разработанное под конкретную мобильную платформу (iOS, Android, Windows Phone и т. д.). Предназначено для использования на смартфонах, фаблетах, планшетах, умных часах и других мобильных устройствах.

Мобильные приложения пишутся на языках программирования высокого уровня, а затем компилируются в машинный код операционной системы для получения максимальной производительности.

Как и в каждой сфере разработка приложений имеет свои характерные особенности: в отличие от персональных компьютеров мобильные устройства оснащены батареей и, как правило, оснащены менее производительными процессорами и прочими комплектующими нежели персональные компьютеры. Помимо этого, современные мобильные устройства комплектуются и вспомогательными устройствами такими как: гироскопы,

акселерометры и фотокамеры, которые позволяют дать дополнительный функционал приложения.

1.2.Рост рынка мобильных приложений

В большинстве своём устройства в продажу поступают уже с предустановленными приложениями, а дополнительные пользователь может скачать по своему усмотрению, как на платных, так и на бесплатных ресурсах таких как: Apple AppStore, Google Play, Windows Phone Store и прочие. Первооткрывателями в отрасли продажи мобильных приложений стали такие магазины как: Apple AppStore и Android Market, который в последствии сменил название на Google Play, были созданы в 2008 году. Годом позже Американское диалектическое общество признало словом года термин «приложение».

По завершению 2015 года в базе данных двух крупнейших маркетов находилось около 3 миллионов приложений. А количество загрузок, произведённых за одни год, превышало 300 миллионов скачиваний.

1.2.1.Рост рынка в 2018 на 20% до $76 млрд

В 2018 году в Apple App Store и Google Play было зафиксировано 113 млрд загрузок приложений и игр на сумму $76 млрд, что соответственно на 10% и 20% больше показателей годичной давности. Такие данные 20 декабря привели в аналитической компании App Annie.

В данные статистические расчёты не были взяты данные скачиваний в китайских сторонних маркетов. Если учитывать информацию с данных порталов, то итоговая картина может существенно измениться.

По мнению экспертов, увеличение рынка приложений для мобильных устройств напрямую связано с тем, что расходы потребителей на игры увеличиваются, а они в свою очередь являются одним из самых прибыльных источников получения доходов для разработчиков.

В 2018 году наибольшую популярность приобрели такие игры как Fortnite, PUBG и Roblox, разработчики которых в ходе создания учитывали постоянно растущую производительность смартфонов и кроссплатформенный подход. По мнению аналитиков, в 2019 году число проектов, которые получат большую популярность, должно увеличиться. Связано это с тем, что производительность современных мобильных устройств по своим характеристикам всё больше приближается к уровню консолей, что открывает большие перспективы для данной отрасли[1].

Также, одним из драйверов рынка мобильных приложений стали подписки, эта бизнес-модель предусматривает регулярную оплату определённых товаров, услуг, функций или доступ к контенту. По мнению экспертов именно благодаря данной бизнес-модели будет всё больше увеличиваться рост потребительских расходов на рынке приложений в 2019 году. Что, в сою очередь, приведёт к тому, что продажи программного обеспечения для мобильных устройств подскочат до отметки в 122 миллиарда долларов США.

Из статистических данных можно сделать вывод, что за 2018 год пользователи в среднем увеличили время провождения за приложением до 110% процентов по сравнению с прошлым годом и составляет около 3 часов в день. Также это на 20% больше чем в 2016 году.

1.2.2.Прогноз App Annie на 2022 год

В 2022 году оборот рынка мобильных приложений достигнет $6,3 трлн. Такие цифры приводит компания App Annie, занимающаяся статистикой этого рынка. В 2016 году этот показатель достиг $1,3 трлн. Драйвером роста станет рост объема покупок товаров и услуг в гипермаркетах, сервисах такси и туристических приложениях, к которым пользователи «привязывают» карты[2].

Хотя, судя по статистическим данным, количество скачиваний на человека не увеличилось. App Annie предполагают, что число пользователей должно быть удвоено до отметки в 6,3 миллиарда человек в ближайшие 5 лет, а время, которые пользователи будут проводить в приложениях, увечится белее, чем в двое. Что, в свою очередь, приведёт к увеличению оборота денежных средств на рынке мобильных приложений, включая такие отрасли как: встроенные покупки, издержки на рекламу и одну из важнейших категорий - электронную коммерцию. Траты в приложениях вырастут от $379 до $1 008 на человека к 2021 году[3].

Огромное влияние на статистические показатели мобильной коммерции, оцененные App Annie, имеют покупки через таких гигантов как Amazon и Alibaba, а также оплата сервисов такси Uber и путешествий, забронированных через приложения, и содержащих вашу кредитную информацию. Предполагаемые цифры также основаны на том, что люди переключатся с покупок в физических магазинах на покупки через приложения. Всё это приведет к тому, что мобильная коммерция (то есть оплаты товаров и услуг в приложениях) будут занимать до 95% всего объема платежей к 2021 году.

Потребители, покупающие сами приложения и совершающие встроенные покупки, вместе с доходом с рекламы, создали 10% оборота ($134 млрд) рынка мобильных приложений в 2016 году, а в 2021 доля этих доходов сократится вдвое — до 5% ($340 млрд).

Мобильная коммерция не только станет самым большой частью рынка приложений, но и покажет самый высокий ежегодный темп роста в 39%. Оплаты в маркетах приложений и реклама в них будут расти с темпами 18% и 23% соответственно.

1.3.Подтверждение проблемы

Одним из главных факторов, оказывающих влияние на ведение преуспевающего бизнеса, является обладание ценной информацией и

особенно это становится заметно с развитием информационных технологий. Одновременно с этим все более актуальной становится защиты информации, которая не должна быть публичной, а также выбор средств, обеспечивающих безопасность. Исключением не стала и такая активно развивающаяся отрасль как мобильные приложения и мобильные устройства. В связи с этим разработка средств защиты на данный тип устройств приобретает всё большую актуальность[4].

1.3.1.Типы угроз безопасности

Под угрозой безопасности информации понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов.

Принято разделять угрозы на:

- умышленные
- и не преднамеренные (случайные).

Источниками случайных угроз могут выступать как ошибки в программном обеспечении, так и то, что аппаратные средства вышли из строя. Также подобный вид угроз может случаться по вине пользователей и тому подобные причины. Умышленные в отличие от случайных направленны на нанесение ущерба пользователям АИС

Умышленные угрозы условно можно поделить на пассивные и активные. Целю работы пассивных является несанкционированное использование информационных ресурсов, при этом они не оказывают влияния на функционал. В то время как активные угрозы наоборот нарушают сложившийся процесс путём целенаправленного воздействия на аппаратные, программные и информационные ресурсы[5].

1.3.2.Утечки информации

Утечки информации - неправомерное получение конфиденциальной информации (информация важная для различных компаний или государства,

персональные данные граждан), которое может быть умышленным или случайны. Каждая информация, которая хранится на компьютере, обладает своей ценой. Кража личных данных пользователя компьютера по средствам вредоносного программного кода в состоянии нанести вред пользователю. Обладая информацией о логинах и паролях, а также о карточках банка и счетах, злоумышленники могут красть деньги граждан, тайны и промышленные секреты предприятия. Утечка информации происходит в итоге бесконтрольного распространения тайн за пределы периметра, в котором они должны сохраняться. Данное проишествие может произойти из-за несоблюдения норм и правил информационной защиты и их некорректного соблюдения. Несоблюдение правил защиты и хранения данных могут повлечь за собой их хищение и распространение в местах для этого не предназначенных таких как интернет, к примеру[6].

1.3.3.Классификация видов утечки информации

Утечка информации возможна можно по разным причинам, а именно:
Умышленные утечки

1. Инсайдеры и избыточные права. Это слив информации сотрудниками компании.
2. Кража информации (извне). Хищение информации из-за взлома компьютера.
3. Взлом программного обеспечения. На хакерские атаки приходится 15% от всей утечки информации. Для данного вида также актуально применение троянов. Главное отличие этого вида утечки – активные действия внешних лиц с целью доступа к информации.
4. Вредоносные программы (бекдоры, трояны). Целю является нанести вред владельцу, дают возможность незаметно похищать или искажать информацию.
5. Кражи носителей. Один из распространённых способов, заключается в том, что происходит кража носителя с информацией.

6. Случайные утечки. К данному виду относятся веб-утечки. Заключаются в том, что в сети появляются закрытые данные из-за потери носителя с данными или ошибки сотрудника.

Данные глобального исследования, опубликованные в июне 2016 года, в рамках которого исследовались финансовые последствия утечек данных, произошедших в 2015 году, выявили что одна утечка данных обходится компании в 4 миллиона долларов в среднем, что показывает увеличение на 29% по сравнению с 2013 годом[7].

Данное исследование проводилось компанией Ponemon Institute при помощи IBM. Данные взяты почти у 400 компаний в мире.

Согласно статистике, рост инцидентов, напрямую связанных с кибербезопасностью, как количественный, так и качественный, продолжает расти. В 2015 году согласно статистике количество инцидентов увеличилось на 64% по сравнению с 2014 годом. Чем более сложные становятся данные угрозы, тем дороже они обходятся предприятию.

Исследование выявило, что с каждой скомпрометированной записи данных организация теряет примерно 158 долларов. Утечки данных в жёстко регламентируемых отраслях обходятся ещё дороже, так, к примеру, 355 долларов в здравоохранении, что на 100 долларов больше, чем в той же отрасли в 2013году.

Если верить результатам исследования, одним из ключевых факторов, позволяющим снизить убытки, является организация команды профессионалов ответственных за инциденты. Это дало возможность компаниям сэкономить в среднем практически 400 тысяч долларов или, если рассчитывать на одну запись, то 16 долларов.

Стоимость мер реагирования (расследование причин, создание горячих линий для клиентов, найм юристов, издание предписаний регулирующих органов) составляет 59% от суммы ущерба от утечки данных. Часть этих

затрат может объясняться тем, что 70% руководителей компаний США, курирующих вопросы безопасности, сообщили об отсутствии планов реагирования на инциденты.

Исследование выявило прямую зависимость между количеством времени для обнаружения и пресечения утечки данных и стоимостью ликвидации ее последствий. В то время, как утечки, выявленные менее чем за 100 дней, обходятся компании в среднем $3,23 млн, стоимость утечек, обнаруженных позднее 100-дневной отметки, составляет в среднем на $1 млн больше ($4,38 млн).

На сегодняшний день ни для кого не секрет, что роль информации сейчас намного больше, чем была для любых компаний или государственных организаций несколько лет назад. Как говорится «кто владеет информацией, тот владеет миром», а кто владеет чужой информацией, тот намного более подготовлен к конкуренции, нежели его соперники[8].

1.3.4.Чем могут быть опасны утечки конфиденциальной информации для тех, у кого они происходят?

Компании внедряют новые информационные технологии, что ставит их в определённую зависимость от информационной системы, в свою очередь переход к электронным носителям заставляет компании в серьёз задумываться об информационной безопасности. Вмешательство любого объёма в информационную систему независимо от того, что это было - кража, несанкционированный доступ к данным, уничтожение в состоянии привести к весомым убыткам или даже стать причиной ликвидации компании, если речь заходит о коммерческой тайне или ноу-хау.

Обеспокоенность внутренними угрозами информационной безопасности обоснована. Государственные структуры, а также представители бизнеса недаром ставят утечку информации на первое место. Что обусловлено тем, что отрицательные последствия от данного действия очевидны: удар по

репутации, прямые финансовые убытки, потеря клиентов. Сравнение индексов обеспокоенности внутренними и внешними угрозами ИБ демонстрирует, что инсайдерские риски превалируют в списке наиболее опасных угроз. Кроме того, максимальный рейтинг опасности приходится на утечку конфиденциальной информации.

Согласно данным портала информационной безопасности Content Security степень опасности внутренних и внешних угроз такова:

- разглашение (излишняя болтливость сотрудников) — 32%;
- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок — 24%;
- отсутствие в фирме надлежащего контроля и жестких условий обеспечения информационной безопасности — 14%;
- традиционный обмен производственным опытом — 12%;
- бесконтрольное использование информационных систем — 10%;
- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций, связанных с отсутствием высокой трудовой дисциплины, психологической несовместимостью, случайным подбором кадров, слабой работой кадров по сплочению коллектива — 8%.

Как показывает практика, наибольшая актуальность и значимость угрозы, как это не горько, источниками которых выступают непосредственно сами пользователи систем и персонал, созданный для её обслуживания. Данная тенденция доказывается не только исследованиями крупнейших аудиторских компаний, но и отмечается в ежегодных докладах МВД России, связанных с правонарушениями в сфере информационной безопасности.

Для примера возможно рассмотреть «утечку» клиентской базы из компании в конкурирующею фирму вместе с сотрудниками. Согласно неофициальной информации с подобной проблемой столкнулся один из филиалов коммерческого банка ОАО «Уралсиб» в Воронеже, когда в конце

2009 года ряд сотрудников «Уралсиба» сменили место работы на филиал банка Банка «Поволжский», принеся с собой большую часть клиентской базы предыдущего работодателя. В результате чего клиенты «Уралсиба» стали получать назойливые предложения от нового банка. Подобное может привести к уменьшению числа клиентов, удару по репутации банка и вероятным судебным тяжбам. Но данный инцидент оба банка предпочитают не комментировать.

Такая проблема, как утечка информации, появилась достаточно давно и такие вещи, как привлечение специалистов из других конкурирующих компаний вместе с наработанными ими данными и промышленный шпионаж, известны человечеству достаточно давно. В современное время, как никогда, увеличилась их значимость и актуальность, так как современные методы хранения и обработки данных предоставляют практически безграничный потенциал для желающих заполучить данную информацию в своё распоряжение. Так как, если раньше для этого требовалось выносить целые пачки ценной документации, то сейчас есть возможность переслать информацию по сети или переписать на небольшой портативный носитель, умещающийся в кармане. Также, количество информации, которую на сегодняшний день возможно без проблем «слить», увеличивают важность угроз утечек конфиденциальной информации.

Для того, чтобы более конкретно рассуждать о вероятных последствиях утечек информации, необходимо изначально посмотреть на то, какая информация может вообще «утекать» из компании. Согласно статистике, на сегодняшний день сотрудники, как случайно, так и преднамеренно, передают за периметр своей организации больше всего подобные сведения:

- Документы, характеризующие финансовое состояние и планы организации (финансовые отчеты, различная бухгалтерская документация, бизнес-планы, договора и т.д.);
- Персональные данные клиентов и сотрудников организации;

- Технологические и конструкторские разработки, ноу-хау компании и т.п.;
- Внутренние документы (служебные записки, аудиозаписи совещаний, презентации «только для сотрудников» и т.д.);
- Технические сведения, необходимые для несанкционированного доступа в сеть организации третьих лиц (логины и пароли, сведения об используемых средствах защиты и т.п.);

Как можно увидеть заинтересованность инсайдеров — сотрудников, нелегально передающих закрытые данные, к которым у них есть доступ, - достаточно обширны. В большинстве случаев то, какие данные требуются инсайдеру, напрямую зависит от того, как в будущем он намерен её применять. Таким образом, к примеру, в большинстве случаев инсайдерам, «купленным» конкурирующими фирмами, в большей степени интересны бизнес-планы, ноу-хау и клиенты, в отличие от того, как сотрудники, желающие отомстить руководству, которое по их мнению не справедливо с ними поступило, более направлены на обнародование документов, способных в большей степени очернить нелюбимое ими начальство или саму компанию, к примеру, записи с совещаний, написанные с ошибками письма в адрес сотрудников, жалобы клиентов и др.

1.3.5.Любая ли атака в состоянии нести за собой денежные потери и каким именно способом пострадавшая компания несёт убытки от утечек информации?

Естественно, любые утечки информации по итогам которых, к примеру, доступ к новейшим разработкам компании получает конкурирующая фирма, несут за собой крайне тяжёлые последствия, так как в итоге таких утечек все ресурсы, которые были потрачены на R&D (Research & Development), фактически оказываются подаренными конкурирующему предприятию. Также, существенный урон могут нанести утечки финансовой документации, особенно, если они были совершены в период, когда предприятие находилось

в затруднительном финансовом положении, такие утечки в состоянии привести компанию в состояние вплоть до полного банкротства.

Некоторые утечки данных на первый взгляд кажутся вполне безобидными как, например, утечки тех же персональных данных. Но, согласно статистике, именно такие утечки являются причиной наиболее частых потерь компаний, связанных с утечкой данных. Компания несёт потери из-за судебных исков физических лиц, пострадавших в следствии того, что их персональные данные были опубликованы, и, тем самым, скомпрометированы, а также от штрафов, выписанных регулирующими органами, которые занимаются защитой информации на государственном уровне. Данная проблема пока не является настолько актуальной в Российской Федерации как в прочих странах запада, в которых даже самые крупные компании регулярно попадают на обложки новостных изданий из-за штрафов, выписанных им из-за утечки персональных данных сотрудников и клиентов. Но, в последнее время ситуация в нашей стране стала манятся из-за вступления в силу закона о персональных данных.

Подобным образом источником убытков становятся и утечки внутренних данных, к примеру презентаций, и тех же служебных записок. Источниками прямых убытков в виде компенсаций вреда компании, допустившей это, путём ухудшения её репутации. Испорченная репутация в свою очередь подразумевает упущенную выгоду, так как часть партнёров и потенциальных клиентов могут поменять своё решение в выборе между данной компанией и её конкурентами. Причиной тому подобных изменений может выступать не только информация, ставшая публичной по итогам утечки информации, но и сам факт того, что подобная утечка имеет место быть.

Таким образом, можно сказать о том, что любая потеря данных может нести в себе всевозможные негативные экономические последствия для пострадавшей компании. С данным мнением соглашаются и представители индустрии информационной безопасности, которые утверждают, что не

бывает безобидных утечек информации и каждая наносит свой ущерб для бизнеса, если не в данный момент, то в будущем. По словам Льва Матвеева, являющегося генеральным директором компании SearchInform - в некоторых случаях достаточно проблематично предсказать где и как «выстрелят» документы, похищенные инсайдерами из офиса пострадавшей компании. Таким образом, бывает проходит несколько месяцев или, может быть, даже лет прежде, чем украденная информация сделает своё чёрное дело, попавшись на глаза конкурентов или даже журналистов. Именно поэтому важно применять комплексную защиту данных, а не разделять их на неважную информацию и важную. Информация, которая не предназначается для публичного разглашения, должна быть закрытой. По этой причине её следует защищать от вероятных утечек.

1.3.6.Как можно произвести оценку возможного ущерба от утечки конфиденциальной информации?

Перво-наперво необходимо сверится со списком вероятных источников ущерба:

- Упущенная выгода в результате испорченного имиджа;
- Штрафы со стороны регуляторов;
- Компенсации по судебным искам;
- Снижение котировок акций (для акционерных компаний) в результате попадания на рынок инсайдерской информации;
- Прямые убытки: стоимость разработки технологических решений, стоимость проигранных в результате утечек данных тендеров и т.д.

Любая утечка данных «ставит галочку» против, как минимум, одного из выше перечисленных пунктов, наиболее серьёзные утечки в состоянии принести в компанию полный список этих проблем. Собственно, полная сумма нанесённого ущерба от одной утечки складывается из цены потери каждого источника ущерба.

Естественно, не для всех перечисленных пунктов просто подсчитать стоимость вероятного ущерба. К примеру, если штраф от регуляторов или цену технологических разработок рассчитать не представляет особого труда, то сделать предсказания, каким образом отреагирует рынок ценных бумаг в ответ на данные, которые будут опубликовано инсайдерами, или то, какое число клиентов захотят отказаться от услуг компании по результатам ухудшившийся репутации, является практически невозможной задачей. По данной причине в проведении оценки рекомендуется не придерживается оптимистичного исхода, а закладывать в бюджет сумму максимально возможных потерь по причине утечки. К сожалению, в России на данный момент нет достоверных данных, которые бы показывали среднюю стоимость утечки данных, однако, в данном вопросе возможно ориентироваться на данные, полученные от других стран, которые с большой долей вероятности будут очень схожи с данными по России

Согласно опубликованным исследованиям Ponemon Institute, средняя стоимость, в которую обходились утечки данных в Великобритании в 2008 году, составляла 1,7 млн фунтов, что составляет около 80 миллионов российских рублей. Также, согласно подсчётам средние убытки, которые несёт компания из-за потери одного служебного ноутбука, составляют почти 50 тысяч долларов. Данные сведения были получен от 29 компаний,которые пережили 138 отдельных случаев утери ноутбуков постоянными или временными сотрудниками, сообщает Руформатор, ссылаясь на PCWorld. Данная сумма была получена при помощи *учета семи различных факторов* определения утраченных данных, экспертизы и расследования условий потери, сообщения об утечке информации, действий по уменьшению потерь производительности, стоимости самого ноутбука, утери интеллектуальной собственности, и других юридических и нормативных затрат.

Также, согласно подсчётам экспертов, чем быстрее компания сможет среагировать на потерю компьютера, тем меньше потерь она понесёт. В

случае, если потерю удалось обнаружить в день потери, то и затраты могут составить по средним подсчётам всего 8 950 долларов. По прохождению недели они могут составлять уже 115 849 долларов.

Шифрование данных приводит к значительному уменьшению потерь при утере устройства. Так, если данные, находящиеся на жёстком диске ноутбука, зашифрованы, потеря обходится в 37 443 долларов, в случае, если этого не было, то в 56 165 долларов.

Также, не в последнюю очередь на финансовые потери организации влияет то, какую должность в компании занимает человек, который потерял компьютер, или утративший его в результате противоправных действий. Большей ценностью обладает ноутбук, как не странно, не высшего должностного лица, а менеджера или директора. В случае, если потеря была совершена топ-менеджером, инцидент обходится в среднем в 28 449 долларов, но, в случае, когда потеря была совершена директором или менеджером, сумма составляет 60 781 долларов и 61 040 долларов соответственно.

Это является свидетельством о присутствии высокого уровня риска для корпоративных сетей, так как доступ к сайтам для взрослых, поиск работы на непроверенных ресурсах и прочие виды нецелевого применения рабочих ноутбуков могут стать причиной серьёзных утечек информации, и в ряде случаев и к проникновению вредоносного ПО в сеть организации.

1.3.7.Зачем проводить оценку возможного ущерба от утечки данных?

В первую очередь для того, чтобы определить какую цену действительно имеет конфиденциальная информация, которая находится в распоряжении организации, а также определить насколько выгодно будет внедрять средства защиты информации от её возможных утечек, к примеру, DLP-систем. Выгода во внедрении и будет присутствовать, когда сумма вероятной утечки хотя бы в 2 превышает цену внедрения систем данного типа. Судя по статистическим

данным для большей части компаний внедрение DLP-систем будет более, чем целесообразно.

Картину распределения утечек по отраслям регламентируют 2 основных фактора – это защищённость информации и ликвидность. В отраслях, где данные обладают большей ценностью, способом защиты информации уделяется больше внимания, нежели в остальных. К примеру, в страховых организациях, госсекторе и банках объём утечек значительно меньше. Организации данного вида применяют защиту информации с помощью технических и организационных мер: применяют SIEM, DLP и прочие профильные ИБ-системы, следят за уровнем цифровой грамотности сотрудников. Некоторое время назад бизнес охотнее вкладывался в сбережение собственной интеллектуальной собственности, ноу-хау, и коммерческих секретов, при этом относясь к защите данных пользователей с меньшим интересом, то с применением значительных штрафов за утечки ПДн эта ситуация поменялась.

1.3.8.Статистика по утечкам информации

2 апреля 2019 года компания InfoWatch сообщила, что по результатам глобального исследования Аналитического центра компании InfoWatch, в мире в 2018 году было зарегистрировано 2263 публичных случаев утечки конфиденциальной информации. В 86% инцидентов были скомпрометированы персональные данные (ПДн) и платежная информация — всего около 7,3 млрд записей пользовательских данных против 13,3 млрд записей данных годом ранее. В 2018 году существенно сократился объем данных, скомпрометированных в результате утечек из организаций сферы высоких технологий, финансово-кредитного и страхового сектора, а также предприятий промышленности[9].

По данным компании, наибольшей привлекательностью для злоумышленника обладают сведения из организаций финансово-кредитной и страховой сферы, в которых в свою очередь примерно 65% случаев утечки

имели умышленный характер. Также, согласно данным, большой интерес представляют данные из промышленных и транспортных систем, компаний сфер торговли и HoReCa, а также высокотехнологичного бизнеса в данных отраслях более 50% утечек имели умышленный характер.

Отраслями, лидирующими в количестве утекающей информации, становятся высокотехнологичные компании, к такому же количеству утечек относятся предприятия сферы торговли, медицинские и муниципальные учреждения, а также HoReCa. На данные отрасли приходится в сумме около 70% объема утечки данных, происходящих в год.

Как и в 2017 году, 30% мирового объёма утечек информации о пользователях пришлось на сферу высоких технологий. Одновременно с этим согласно статистике, средняя мощность произошедших инцидентов в высокотехнологическом секторе уменьшилась более, чем в двое, вплоть до показателей 9 миллионов записей на одну утечку в 2018 году.

Также, согласно данным, размер утечек данных о пользователях сократился в страховой и финансово-кредитной сферах. Предприятиях транспорта и промышленности. Количество утекшей информации, если брать финансовые и страховые компании, уменьшилась в четверо, а показатели мощности в среднем снизились с 840 до 190 тысяч записей данных. До семи раз уменьшился объём записей данных, в промышленности и транспортных предприятиях, которые были скомпрометированы, их мощность составила менее 100 тысяч записей.

Значительные массивы информации теряли организации в сфере торговли и HoReCa – более 18% утекшей информации. Согласно данным, средняя мощность каждой утечки составляла до 430 тысяч записей данных. По 9% и 12%, соответственно, в общемировом количестве утечек платёжной информации и ПДн, соответственно. Однако, доли муниципальных и медицинских учреждений: согласно статистике, каждая утечка из муниципалитета способна привести к компрометированию 400 тысяч записей

данных, в отличие от медицинской отрасли, где для каждого инцидента показатель мощности составляет порядка 60 тысяч записей.

Рекордные потери, вызванные потерей данных у компании, зарегистрированы в 2018 году японской крипто биржей Coincheck. В результате утечки данных онлайн кошельки её клиентов были скомпрометированы, ущерб оценивается в 534 миллиона долларов.

За всю историю самый большой штраф, выписанный компании за утечку данных, был выписан Компани Uber за потерю данных клиентов и водителей её обязали выплатить 148 миллионов долларов США.

По итогам 6,5 тысяч утечек компрометированию подверглись 5 миллиардов конфиденциальных записей данных.

Компания Risk Based Security опубликовала 20.02.2019 года данные о том, что в 2018 году было проведено более 6500 утечек данных компаний, что в сравнении с 2017 годом снизалось лишь на 3,2%.

В итоге 5 миллиардов записей данных, которые являлись конфиденциальными, попали в публичный доступ. Согласно данным на компанию HoReCa, технологические компании, ретейлеры и финансовые организации пришлось 66% утечек.

«В ходе исследований компании Risk Based Security лишний раз подтвердилось то, что нельзя относиться к защите информации, как к второстепенной сфере, а следует уделять ей достаточно внимания и не забывать про этот столь важный аспект.

Также, *полноценная защита не может осуществляется без аналитики и мониторинга.* По итогам 2018 года лишь 30% компаний, чьи конфиденциальные данные были подвержены компрометированию, смогли идентифицировать проблему своими ресурсами в отличие от оставшихся 70%, которые узнали о проблеме от источников из вне по факту

компрометирования.» - Заявил главный инженер представительства Citrix Сергей Халяпин в Росси и странах СНГ[10].

В настоящие время существуют современные системы, основанные на ИИ и машинном обучении, которым под силу не только своевременно находить прорывы периметра безопасности, но также и самостоятельно указывать на возможные угрозы безопасности.

Согласно данным можно сказать, что 57% скомпрометированных записей данных содержали в себе сведения о логинах и паролях пользователей. Для того, чтобы минимизировать вред от раскрытого пароля, будет целесообразно компаниям применять многофакторную аутентификацию, поведенческий анализ и контекстный доступ к сети. В таком случае при получении пароля злоумышленником и какиой-либо другой информации для МФА, к примеру, способом социальной инженерии, система будет в состоянии ограничить его доступ к сети, как только его действия начнут не соответствовать определённому шаблону поведения.

1.3.9.75% утечек информации имеют за собой целенаправленный характер и не являются случайными.

Компания InfoWatch, а именно её аналитический центр, сообщил 11 февраля 2019 года ключевые сведения о потерях данных компаний из сферы транспорта: компании-перевозчики, аэропорты, вокзалы, морские и речные порты, каршеринговые компании.

Количество произошедших утечек в данной отрасли в 2018 году снизилось на 6% по сравнению с предыдущим годом, но при этом количество скомпрометированных данных увеличилось на 75%. Доля специально устроенных утечек увеличилась с 55 до 76 процентов. Вместе с этим количество утечек, виной которых стали руководители и сотрудники, увеличилось почти в 3 раза. Таким образом, в 2017 году умышленными были 18 процентов утечек, то уже на следующий год половина. Также значительным

изменениям подверглась структура данных, подвергшихся компрометированною. Таким образом, в 2018 году объём персональных данных увеличился с 71 до 79 процентов, а вот ноу-хау коммерческих секретов изменился куда более кардинально, увеличившись в 4 раза с 3,5 до 14 процентов.

Большая часть произошедших утечек в области транспорта была направлена на авиакомпании и аэропорты. В 2018 году был зафиксирован самый крупный инцидент, произошедший на азиатском континенте. Авиакомпания Cathay Pacific находящаяся в Гонконге, занимающая 6 место в рейтинге мировых воздушных перевозок, была вынуждена сообщить, что злоумышленникам удалость выкрасть данные более, чем 9 миллионов пассажиров, а именно: даты рождения, имена, номера телефонов, паспортные данные, адреса электронной почты. В итоге подверглись компрометированию более 800 тысяч паспортных данных.

Также компания British Airways сообщила о том, что у неё были украдены данные включая: персональные и платёжные данные клиентов, которые пользовались её услугами в период с 21 августа по 5 сентября 2018 года, при этом оформляя билеты удалённо, как через мобильные приложения, так и через их официальный сайт. Первоначально велась речь о том, что были утеряна данные 380 тысяч пассажиров, но позже представители компании заявили о том, что также были затронуты данные ещё 185 тысяч человек. Чуть позже киберполиция Украины обнаружила хакера, на чьём компьютере была обнаружена полная база данных одной из крупных международных транспортных Компаний. По некоторым данным известно, что база содержит данные 120 тысяч человек.

GoAir – индийская авиакомпания, выдвинула обвинения в адрес своего бывшего генерального директора Вольфганга Прок-Шауэра, утверждая, что тот провёл хищение конфиденциальной информации. Прок-Шауэр в начале 2018 года был главой индийской авиакомпании. Юристы данной компании

предъявили суду ряд доказательств, которые показывали, что гендиректор забрал с собой часть конфиденциальных данных при переходе на другое место работы.

1.3.10.Было обнаружено более 5 тысяч потери данных, виной которых стали только инсайдеры.

Компания InfoWatch представила 28 декабря 2018 года результаты проведённого ею анализа инцидентов кражи конфиденциальных данных, причиной которых послужили внутренние нарушения, произошедшие в организациях сроком за последние 5 лет. За данный срок было выявлено число утечек конфиденциальных данным по некоторым данным превосходящие 5 тысяч из-за действий инсайдеров: работников организаций, подрядчиков, топ-менеджеров. Практически 60 процентов данных утечек имели случайный характер, в итоге больше 95% от общей суммы пострадавших по вине сотрудников, записи данных были подвержены компрометированию из-за несоблюдения правил безопасности, незнанию правил пользования или перебоев с функционированием систем, занимающихся обработкой данных.

В период с 2014 по 2018 год подверглись существенным изменениям в сторону внутренних утечек. Также можно заметить, что существенно изменилась мощность утечек в большую сторону.

Вывод.

Всё выше сказанное свидетельствует о том, что в век развития информационных технологий защита информации является весьма актуальной проблемой. Растёт разнообразие мобильных устройств, они занимают всё больше места в нашей жизни и всё чаще становятся объектами внимания мошенников. Потому, информационная безопасность мобильных устройств становится всё более важной.

2.Глава оценка коммерческого потенциала

Оценка коммерческого потенциала состоит из 2-х частей: оценка коммерческого потенциала интеллектуальной собственности, собственно, являющееся самой инновацией, и коммерциализация самого готового приложения для того, чтобы правильно оценить наиболее рентабельные пути реализации, наиболее перспективные и долговечные инвестиции и в общем смысле понимать будет ли продукт в каком-либо виде окупаем и какой способ реализации будет предпочтителен для данного продукта.

2.1.Оценка коммерческого потенциала интеллектуальной собственности

Одной из важнейших задач в инновационной стратегии является задача коммерциализации объектов, являющихся интеллектуальной собственностью. Это определяется тем, что эффективность решения данной проблемы напрямую влияет на конкуренцию национальной продукции на международном рынке[11].

Признание объектов интеллектуальной собственности товаром, объектом коммерческой реализации формирует новую функцию промышленных организаций, которая заключается в сотворении характерного продукта – интеллектуальной собственности, который может быть введен в хозяйственный оборот.

Конкурентоспособность организаций в случае, когда речь идёт о инновационной экономике, помимо способности удовлетворять общественную потребность в реализации и создании продукции, определяется ещё способностью осуществлять и создавать правовую охрану и грамотно реализовывать интеллектуальную собственность, которая будет востребована как отечественным, так и мировым рынком[12].

На текущий момент для большей части российских компаний является типичной ситуация, когда частью их активов выступают объекты, являющиеся частной собственностью, многие из которых в течении нескольких лет не

используются предприятием, но и более того, даже в процессе сотворения не планировались использоваться. Несмотря на это предприятие поддерживает патент, тем самым неся убытки от патента, заведомо не нужного предприятию[13].

Тем не менее, для нынешней экономики более логично будет в первую очередь оберегать инновации, способные работать, благодаря чему компании смогут получать доход. Первоначально нужно из всего многообразия итогов научно технической деятельности выявить объекты, которые наиболее вероятно могут приносить доход, и лишь за тем заниматься их защитой в соответствии с законодательством и мировым правом[14].

2.2.Но каким методом можно произвести перевод коммерческого потенциала инновации конкретные показатели, укладывающиеся в систему?

Наиболее подходящей формой установки приоритетов и оценивания потенциала итогов научно технической деятельности выступают шкалы оценок и системы показателей инноваций. В виде основополагающих критериев оценивания коммерческого потенциала итогов научно технической деятельности можно обозначить далее указанные категории показателей, описывающие объекты интеллектуальной собственности[15].

- технические – вид объекта, его технические характеристики, изобретательский уровень, конкурентные преимущества, основанные на уникальности и новизне научной разработки;

- правовые – форма, надежность правовой защиты, объем, территория и срок действия исключительных прав;

- рыночные – емкость рынка, количество и качество аналогов;

- экономические – показатели, характеризующие уровень производственной готовности и коммерческого риска освоения разработки,

степень промышленной применимости, направления и способы использования, универсальность применения.

2.3.Таблица Система показателей оценки коммерческого потенциала инноваций

Эта система показателей в состоянии быть применена промышленной компанией как одного из методов, по которым оценивается коммерческий потенциал разработок, которой владеет компания. К примеру, по оценкам экспертов максимальной коммерческую ценность будут представлять объекты интеллектуальной собственности, сумма баллов которых будет в диапазоне от 250 до 380. По данной шкале средним уровнем коммерческого потенциала обладают разработки, соответствующие по данной шкале диапазону 100 – 250 баллов. В случае, если значение ниже 100 баллов по данной шкале, это означает, что данный продукт характеризуется низким уровнем коммерческой привлекательности.

2.3.1.Метод ранжирования

В таблице представлены: предварительная оценка объекта с точки зрения коммерческого потенциала и выбор наиболее привлекательного объекта путём применения метода ранжирования.

Таблица Форма предварительной оценки коммерческого потенциала оцениваемых объектов

Параметр оценки	Количество баллов по оцениваемым объектам			Вес	Итоговая оценка, баллы		
	1	2	3	параметра	1	2	3
новизна	5	5	5	5	25	25	25
правовая охрана	10	10	10	5	50	50	50
технико-экономическое значение	5	5	5	5	25	25	25
оставшийся срок действия исключительных прав	5	10	10	3	15	30	30
объем потенциального рынка	10	5	5	3	30	15	15
наличие аналогов	5	0	0	2	10	0	0
объем исключительных прав	10	10	10	2	20	20	20
территория действия исключительных прав	5	5	5	2	10	10	10
степень устаревания	5	5	5	3	30	15	15
уровень производственной готовности	10	10	5	3	30	30	15
уровень коммерческого риска	5	5	0	2	10	10	0
срок окупаемости	5	5	0	1	5	5	0
область и направления использования	5	5	5	4	20	20	20
Итого:					265	245	215

По итогам предварительной оценки, проведённой методом ранжирования, выходит, что наибольший коммерческий потенциал присущ объекту № 1. Количество набранных баллов равно 265, что относит его к категории высокой коммерческой привлекательности данной инновации для организации. Для данного объекта в таблице выигрышными являются такие пункты как производственная готовность данного изобретения, его конкурентно способность, а также наличие существенного потенциала для дальнейшего его развития и расширения сегмента на рынке.

Данные, полученные из шкалы, приведённой выше, частично имеют субъективный характер. Но вместе с тем они дают возможность организациям сложить первоначальное представление о потенциале коммерциализации, а также о распространении научно технических разработок, находящихся в их собственности[16].

В промышленных организациях необходимость управления и оценки интеллектуальной собственности можно объяснить обширным числом направлений применения и существенной доходностью операций, связанных с коммерческой реализацией интеллектуальных ресурсов.

2.4.Коммерциализации технологий

Успех коммерциализации технологий по большей части обуславливается первоначальным выбором наиболее перспективных технологий или продуктов, на которых в последствии сосредотачиваются финансовые ресурсы и человеческие усилия. В последние время оценка, на которой основывается подобный отбор, данная процедура всё больше приобретает профессиональные черты, полагающаяся на комплексном понятии о возможных перспективах данного инновационного проекта (или базового курса инновационной компании). Надлежащие приемы и инструменты приобрели наименование оценки технологий или технологического аудита[17].

Согласно многократным изучениям провалов и успехов, показатели риска меняются в направленности от улучшения данного продукта для известных рынков к новоиспеченным для компании продуктам для известных рынков и далее к новоиспеченным продуктам для новых рынков, где риск работы на неизведанном рынке превышает риск вовлечения в новый продукт. При создании проектов программ НИОКР или инвестиционного портфеля необходимо избежать одномоментного исполнения нескольких проектов, характеризующихся высоким показателем риска[18].

Профессиональное проведение оценок технологий даёт возможность увидеть продукт нового уровня, а также найти на раннем этапе проекта коммерческий потенциал разработки или, наоборот, ее коммерческую бесперспективность.

В принятии решения роль данных оценок играет не последнюю роль, также высокой ценностью является информация, полученная в ходе оценки. В такие случаи компании, специализацией которых является технологический аудит, и ряд банков применяют собственный алгоритм оценки коммерческого потенциала технологий, считают данные методики и практику применения этих технологий конфиденциальной информацией, своими коммерческими “ноу-хау” [19].

2.5.Стандартные подходы к оценке коммерческого потенциала технологий

Главной составляющей к проведению оценки потенциала коммерциализации результатов НИОКР, а также технологий выступает осознание основополагающих законов открытой рыночной экономики, в которой успешное существование бизнеса гарантируется только при условии обеспечения соответствующей конкурентоспособности. Продукт, являющийся лучшим из всевозможных в данном регионе, в состоянии иметь лишь временное право на существование. Конкурировать – означает состязаться с лучшими[20].

Не стоит мешать технологическую экспертизу и такую вещь как оценку технологии с точки зрения коммерческой привлекательности. В случае с оценкой коммерческого потенциала технологии не имеет большого значения, способ, которым были достигнуты те или иные параметры, но в большей степени важны конкурентные преимущества и уверенность в том, что они будут сохраняться ещё продолжительное время, а также выявление потребителей, заинтересованных в продукте[21].

Осуществление данной оценки сфокусировано преимущественно на выявлении необходимости реализации новых идей/технологий и осуществимости данных в масштабах промышленного размера.

Данные оценки обычно состоят из рассмотрения определённого количества блоков вопросов, из которых обязательными являются следующие:

- преимущества перед конкурентами: определяются соперничающие продукты, проводится оценка уровня преимущества предполагаемого продукта и его характера, берутся для рассмотрения всевозможные мотивы потребителя перейти с текущего продукта на новый.

- характеристики предполагаемого рынка: размер, динамика роста, основные сегменты, трудности вхождения в конкретный рынок.

- предполагаемые конкуренты: определяются главные конкуренты, кто является их потребителями и их поставщиками, стратегия, которую они применяют для своих новых разработок, интерес к конкурентному сегменту, в котором предполагается продвижение нового продукта.

- реализуемость идеи: проверяется возможность создания работающего прототипа, возможность масштабирования, независимость данной разработки от прочих разработок, специальных разрешающих процедур, экологических норм, которые действуют в настоящее время, также проверяется наличие поставок дефицитных составных, которые могут быть заблокированы конкурентами.

- защищённость идеи: проводится оценка, как легко возможно скопировать имеющийся продукт конкурентами, возможность применения правовой защиты, а также теоретическая “высота забора и ширина территории” предполагаемых патентов.

- обеспечение ресурсами: оценивается возможность разработки и реализации на оборудовании, доступном в данный момент, возможность привлечения дополнительного персонала, возможность доступа к разнообразным источникам финансирования.

Так как нужные условия успеха коммерциализации – устойчивое вхождение и существование на рынке, анализ рынка имеет ключевое значение. Таким образом, получается, что *появление нового продукта становится возможным при соблюдении одного из трёх условий:*

Спрос на рынке полностью не удовлетворён

Рынок имеет тенденции к заметному росту

Существует шанс вытеснения конкурента с рынка

Проводя оценку преимуществ для потребителя, стоит делать акцент на переход с существующего продукта на новый, стараясь выявить, в какой степени предлагаемые преимущества смогут убедить потребителя приобретать текущий продукт у известного ему поставщика и начать отдавать преимущества новому товару с новым поставщиком, покупать нужное для новой технологии специализированное оборудование и т.д.

Типовой список данных, которые предпочтительно знать о конкурентах, состоит из:

Формат доработанной продукции конкурентов или её новый продукт

Формат проводимых ими НИОКР

Цены конкурентов и себестоимость их товара

Партнёры конкурентов и их основные потребители

Основные направления развития продукции, выпускаемой конкурентами

2.6.Дальнейшие планы развития конкурентов

В случае, если планируемый продукт будет успешным, все предприятия, в том числе и конкуренты, захотят примкнуть к успеху и производить аналогичные продукты, или же пользоваться подобной технологией. По этой причине правильная защита интеллектуальной собственности выступает важным фактором, положительно влияющим на риск раннего угасания периода продаж нового товара.

Также существуют кроме качественного ещё и количественные методы оценки коммерческого потенциала технологий, наибольшей полезные в случае сравнительного анализа технологии и их ранжирования по коммерческому потенциалу или надлежащим рискам.

При данном подходе всем признакам назначается определённый бал и ставятся конкретные оценки для каждого конкретного пункта, относящиеся к конкретному проекту. По завершению определения всех параметров могут устанавливаться коэффициенты “весомости” для каждого конкретного продукта, к примеру: низкие цены или патент, полученный за рубежом. Или выявляются группы факторов такие как например: большая юридическая защита продукта, рассматриваемых в совокупности рассматриваемых параметров.

Практика осуществления качественной комплексной экспертной оценки технологий базируется на трех группах методов, которые включают:

Сканирование среды

Функциональный анализ

Оценка и прогнозирование.

2.7.Роль и методы прогнозирования изменения (развития) технологий

Полный цикл развития инновационного проекта, в большинстве случаев занимает несколько лет, и некоторые компании в следствии неготовности к обязательным изменениям технологий у конкурентов или некорректного учёта всевозможных характеристик, регламентирующих изменения рынка терпят неудачу[22].

Для успешного процесса коммерциализации технологий нужно предвидеть какие изменения и в какой степени могут повлиять на конкретный бизнес. Зачастую эффективность коммерциализации технологии или, более того, возможность реализации её зависит от того, насколько эффективно получается предсказать или среагировать на самые первые и малозаметные признаки грядущих рыночных изменений.

Способы предсказания развития этого направления технологий, составляют главную часть комплексной оценки коммерческого потенциала НИОКР, которые включают ряд методик и средств, зачастую применяемых в целях предсказания не только для технологий и технологических продуктов.

2.8.Анализ тенденций.

Основные методы данного подхода – экстраполяция тенденций или, как ещё можно сказать, оценки, повторяющиеся во времени, дающие возможность проекции прошлого на будущее на несколько лет вперёд. Кроме подхода экстраполяции также существуют методы, основанные на вероятности того, что развитие продукта со временем затухает, в такие случаи кривая экстраполяции принимает S-образный облик. Оценки такого типа позволяют понять верхний предел вероятных параметров и дают возможность учесть вероятное воздействие не предсказанных событий. Также стоит отметить, что дополнительное применение статистических подходов даёт возможность определить тенденции, являющиеся систематическими на фоне случайных изменений, а также заниматься прогнозированием будущего в функции

значимых систематических переменных; получить регрессивнные выражения, описывающие взаимосвязи ряда факторов[23].

Особое положение занимают методы, являющиеся специфическими для оценки технологии, а, именно, методы анализа научно технической литературы и патентных тенденций.

Экспертные оценки. Данный способ имеет наиболее распространение, прогнозирование технологии базируется на применении индивидуальных интервью, всевозможных групповых методов на подобии метода Дельфи, направленного на получение согласованного мнения экспертов, а также применения анкетирования.

Многопараметрический анализ. Данный подход позволяет рассматривать многовариантность будущих исходов, а также включает приёмы типа построения древа гипотетически возможных исходов, также применение метода разработки альтернативных сценариев дальнейшего развития технологии.

2.9.Методы экспресс-оценки коммерческого потенциала технологий

Цель данных экспрессных методов заключается в том, что - по возможности раннее обнаружение коммерческой заинтересованности в идее, изобретении, сфере исследований. Значительными возможными достоинствами данных заключений является выявление потенциально возможных партнеров, потребителей или покупателей лицензий. Либо наоборот, осуществляемая оценка в состоянии дать ранний сигнал тревоги в случае касательно возможного одобрения идеи или изобретения рынком, или возможно, даже найти факторы, указывающие на неперспективности выделения дальнейших ресурсов на рассматриваемою разработку.

Данные экспресс-оценки направленны преимущественно на осознание возможного принятия инновации рынком, таким образом, не предусматривают обширного “библиотечного” анализа, необходимого для

полномасштабных маркетинговых исследований, к примеру, в процессе лицензирования технологий.

Данное предварительное исследование предполагаемой реакции рынка направлено по большей части на взаимодействие с гипотетическими потребителями или покупателями лицензии.

2.10.Использование методов оценки коммерческого потенциала технологий

Успех коммерциализации технологий в большей степени зависит от начального отбора продукта, обладающего наибольшей перспективой, на котором в последствии сосредоточиваются людские и финансовые ресурсы. В последнее время оценка, находящаяся в основании данного отбора, приобретает всё более профессиональные черты, полагающиеся на комплексное суждение о перспективах инновационного проекта (или базового направления инновационной компании). Подобные приемы и инструменты получили название оценки технологий (technology assessment) или технологического аудита (technology assessment) [24].

Способы оценки технологий применяется на всевозможных стадиях реализации инновационного процесса. С наибольшей частотой оценка применяется на следующих стадиях:

-·Анализ итогов промежуточного этапа выполнения НИОКР для утверждения решений о необходимости его продления (от данного анализа ожидают бинарной и крайне важной рекомендации,” да” или “нет”)

-·Передача технологии из организации, занимающей исследованиями в частный сектор, дочерней фирмы или частному предпринимателю, который в свою очередь желает знать профессиональный взгляд о ее коммерческих возможностях.

-·Определение относительного уровня технологии и выбор максимально привлекательных альтернативных работ из представленного набора

предложений для дальнейшего финансирования при создании планов НИОКР (ранжирование проектов по потенциалу коммерциализации)

-·Аргументирование целесообразности финансирования определённого проекта, в случае, когда итоги оценки технологий выступают в качестве начальной основы расчета перспективной коммерческой отдачи

-·Создание инвестиционного портфеля, уравновешенного по уровню рисков провала коммерческого успеха, определившихся при проведении оценки технологии.

-·По результатам обширного числа исследования удач и провалов, уровень риска увеличивается по направлению противоположному улучшению рабочего продукта для существующих рынков к новоиспеченным для компании продуктам, где риск работы на неизвестном ранее рынке превосходит риск втягивания в свежий продукт. При создании проектов программ НИОКР или для инвестиционного портфеля хорошо бы избегать одномоментной реализации нескольких проектов, связанных с большим риском.

-·Профессиональное осуществление оценки технологий даёт возможность узреть продукт абсолютно нового поколения, а также обнаружить на начальном этапе проекта коммерческий потенциал разработки или, наоборот, ее коммерческую несостоятельность.

-·Значение данных оценок в принятии решений крайне значительно, а приобретенная информация имеет значительную ценность. В этой связи часть компаний, специализирующихся на технологическом аудите, и часть банков, применяющих свой неповторимый алгоритм оценивания коммерческого потенциала технологий, относят данные методики и практику их применения конфиденциальной информацией, собственными коммерческими “ноу-хау”.

Исходя из всего выше сказанного можно провести оценку коммерческого потенциала и на его основе сделать выводы о том, насколько

рентабельным будет являться данный продукт и о наиболее приемлемых способах его реализации на имеющихся рынках сбыта.

Одним из важнейших факторов, влияющих на коммерциализацию, является необходимость в данной технологии и готовность рынка к ней. Одним из таких показателей для данного продукта будет служить то, сколько банки тратят на обеспечение ИБ - существенные суммы денег, что косвенно показывает их готовность к применению новых видов защиты и необходимости в данном продукте.

Так, к примеру, некоторые банки, принявшие участие в исследовании «Сколько стоит безопасность», выделялись на фоне остальных компаний по объему бюджета на обеспечение ИБ, который в среднем составил 80–150 млн рублей. Для сравнения, большинство финансовых учреждений ограничиваются суммами в 20-40 млн рублей.

Данные от проведённых исследований выявили что банковская отрасль — является единственной отраслью, в которой присутствует 100% тенденция к обучению компаниями своих сотрудников основам ИБ. Более того, всю деятельность по донесению информации по вопросам ИБ нужно доносить по требованиям PCI DSS и рекомендации Банка России[25].

В топ – 10 финансовых организациях (по выделяемому бюджету на ИБ) применяются самые совершенные подходы к защите, но ситуация в остальных банках не является столь радостной. К примеру, межсетевые экраны прикладного уровня (Web Application Firewall), применяемые для обеспечения безопасности веб-приложений используются в 70% из списка топ-10 по ИБ-бюджету, но у остальных ситуация не столь радужная и составляет всего 13%. При этом собственные ситуационные центры информационной безопасности (Secutiry Operation Center) имеют все банки из топ-10 и только 40% — среди остальных. 37% всех финансовых учреждений, принявших участие в исследовании, иногда привлекают экспертов сторонних компаний для

расследования инцидентов, причем большинство из них при этом имеют внутреннее подразделение SOC. SIEM-системы применяют 65% финансовых компаний (среди банков из топ-10 по бюджету на ИБ этот показатель — 100%). У 25% банков-респондентов отсутствует контроль установки обновлений ПО, 8% не отслеживают появление информации о новых уязвимостях (0-day). Кроме того, 10% финансовых учреждений никогда не проводили работ по тестированию на проникновение или комплексный аудит информационной безопасности, несмотря на требование стандарта PCI DSS 3.2 и рекомендации Банка России[26].

2.11.Шесть компонентов защиты

В Positive Technologies выделили шесть компонентов защиты, которые в дополнение к стандартным средствам защиты позволят не только соответствовать требованиям регуляторов, но и уверенно противостоять киберпреступникам. Среди них:

- регулярное проведение тестов на проникновение,
- готовность к реагированию на инциденты,
- контроль сетевого периметра,
- наличие WAF и SIEM,
- обучение сотрудников основам ИБ.

Согласно проведённым исследованиям оказалось, что среди опрошенных банков всего 13% из них используют схожий комплексный подход к защите от киберугроз. Но в других отраслях дела обстоят ещё хуже, так как такие компании отсутствуют вовсе.

Исходя из всего выше сказанного получаем, что система, в которой будут применятся все шесть компонентов, будет выступать наиболее защищённой от всевозможных угроз, что непременно позволит ей стать наиболее привлекательной для потребителя.

Не менее важным критерием является то, с какой лёгкостью будет возможно восстановить систему после произошедшего проникновения. Связанно это с тем, что стоимость дня простоя наносит существенный ущерб организации.

2.12.Затраты на восстановление

Помимо прямых финансовых потерь от киберинцидента в Positive Technologies также провели оценки затрат на восстановление корпоративной инфраструктуры после вывода из строя всех ресурсов домена. 12% банков оценивают восстановление в сумму от 10 до 50 млн рублей, а каждый третий банк (33%) готов потратить на эти мероприятия от 2 до 10 млн рублей[27].

2.13.Стоимость дня простоя

День простоя из-за кибератаки может обойтись банку в 50 млн рублей — в такую сумму оценивают потери 30% российских кредитных организаций, опрошенных Positive Technologies в ходе исследования.

Остальные банки, участвовавшие в опросе, оценили возможный ущерб от отказа в работе корпоративной инфраструктуры в течение одного дня в сумму: от 10 до 50 млн рублей — 7% опрошенных, от 2 до 10 млн рублей — 25%, и от 0,5 до 2 млн рублей — 38%[28].

Вывод

Для того, чтобы инновация имела наибольший коммерческий потенциал, необходимо уделить особое внимание таким пунктам при её создании как: новизна, правовая охрана, технико-экономическое значение, область и направления использования. Также необходимо не забывать об остальных пунктах, максимальное соблюдение которых увеличит коммерческую привлекательность инновации.

3.Глава разработка

Для того, чтобы применять методы по улучшению безопасности приложения, нужно для начала понимать основные способы взлома и иметь представление о том, как каждый из них функционирует и взаимодействует с ПО, а также как и в каких случаях может быть применён и насколько будет эффективен в каждом случае.

3.1.Классификация и способы взлома.

Методы взлома онлайн-банкинга, аналогичны методам взлома любого веб-приложения:

3.1.1Фишинг.

3.1.1.1.Источник угрозы

Технологии, которыми пользуются фишеры, подвергаются постоянному совершенствованию. Так, к примеру, с недавнего времени появилось такое понятие как фарминг. Целью данного вида атак является получение персональных данных пользователя. Используя вирусные программы, злоумышленники изменяют файл hosts, после данной процедуры компьютер автоматически начинает перенаправление с заданных сайтов на сайты двойники, которые являются точными копиями оригинальных сайтов. Данную подмену будет проблематично обнаружить даже пользователям с опытом. Наиболее частыми мишенями для злоумышленников служат: Сбербанк, Ebay, PayPal и прочие финансовые организации. Атаки фишеров носят как случайный, так и целенаправленный характер. В случае, если атака проводится «наобум», то её целями служат, как правило, достаточно большие проекты такие как, Ebay, на данном ресурсе зарегистрировано большое количество из разных стран и континентов. В случае, если атака является целенаправленной, то злоумышленник собирает информацию о том, какой провайдер, платёжная система и банковское учреждение применяется жертвой. Даная атака является более сложной и требует больше усилий, однако, она позволяет проводить рекордный процент удачных атак[29].

3.1.1.2.Анализ риска

Существуют разнообразные способы для борьбы с такого рода мошенничеством. Речь идет о законодательстве и разнообразных технологиях. Чтобы защититься от фишинга, пользователь должен быть крайне внимательным. Рекомендации, благодаря которым можно обезопасить себя от фишинга (phishing):

1. Нужно проверить написание домена, с которого пришло письмо, корректно ли написан домен, нет ли подмены.
2. Если сайт не вызвал подозрений, то следует проверить страницу, указанную в сообщении на специальном ресурсе, например, virustotal.com. Сайт может быть заражен.
3. Потребуется проверка цифрового сертификата сайта.
4. Посмотрите, есть ли опечатки в тексте письма или какие-либо странности оформления. Уважаемые организации не позволят себе этого.
5. Используйте защитные программы, имеющие в арсенале веб-антивирус и веб-фильтры вредоносных и подозрительных адресов.
6. В случае любого подозрения лучше удалить сообщение и вручную зайти на веб-ресурс указанной в нем организации, связаться с клиентской службой по телефону (основа успеха данного взлома - доверчивость пользователя).

Как с помощью браузера узнать об угрозе фишинга? Еще один вид борьбы с мошенниками заключается в создании списка фишинговых сайтов и сверяться с ним в дальнейшем[30].

3.1.2.Кража личных идентификаторов (личности).

Кража личных идентификаторов (личности). Во многих интернет системах, в том числе и в системах веб-банкинга, присутствует такая вещь как аутентификация по паролю, успешный перехват которого позволит

злоумышленнику инициировать ряд действий. Помимо этого, в веб приложениях существует такая вещь как воровство идентификатора сессии или, иначе говоря, куки, кража которых даёт возможность злоумышленникам подключаться к сессии пользователя, который ранее был авторизован в системе самостоятельно с действующим паролем. Однако, в данное время банки применяют достаточные замысловатые системы авторизации, которые требуют введения различных кодов подтверждения действия. Но при некотором стечении обстоятельств они могут быть перехвачены, что даёт возможность злоумышленнику при необходимых обстоятельствах провести удачные транзакции, которые не были санкционированы. В большинстве случаев для данного действия применяются специальные вредоносные программы, которые функционируют на устройстве пользователя, и вмешиваются в работу клиента для содействия злоумышленнику. Для того, чтобы противодействовать таким устройствам, самым эффективным будет использование антивирусного программного обеспечения и применение квалифицированных сертификатов, которые будут генерироваться на внешнем устройстве[31].

3.1.2.1.Источник угрозы

Принято выделять несколько основных способов, благодаря которым злоумышленник может заполучить необходимые им данные, с помощью которых они смогут в дальнейшем совершать необходимые им противоправные действия:

Взлом и похищение баз данных у государственных структур, медицинских и образовательных учреждений или приобретение их у других хакеров.

Физическая кража документов, банковских карт или чеков.

Восстановление личных данных с жестких дисков и других электронных носителей информации, не подготовленных перед их утилизацией или продажей.

Кража или подделка отпечатков пальцев, голоса и прочих биометрических данных.

Получение информации из социальных сетей или других открытых источников, включая резюме на биржах по поиску работы.

Заражение устройств вредоносными программами для получения нужной информации разной степени конфиденциальности[32].

3.1.2.2.Анализ риска

В 2016 году было выявлено значительное число утечек данных, количество которых превышает прошлогодний показатель в двое. Согласно данным, последствием каждой утечки стала публикация более чем 10 миллионов персональных данных, суммарно на эти утечки пришлось 94,6% всех записей, подвергшихся компрометированию. Рекомендации, приведённые ниже, в состоянии понизить уровень риска:

- Сами беспокойтесь о сохранности своих персональных данных, не стоит заполнять подробные анкеты в учреждениях, не вызывающих доверия, или для участия в конкурсах.

- Сохранять копии своих важных документов.

- Иметь на всех своих устройствах антивирусное программное обеспечение и не забывать обновлять его, данная операция усложнит жизнь нарушителя и создаст дополнительные сложности по доступу к файлам на вашем устройстве.

- Пользоваться наиболее сложными паролями для доступа к любым учётным записям вне зависимости от их использования.

- Не стоит в социальных сетях указывать данные о вашем проживании и месте работы, личные фотографии, которые в состоянии вас скомпрометировать, любые данные, связанные с финансами (номера карт, щитов и т.д.), данные о вашем месте пребывания в свободное время и любую информацию, которая может содействовать взлому пароля.

В случае подозрения на то, что вы подверглись нападениям подобного рода, обратиться в соответствующие органы.

3.1.3.Взлом сайтов

Взлом веб-сайта банка. Так как онлайн-банк представляет собой ни что иное, как веб приложение, то в нём могут присутствовать уязвимости, которые дадут возможность при помощи внедрённых JavaScript или специализированных ссылок проводить различные манипуляции с приложением. Целью данной операции является использование данного приложения для своих целей, к примеру, навязывание различных транзакций или подмена одного счёта на другой, или же, возможно, даже полная блокировка интерфейса с целю требования выкупа. Если постараться избегать подозрительных сайтов и никогда не переходить по ссылкам из неизвестных источников, то можно избежать подобных проблем. Для банка же будет наиболее полезным проводить аудит кода и исправлять его и, желательно, особенно остро относиться к ошибкам нулевого дня[33].

3.1.4.Социальная инженерия (Social engineering)

Социальная инженерия. При подобном случае атаки основной акцент ставится не на специализированные программ, а в основном на самый уязвимый компонент любой системы – человеческий фактор. К примеру, были зарегистрированы случаи, когда для взлома злоумышленник выдавал себя за сотрудника ИТ-департамента банка и просил для проверки приложения провести якобы тестовые транзакции. При таком виде нападения не нужно даже оказывать влияние на работу банковского приложения – если сотрудник не был подготовлен к подобного рода манипуляциям, то он сам все сделает,

при этом не потребуется совершать абсолютно никаких манипуляций с приложением, что снижает уровень риска злоумышленника. Для успешных противодействий такого рода более эффективно - не доверять полномочия по управлению счетами одному человеку, а разделить их между рядом сотрудников, которые занимались бы подготовкой транзакций, проверкой их корректности и исполнением. При этом желательно, чтобы хотя бы один из них имел квалификацию в информационной безопасности[34].

3.1.5.DDoS-атаки

DDoS-атака. Злоумышленники могут вывести из строя онлайн-банк. Например, если удалить секретный ключ сертификата, то клиент не сможет подключиться к банку. Вывод из строя веб-сайта обычно используется для скрытия другой атаки, чтобы атакованный клиент не мог заметить воровства денег и не попытался заблокировать несанкционированную транзакцию. Поэтому, если веб-интерфейс оказался недоступен, то это повод попытаться проверить состояние своего счета другим способом, возможно, ваш клиент заблокирован специальным вредоносом.

Для разработки инновационного приложения, отвечающего всем нормам безопасности, необходимо чтобы он сочетал все или большинство компонентов защиты, как перечисленные выше, так и те, которые целесообразно использовать для защиты информации и обеспечения безопасности пользователя.

Для этого необходимо более подробно рассмотреть системы, максимально удовлетворяющие данным запросам[35].

3.2.Способы борьбы с выше перечисленными угрозами

3.2.1.Технология защиты от фишинговых атак

Ни одна из существующих технологий защиты от фишинговых атак не в состоянии предотвратить данную атаку, если её использовать в одиночку. Для того, чтобы борьба с данным типом атак была более действенной, нужно

применять многоуровневый подход, который может уменьшить количество атак и снизить ущерб в случае их осуществления. Для предотвращения данных атак необходимы технологии сетевой безопасности такие как: защита электронной почты и веб-ресурсов, защита от вредоносного ПО, отслеживание поведения пользователей и контроль доступа[36].

Для защиты от фишинговых атак следует реализовать многоуровневый подход, при котором предусматривается мониторинг веб-трафика и писем, приходящих из любой точки мира; также используются сложные фильтры веб-репутации и современные технологии проверки подлинности сообщений, приходящих по электронной почте.

Для этого следует создать сеть, подконтрольную предприятию, для выполнения постоянного мониторинга значительной части всего мирового почтового трафика и веб-трафика. С использованием информации об IP-адресах, что позволит отслеживать значительную часть критически важных параметров, так, например, если мониторить 30% трафика, станет возможным отследить более 150 параметров, например: объем письма при отправке и объем трафика с веб-сайта, уровни жалоб, параметры учета в «ловушках спама», разрешение имен DNS, страна происхождения и наличие в черном списке. Затем система использует полученные данные для определения показателя репутации, который указывает уровень угрозы для каждого письма, приходящего в организацию, а также URL-адреса, которые содержатся в каждом письме. Поскольку 90% вредоносных сообщений содержат URL-адреса, то ключевым компонентом для эффективного выявления и блокировки целенаправленных фишинговых атак продуктами IronPort является уникальная способность SenderBase отслеживать как веб-трафик, так и почтовый трафик[37].

3.2.1.1.Фильтры web-репутации.

Фильтры веб-репутации присваивают URL-адресам во всех письмах показатели репутации исходя из сходства каждого URL-адреса с вредоносным содержимым хост-сервера. Затем на основании этих показателей репутации

устройства, обеспечивающие безопасность электронной почты и веб-безопасность, могут разрешить, пометить флажком или заблокировать письма от определенных отправителей; аналогичным образом обрабатывается и трафик с определенных веб-сайтов[38].

Показатели репутации основаны на данных и результатах дополнительного анализа таких сведений об IP-адресе, которые трудно фальсифицировать, например, когда было зарегистрировано доменное имя, в какой стране расположен веб-сайт и (или) насколько часто меняется расположение, действительно ли домен, приписываемый компании Fortune 500, на самом деле принадлежит этой компании.

Создание такой технологии, которая базировалась бы не на дорогостоящем сетевом оборудовании, а на устройствах пользователей и серверах компании, несомненно бы оказывала существенное положительное влияние на вероятность попадания под фишинговую атаку.

Так, например,

Сеть SenderBase, с которой работают устройства Cisco IronPort, и фильтры репутации совместно блокируют 99% фишинговых писем. Однако, основным фактором для их эффективной работы является углубленный анализ IP-адресов и связанных с ними действий.

3.2.1.2.Проверка электронной почты с помощью SPF и DKIM.

На данный момент существуют системы, которые позволяют определить соответствуют ли идентификационные данные, заявленные в электронной почте, действительным данным пользователя, отправляющего сообщение.

SPF (Sender Policy Framework) и DKIM (DomainKeys Identified Mail) – наиболее часто используемые и взаимодополняющие методы проверки подлинности сообщений, которые пользователь получает по электронной почте. Данные способы дают возможность определять из всего числа сообщений сообщения, присланные злоумышленником[39].

3.2.1.3.Очистка HTML.

Очистка HTML (известная также как HTML-Convert или преобразование HTML) позволяет дать повышенную защиту письмам, которые соответствуют ранее определённым параметрам, к примеру, в случае, когда, SPF и DKIM не в состоянии определить подлинным является сообщение или нет. В случае, когда функция очистки HTML была применена, становится недоступной такая функция как переход по URL-адресам, и данный тип преобразуется в обыкновенный текст сообщения, в результате данной операции пользователь может увидеть скрытое потенциально опасное содержимое.

3.2.2.Способы защиты от Identity theft

Наиболее часто используются такие методы как:

Шифрование сессии SHA512, IP + USER_AGENT, ssl, а также возможно использовать VPN соединение для этих целей.

Так как IP + USER_AGENT использует для работы привязку к IP-адресу, это может создавать проблемы для мобильных пользователей и по этой причине он не будет рассматриваться для применения в рамках данного проекта[40].

3.2.2.1.SHA-512

SHA-512 – алгоритм хеширования, который является функцией криптографического алгоритма SHA-2.

SHA-512 очень близок к SHA-256, за исключением того, что он использует 1024 битные «блоки» и принимает в качестве входных данных длину строки длиной 2 ^ 128 бит. SHA-512 также имеет другие алгоритмические модификации по сравнению с SHA-256[41].

SHA-512 имеет структуру:

слова имеют длину 64 бита,

используется 80 раундов вместо 64,

сообщение разбито на чанки по 1024 бит,

начальные значения переменных и константы расширены до 64 бит,

постоянные для каждого из 80 раундов — 80 первых простых чисел,

сдвиг в операциях rotr и shr производится на другое число позиций.

Начальные значения переменных h0-h7 в SHA-512:

h0 := 0x6a09e667f3bcc908

h1 := 0xbb67ae8584caa73b

h2 := 0x3c6ef372fe94f82b

h3 := 0xa54ff53a5f1d36f1

h4 := 0x510e527fade682d1

h5 := 0x9b05688c2b3e6c1f

h6 := 0x1f83d9abfb41bd6b

h7 := 0x5be0cd19137e2179

SHA-2 (англ. Secure Hash Algorithm Version 2 — безопасный алгоритм хеширования, версия 2) — семейство криптографических алгоритмов — однонаправленных хеш-функций, включающее в себя алгоритмы SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224[42].

Хеш-функции предназначены для создания «отпечатков» или «дайджестов» для сообщений произвольной длины. Применяются в различных приложениях или компонентах, связанных с защитой информации.

3.2.2.2.TLS

TLS(1.3) (англ. transport layer security — Протокол защиты транспортного уровня), как и его предшественник SSL (англ. secure sockets layer — слой защищённых сокетов), — криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Протокол TLS широко применяется в приложениях, работа которых в большей степени связана с работой сети интернет, таких как веб-браузеры, работа с электронной почтой, обмен мгновенными сообщениями и IP-телефония (VoIP)[43].

Данный протокол был основан на спецификации SSL протокола версии 3.0, который был разработан компанией Netscape Communications. В настоящие время развитием данного протокола занимается IETF. Последняя версия протокола TLS создана в 2018 году и получила наименование TLS 1.3.

3.2.2.2.1.Безопасность

Протокол TLS обладает большим количеством мер безопасности:

1) Защита от перехода к предыдущей версии протокола, которая является менее защищённой, или перехода к менее надёжному алгоритму шифрования;
2) Нумерация последовательных записей приложения и использование порядкового номера в коде аутентификации сообщения (MAC);
3) Использование ключа в идентификаторе сообщения (только владелец ключа может сгенерировать код аутентификации сообщения). Алгоритм вычисления кода аутентификации (HMAC), используемый во многих сессиях TLS, определён в RFC 2104;

4) Сообщение, которым заканчивается подтверждение связи («Finished»), используется для подтверждения аутентичности ранее переданных сообщений и, таким образом, выбранных параметров TLS-соединения.

В протоколе TSL 1.0 ранее была уязвимость, считавшаяся теоретической. Но она была продемонстрирована на практике в 2011 году на конференции Ekoparty. В демонстрацию данной уязвимости входил процесс дешифровки cookies и использование результата для аутентификации пользователя[44].

В августе 2009 года была выявлена уязвимость в фазе возобновления соединения, которая давала возможность крипто аналитику, который способен взломать https соединение, добавлять собственные запросы в сообщения, которые были отправлены от клиента серверу. Из-за того, что крипто аналитик не в состоянии дешифровать переписку сервера и клиента, данный тип атаки имеет ряд отличий от стандартной атаки типа человек посередине. В том случае, когда пользователь игнорирует сообщение, выдаваемое браузером о том, что сессия не является защищённой, данная уязвимость может быть применена для уязвимости типа человек посередине. Для того, чтобы устранить данную уязвимость, было решено применить добавление информации о предыдущем соединении и проводить проверку в случае возобновления соединения. Данные изменения были представлены в стандарте RFC 5746, а также реализованы в последних версиях OpenSSL и других библиотеках.

3.2.2.3.VPN

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети

(например, Интернет). В независимости от того соединение осуществляется через сети с малым или неизвестным уровнем доверия, как, например, публичные сети, из-за применения средств криптографии таких, как: аутентификация, средства для защиты от повторов и изменения, передаваемых по логической сети сообщений, шифрования, инфраструктуры открытых ключей, уровень доверия к построенной логической системе не коим образом не связан с уровнем доверия к базовым сетям[45].

Сеть VPN в состоянии создавать соединения трёх различных видов:

- узел-узел,
- узел-сеть
- сеть-сеть.

Выбор типа соединения осуществляется на основании того, какие протоколы применяются в сети, и для чего она нужна.

3.2.2.3.1. Уровни реализации

В большинстве случаев развёртывание VPN осуществляется на уровнях не выше сетевого, что обосновывается тем, что это даёт возможность применять криптографию, при этом не изменяя протоколы транспортного уровня (такие как TCP, UDP)[46].

Для наибольшей защищённости соединения целесообразно будет разбить одну сессию на две однонаправленные сессии, протекающие в защищённом VPN соединении, в одном направлении которой будет применён SSL, а в противоположном SHA-512, что многократно затруднит подключение к данному соединению.

Так как атаки типа: взлом веб-сайта, социальная инженерия, DDoS-атака являются атаками, относящимся к атакам на сайты и серверные мощности предприятий, они не имеют отношения к приложениям, не будут рассматриваться.

Так как в исследованиях, проведённых компанией Positive Technologies, было выявлено, что такие технологии как WAF и SIEM окажут существенный положительный эффект на устойчивость предприятия перед кибератаками, их и расмотрим.

3.2.2.4SIEM

SIEM (Security information and event management) — объединение двух терминов, обозначающих область применения ПО: SIM (Security information management) — управление информационной безопасностью, и SEM (Security event management) — управление событиями безопасности.

Данная технология в состоянии проводить анализ угроз безопасности, причиной которых могут являться различные сетевые устройства и приложения, также она в состоянии реагировать на данные угрозы до момента, когда будет нанесён существенный ущерб[47].

По заявлению Gartner, SIEM-система должна собирать и представлять данные из сетевых устройств безопасности и заниматься анализом полученных ею данных. Для наилучшей работы в данную систему также должны быть включены следующие компоненты: инструменты управления уязвимостями, приложения для управления доступом и идентификацией, базы данных и приложений. Для наглядности можно привести в пример некоторые функции, которые е обычно входят в состав SIEM систем: Возможность отправки предупреждений на основе предопределенных настроек. Отчеты и логирование для упрощения аудита. Возможность просмотра данных на разных уровнях детализации[48].

Как правило, размер хранилища зависит от количества обрабатываемых событий в сети компании. Из лидеров мирового рынка SIEM можно выделить следующих:

HP ArcSight

IBM QRadar SIEM

Tibco Loglogic

McAfee NitroSecurity

RSA Envision

Splunk

LogRhythm

Есть и российские SIEM-системы:

MaxPatrol SIEM от Positive Technologies

КОМРАД от «НПО «Эшелон»

RUSIEM

3.2.2.4.1.SIEM в качестве улучшенной системы обнаружения вторжений.

Согласно мнению некоторых специалистов, SIEM является системой, предоставляющей улучшенные возможности по определению и выявлению системных аномалий и вредоносных активностей. Благодаря работе SIEM можно получить более полную систему того, какая активность происходит в сети и о событиях безопасности. В случае, когда обычные средства не в состоянии обнаружить атаку, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников. По данной причине значительная часть организаций отдают предпочтение SIEM-системам в качестве одного из наиболее важных элементов системы защиты и предотвращения целевых атак. И по этой же причине её использование в прочих средствах защиты будет наиболее предпочтительным[49].

3.2.2.4.2.Типовые сценарии использования SIEM-системы

Рассмотрим наиболее часто используемые сценарии, в которых применяется SIEM: Отслеживание аутентификации и обнаружение компрометации аккаунтов пользователей и администраторов. Отслеживание случаев заражения. Обнаружение вредоносных программ с использованием исходящих журналов брандмауэра и журналов веб-прокси, а также

внутренних журналов подключения и сетевых потоков. Мониторинг подозрительного исходящего трафика и передаваемых по сети данных с использованием журналов брандмауэра, журналов веб-прокси и NetFlow. Обнаружение кражи данных и других подозрительных внешних соединений. Отслеживание системных изменений и других административных действий во внутренних системах и их соответствия разрешенной политике. Отслеживание атак на веб-приложения и их последствий с использованием журналов веб-сервера, WAF (Web Application Firewall, экран для защиты веб-приложений) и логов приложений. Обнаружение попыток компрометации веб-приложений путем анализа разных отчетов.

3.2.2.5.Waf

Waf — это система для автоматизации сборки, то есть программа, которая производит автоматическую компиляцию и установку других программ и библиотек[50].

3.2.2.5.1.Возможности:

Файлы конфигурации представляют из себя ничто иное как сценарии, написанные на языке Python, что в свою очередь даёт возможность в полной мере использовать все возможности данного языка.

Встроенная поддержка C, C++, D, Java, Fortran и Qt. Возможность генерации документов TeX и LaTeX. Поддержка других языков или форматов файлов может быть реализована с помощью пользовательских расширений (tools).

Для языков C и C++ автоматически анализируются зависимости. В отличие от make не нужно отдельно выполнять команду make depend.

Обнаружение изменения содержимого файлов по контрольным суммам MD5, наряду с традиционным обнаружением изменений по времени записи файла.

Возможность параллельной сборки.

Встроенная возможность поиска необходимых для сборки файлов (#include файлы, библиотеки, и т. д.).

Способность кеширования собираемых файлов для ускорения сборки — подобно ccache, но для любых типов файлов.

Всё это делает возможным перенос возможностей данных устройств в виде программного кода на мобильные устройства в формате приложения или функций, дополняющих приложения.

Устройства, которые оснащены технологией WAF, характеризуются возможностью понимать группы протоколов и зависимостей, которые свойственны веб-приложениям, которые основываются на прикладных протоколах http и https. Технология WAF способна обеспечить DDoS-защиту и интегрируется с другими устройствами, снабжёнными той же технологией в ландшафте ИБ компании. Данная технология в состоянии протоколировать активность пользователя для того, чтобы в дальнейшем выявлять аномалии, что даёт возможность в дальнейшем предотвращать утечки данных.

Обычно WAF располагается в сети в режиме обратного прокси-сервера, перед защищаемыми веб-серверами. В зависимости от производителя могут поддерживаться и другие режимы работы — например, прозрачный прокси-сервер, мост или пассивный режим, когда продукт работает с копией трафика в режиме мониторинга. В данном случае это будет реализовано преимущественно через технологию VPN, что позволит перенести логическое расположение за защищённый периметр.

Следуя из того, что нужно, конкретному бизнесу возможно выбрать наиболее подходящий способ реализации технологии WAF: облачный сервис, агент на веб-сервере или специализированное аппаратное, или виртуальное устройство.

Также, кроме отдельных вирусов и подобных им программ, существуют и, так называемые, вредоносные приложения. Способ борьбы с данным видом угроз не отличим от алгоритма работы обычного антивируса.

В большинстве случаев, антивирусные программы проводят обнаружение вирусов за счёт использования сигнатур, которые представляют из себя подобие образцов вирусного кода, используя который, антивирусной программе удаётся определить вредоносный код в потоке данных, которые в это время загружаются приложением. Сигнатуры должны периодически обновляться от одного раза в неделю. Чем чаще это происходит, тем меньше вероятности того, что новая версия вируса сможет пройти.

По этой причине наиболее передовые антивирусные программы основываются преимущественно на облачных технологиях, принцип работы которых заключается в том, что программа обращается для определения вредоносного кода не только к базам данных, которые были вшиты изначально, но и к тем, что находятся непосредственно на серверах самого разработчика, на которые в свою очередь незамедлительно поступают сведения о новых вирусах и их сигнатурах.

Одним из обстоятельств, влияющих на выбор программы, обеспечивающих безопасность от вирусов, служит предоставление ей возможности защиты устройства в реальном времени. В основном данный вид защиты требуется при посещении веб-сайтов. Дополнительно стоит подчеркнуть, что с течением времени такая функция, как защита устройства в реальном времени, с каждым годом становится всё более актуальной и востребованной, причиной тому служит то, что всё большее количество

пользователей начинают пользоваться мобильными устройствам, а не стационарными персональными компьютерами.

Но, так как речь идёт не об антивирусе, а о программном обеспечении, которое позволяет безопасно обмениваться различными видами информации, то нет необходимости в постоянной работе всех его компонентов, что позволит, во-первых, своим функционалом заменить ряд приложений, что в свою очередь благотворно скажется на месте, занимаемом на устройстве, и сэкономить приличное количество пространства на мобильном устройстве[51].

3.2.3.Защита приложения от взлома и изменения

Одним из способов, которым злоумышленник может попробовать получит интересующие его данные, это изменение приложения, которое пользователь собирается установить или обновить. В следствии чего целесообразным будет применять средства для предотвращение этого.

3.2.3.1.Шифрование строк.

Это особенно полезно в том случае, если внутри приложения вы храните какие-либо сенситивные данные: идентификаторы, ключи, REST API endpoints. Все это поможет взломщику сориентироваться в твоем коде или вычленить из него важную информацию.

Зашифровать строки можно разными способами, например, используя инструменты Stringer или DexGuard. *Преимущество:* полностью автоматизированная модификация уже имеющегося кода с целью внедрения шифрования строк.

По итогу злоумышленник будет не в состоянии увидеть строки, подвергнутые шифрованию, после декомпилирования приложения. Но, разумеется, ему ничего не сможет помешать написать несложный дешифратор, базирующийся на алгоритме, полученном в результате декомпелирования твоего шифратора. Если сказать проще, то это не идеальное

решение проблемы, но оно в состоянии добавить трудности для злоумышленника, тем самым повысив уровень защиты.

Также возможно для защиты зайти ещё дальше, применив одни из ряда инструментов комплексной защиты, таким как к примеру, AppSolid. Данное решение не является бесплатным, но оно даёт возможность шифровать всё приложение целиком без исключений. Данный метод в состоянии отпугнуть большое число реверсеров, но существует набор инструментов, которые в состоянии этому противодействовать, в их числе Java-декомпилятор JEB, который также является платным, но он в состоянии снимать данную защиту в автоматическом режиме.

Также возможно попробовать разделить приложение на большое количество малых кусков кода. Данный метод не в состоянии обеспечить защиту, но он в состоянии хоть и небольшое время создать сложности в работе реверсера. Но он поможет обломать разнообразные автоматизированные системы, занимающиеся кракингом приложений. Им попросту будет невозможно определить, где им проводить поиск кода, находящегося в данном модуле.

Ну и последнее: из кода необходимо обязательно удалить (закомментировать) все обращения к логгеру, то есть все вызовы Log.d(), Log.v() и так далее. Иначе взломщик сможет использовать эту информацию, чтобы понять логику работы приложения.

Также для гарантирования того, что приложение в ходе установки и работы не было изменено намеренно или случайно, целесообразно будет применить сравнение MD5 ключа приложения и исходного хранящегося на сервере.

3.2.3.2.MD5

MD5 представляет собой алгоритм хеширования на 128-битной основе. Под хешированием подразумевается изменение входных данных, основываясь

на определённом алгоритме в битовую строку назначенной длины. При этом результат, который был получен, представляется в шестнадцатеричной системе исчисления. Её называют хешем, хеш-суммой или хеш-кодом[52].

Данный процесс получил широкое применение в веб индустрии и программировании. Как правило для создания уникальных значений в ассоциативных массивах, идентификаторов.

Область применения хеш-кодов:

Создание электронных подписей;

Хранение паролей в базах данных систем безопасности;

В рамках современной криптографии для создания уникальных ключей онлайн;

Проверка подлинности и целостности элементов файловой системы ПК.

MD5 был создан в 1991 году как стандарт хеширования для создания уникального хеш-кода от первоначального значения с функцией дальнейшей проверкой подлиности.

Утилита md5sum, предназначенная для хеширования данных заданного файла по алгоритму MD5, возвращает строку. Она состоит из 32 чисел в шестнадцатеричной системе исчисления (016f8e458c8f89ef75fa7a78265a0025).

Таким образом, хеш, который был получен от функции, принцип действия которой основывался на данном алгоритме, выдает строку в 16 байт (128) бит. И данная строка содержит в себе 16 шестнадцатеричных чисел. При этом, если изменения подвергнется хотя бы один её элемент, то это поведёт за собой непременное изменение всех остальных значений битов строки.

Вывод

Таким образом, если учесть самые актуальные уязвимости, то можно сделать вывод что:

1. При использовании Client/Server VPN можно снизит риск кражи данных во время передачи.

2. Для защиты от фишинговых атак есть смысл проверки файлов, которые автоматически скачиваются и, так как злонаправленные ссылки заранее не известны, есть смысл создания реестра подобных ссылок и блокировать их и ссылки на источники, чей адрес схож с лицензионным.

3. Принудительно перенаправлять пользователя в приложение, обеспечивающее безопасность, и не давать возможности пользоваться услугами без проверки достаточной защищённости ресурса.

4. Обеспечивать своевременное принудительное обновление критически важного софта через защищённые сети в кратчайшие сроки (с использованием WAF) для избежания подмены источника программы.

5. Использовать SIEM для анализа и сбора информации о сетевой и общей безопасности и дальнейшего использования.

6. Для обмена информацией, которая потенциально может заинтересовать злоумышленника, применять шифрование

Для повышения коммерческого потенциала технологии кроме применения технологий, которые были описаны, является также необходимым применить часть пунктов, выведенных выше, а именно: 1) провести оформление данной разработки как промышленного образца, что позволит получить исключительные права, а также получить правовую охрану в отношении данного изделия. 2) заниматься постоянным проведением работ по усовершенствованию продукта, чему способствует технология WAF. 3) также мониторить состояние рынка и по возможности занимать наиболее выгодные новые ниши.

Заключение

В настоящее время остро стоит проблема с конфиденциальностью данных и кибербезопасностью как частных, так и физических лиц, что может привести к существенным финансовым потерям. Вследствие этого проблема усовершенствования безопасности данных, как никогда, является актуальной. Из-за последних тенденций увеличения количества мобильных устройств и платформ они являются также целю злоумышленников и, как следствие, также нуждаются в дополнительной защите и тестировании безопасности всевозможных платформ и устройств. Вследствие чего была выбрана данная тема.

Для того, чтобы определить необходимость данного продукта, необходимо определить коммерческий потенциал продукта. Исходя из всего выше сказанного можно сделать вывод, что данный продукт является востребованным и необходимым для решения данной проблемы.

С технической точки зрения целесообразным будет применение технологии VPN соединения типа клиент – сервер, что позволит значительно снизить попытки проникновения 2-х пользователей в одну сессию и кражи паролей, тем самым увеличить защиту. Также проверка программной среды операционной системы и наличия защитного ПО, которое позволить увеличить отказоустойчивость операционной системы, на которую зачастую происходят нападения, для создания или использования критических уязвимостей, уже существующих в ней, которые могут привести к успешным попыткам злоумышленника.

Таким образом, разработка и внедрение инновационных средств защиты информации организации, например, банка и его клиентов, являются наиважнейшей задачей безопасности.

При использовании всех технологий, описанных выше, и делая акцент на параметры, влияющие на коммерческий потенциал, возможно создать

приложение по защите информации, обладающее наибольшим коммерческим потенциалом.

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. МИРОВОЙ РЫНОК МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДОСТИГ $76 МЛРД // Компьютерра [Электронный ресурс] Режим доступа: https://www.computerra.ru/233689/mirovoj-rynok-mobilnyh-prilozhenij-dostig-76-mlrd/ (дата обращения 25.12.2018).
2. Оборот рынка мобильных приложений достигнет к 2022 году 6,3 трлн долларов США // RETAIL & LOYALTY NEWS [Электронный ресурс] Режим доступа: https://www.retail-loyalty.org/news/oborot-rynka-mobilnykh-prilozheniy-dostignet-k-2022-godu-6-3-trln-dollarov-ssha/ (дата обращения 26.7.2017).
3. Мобильная коммерция «доведет» приложения до $6 трлн // РАЭК [Электронный ресурс] Режим доступа: https://raec.ru/live/member/9640/ (дата обращения 26.7.2017).
4. ПОДХОДЫ И МЕТОДЫ ОБОСНОВАНИЯ ЦЕЛЕСООБРАЗНОСТИ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ // Электронный научный журнал Современные проблемы науки и образования [Электронный ресурс] Режим доступа: https://www.science-education.ru/ru/article/view?id=9131 (дата обращения 13.05.2013).
5. Классификация угроз безопасности информации. Под угрозой безопасности информации понимается действие или событие, которое может привести к разрушению // Хелпикс [Электронный ресурс] Режим доступа: https://helpiks.org/5-59877.html (дата обращения 06.10.2015).
6. Анализ утечек информации в сети и их классификация // КиберПедия [Электронный ресурс] Режим доступа: https://cyberpedia.su/ (дата обращения.10.07.2016).
7. Потери от утечек данных // TADVISER [Электронный ресурс] Режим доступа: http://www.tadviser.ru/index.php/Статья:Потери_от_утечек_данных (дата обращения 16.03.2017).

8. Утечки информации: экономические эффекты // Корпоративный менеджмент [Электронный ресурс] Режим доступа: https://www.cfin.ru/appraisal/info_leakage.shtml (дата обращения 01.02.2011).
9. Утечки данных // TADVISER [Электронный ресурс] Режим доступа: http://www.tadviser.ru/index.php/Статья:Утечки_данных (дата обращения 13.05.2019).
10. Утечки информации в России // TADVISER [Электронный ресурс] Режим доступа: http://www.tadviser.ru/index.php/Статья:Утечки_информации_в_России (дата обращения 10.06.2019).
11. Оценка коммерческого потенциала интеллектуальной собственности // креативная экономика [Электронный ресурс] Режим доступа: https://creativeconomy.ru/lib/2926 (дата обращения 01.12.2008).
12. Ален К. Продвижение новых технологий на рынок. - М.: БИНОМ. Лаборатория знаний, 2007. - 455с.
13. Пестунов М.А. Управление интеллектуальной собственностью. - Челябинск. Изд-во ЧелГУ, 2006. - 409с.
14. Черкасова Е. Проблемы коммерциализации объектов промышленной собственности в военных вузах // ИС. Промышленная собственность. - 2003. - №2. - С.32-33.
15. Козырев А.Н., Макаров В.Л. Оценка стоимости нематериальных активов и интеллектуальной собственности. - М.: Интерреклама, 2003. - 352с.
16. Потенциал предприятия // Энциклопедия Экономиста! [Электронный ресурс] Режим доступа: http://www.grandars.ru/college/ekonomika-firmy/potencial-predpriyatiya.html (дата обращения 7.10.2017).
17. Факторы, определяющие коммерческий потенциал инноваций Социологические факторы оценки и выбора нововведений // uchebnik.online [Электронный ресурс] Режим доступа:

https://uchebnik.online/analiz-innovatsii/faktoryi-opredelyayuschie-kommercheskiy-69920.html (дата обращения 3.7.2016).

18. Научно-технический потенциал как ресурсный фактор инновационной деятельности // STUDME [Электронный ресурс] Режим доступа: https://studme.org/91179/investirovanie/nauchno-tehnicheskiy_potentsial_resursnyy_faktor_innovatsionnoy_deyatelnosti (дата обращения 15.6.2012).
19. Руководства по коммерциализации технологий // инновации и предпринимательство [Электронный ресурс] Режим доступа: http://www.innovbusiness.ru/content/document_r_7376082E-3B98-461C-8FEF-D5D58310B7CD.html (дата обращения 21.08.2017).
20. Оценка коммерческого потенциала (“коммерциализуемости”) технологий // Sinref [Электронный ресурс] Режим доступа: https://sinref.ru/000_uchebniki/00800economica/000_lekcii_menejment_02/413.htm (дата обращения 01.09.2018).
21. МЕТОДЫ ОЦЕНКИ КОММЕРЧЕСКОГО ПОТЕНЦИАЛА ИНТЕЛЛЕКТУАЛЬНОГО ПРОДУКТА // Экономическая библиотека [Электронный ресурс] Режим доступа: http://economy-lib.com/metody-otsenki-kommercheskogo-potentsiala-intellektualnogo-produkta (дата обращения 27.10.2005).
22. СОПРОТИВЛЕНИЕ ОРГАНИЗАЦИОННЫМ ИННОВАЦИЯМ: МЕТОДОЛОГИЯ СОЦИОЛОГИЧЕСКОГО ИССЛЕДОВАНИЯ // Ecsocman [Электронный ресурс] Режим доступа: http://ecsocman.hse.ru/data/2010/12/05/1214827265/5cSherbakova.pdf (дата обращения 05.12.2010).
23. Метод экстраполяции // Studfiles [Электронный ресурс] Режим доступа: https://studfiles.net/preview/8031508/page:2/ (дата обращения 01.06.2019).
24. МЕТОДЫ ОЦЕНКИ КОММЕРЧЕСКОГО ПОТЕНЦИАЛА ТЕХНОЛОГИЙ // Economy24info [Электронный ресурс] Режим доступа:

https://economy24info.com/innovatsionnaya-ekonomika-rf/metodyi-otsenki-kommercheskogo-potentsiala-60872.html (дата обращения 17.04.2014).

25. Потери банков от киберпреступности // TADVISER [Электронный ресурс] Режим доступа: http://www.tadviser.ru/index.php/Статья:Потери_банков_от_киберпреступности (дата обращения 20.05.2019).
26. День простоя из-за кибератаки может обойтись банку в 50 млн рублей // Positive Technologies [Электронный ресурс] Режим доступа: https://www.ptsecurity.com/ru-ru/about/news/den-prostoya-iz-za-kiberataki-mozhet-obojtis-banku-v-50-mln-rublej/ (дата обращения 28.12.2019).
27. СКОЛЬКО СТОИТ БЕЗОПАСНОСТЬ // Positive Technologies [Электронный ресурс] Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf (дата обращения 11.02.2017).
28. ЦБ назвал ущерб российских банков от кибератак в 2018 году // РБК [Электронный ресурс] Режим доступа: https://www.rbc.ru/rbcfreenews/5bc881ea9a7947189fe00a9a (дата обращения 18.10.2018).
29. Фишинг // Википедия [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3 (дата обращения 01.02.2019).
30. Фишинг // Avast [Электронный ресурс] Режим доступа: https://www.avast.ru/c-phishing (дата обращения 08.05.2019).
31. Кража личности // Википедия [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B0%D0%B6%D0%B0_%D0%BB%D0%B8%D1%87%D0%BD%D0%BE%D1%81%D1%82%D0%B8 (дата обращения 04.05.2019).
32. Кража личности // Securitylab [Электронный ресурс] Режим доступа: https://www.securitylab.ru/news/tags/%EA%F0%E0%E6%E0+%EB%E8%F7%ED%EE%F1%F2%E8/ (дата обращения 14.11.2018).

33. Взлом сайта и его последствия // Habr [Электронный ресурс] Режим доступа: https://habr.com/ru/post/262579/ (дата обращения 14.07.2015).
34. Социальная инженерия // Википедия [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F (дата обращения 15.03.2019).
35. DDoS-атака // ddos-guard [Электронный ресурс] Режим доступа: https://ddos-guard.net/ru/terminology/attacks/ddos-ataka (дата обращения 05.10.2016).
36. Как защититься от фишинга // Kaspersky [Электронный ресурс] Режим доступа: https://www.kaspersky.ru/blog/phishing-ten-tips/9744/ (дата обращения 13.11.2015).
37. Целевой фишинг // БЕСПЛАТНАЯ ИНТЕРНЕТ БИБЛИОТЕКА [Электронный ресурс] Режим доступа: http://lib.knigi-x.ru/23raznoe/271163-1-oficialniy-dokument-celevoy-fishing-elektronnaya-pochta-eto-kommunikacionnaya-sreda-kotoruyu-ispolzuet-bolshinstvo-organi.php (дата обращения 30.03.2012).
38. Web репутация Cisco IronPort // cisco [Электронный ресурс] Режим доступа: https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/Web_Reputation.pdf (дата обращения 18.05.2017).
39. Настройка DKIM/SPF/DMARC записей или защищаемся от спуфинга // habr [Электронный ресурс] Режим доступа: https://habr.com/ru/post/322616/ (дата обращения 26.02.2017).
40. Кража личности (Identity theft) // anti-malware [Электронный ресурс] Режим доступа: https://www.anti-malware.ru/threats/identity-theft (дата обращения 22.06.2014).

41. SHA-512 // bitcoinwiki [Электронный ресурс] Режим доступа: https://ru.bitcoinwiki.org/wiki/SHA-512 (дата обращения 26.10.2018).
42. SHA-2 // Википедия [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/SHA-2 (дата обращения 10.04.2019).
43. TLS // Википедия [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/TLS (дата обращения 26.05.2019).
44. Что такое TLS // habr [Электронный ресурс] Режим доступа: https://habr.com/ru/post/258285/ (дата обращения 19.05.2015).
45. VPN // Википедия [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/VPN (дата обращения 04.06.2019).
46. Каналы связи L2 и L3 VPN — Отличия физических и виртуальных каналов разного уровня // habr [Электронный ресурс] Режим доступа: https://habr.com/ru/post/354408/ (дата обращения 26.04.2018).
47. SIEM // Википедия [Электронный ресурс] Режим доступа: http://ru.wikipedia.org/wiki/SIEM (дата обращения 13.05.2019).
48. Что такое SIEM-системы и для чего они нужны? // anti-malware [Электронный ресурс] Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/Popular-SIEM-Starter-Use-Cases (дата обращения 30.06.2017).
49. Обзор мирового и российского рынка SIEM-систем // anti-malware [Электронный ресурс] Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem (дата обращения 23.08.2013).
50. Waf // Википедия [Электронный ресурс] Режим доступа: http://ru.wikipedia.org/wiki/Waf (дата обращения 22.10.2018).
51. Чем защищают сайты, или зачем нужен WAF // habr [Электронный ресурс] Режим доступа: https://habr.com/ru/company/pt/blog/269165/ (дата обращения 20.10.2015).
52. MD5 // Википедия [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/MD5 (дата обращения 19.04.2019).