Екатерина Сергеевна ЛЕБЕДЕВА

кандидат экономических наук, доцент, доцент кафедры экономической экспертизы и финансового мониторинга МИРЭА — Российского технологического университета, г. Москва, katmail79@mail.ru

Карина Эдуардовна ШАГАЛИНА

студентка специальности «Экономическая безопасность» МИРЭА — Российского технологического университета, г. Москва, karinashagalina11@gmail.com

НЕМАТЕРИАЛЬНЫЕ АКТИВЫ ПРЕДПРИЯТИЯ: КАК УЧИТЫВАТЬ И КАК ЗАЩИТИТЬ

Аннотация. Интенсивные кибератаки, особенно в 2022 г., арест США активов Центрального Банка РФ, «слив» базы данных клиентов Яндекс Еда, уход ИТ-компаний и программного обеспечения с российского рынка — все это оказывает влияние на экономическую безопасность предприятий. Перед предприятиями встает вопрос: «Как защитить свой бизнес в текущих условиях?». Если организация владеет нематериальными активами, важно знать, как их учитывать и как защитить свое права собственности на такой объект с целью обеспечения своей экономической безопасности. Данная статья посвящена изучению данного вопроса.

Ключевые слова: нематериальные активы, интеллектуальная собственность, кибербезопасность, кибератака.

Ekaterina Sergeevna LEBEDEVA

Candidate of Economic Sciences, Associate Professor of the Department of Economic Expertise and Financial Monitoring of RTU MIREA, Moscow, katmail79@mail.ru

Karina Eduardovna SHAGALINA

Student of the specialty "Economic security" RTU MIREA, Moscow, karinashagalina11@gmail.com

INTANGIBLE ASSETS OF THE ENTERPRISE: HOW TO ACCOUNT FOR AND HOW TO PROTECT

Abstract. A cyberattack by the country's largest marketplace, the US seizure of the assets of the Central Bank of the Russian Federation, the "drain" of the Yandex Food customer database, the withdrawal of IT companies and software from the Russian market — what does this mean for economic security and how to protect your business in modern realities? If an organization owns intangible assets, it is important to know how to account for them and how to protect its ownership rights to such an object. This article is devoted to the study of this issue.

Keywords: intangible assets, intellectual property, cybersecurity, cyberattack.

В экономическом и цифровом пространстве в настоящее время происходят глобальные изменения точки зрения осознания ценностей владения цифровыми технологиями организациями и государством с целью обеспечения экономической безопасности как организаций, так и страны.

Рассмотрим такой вид актива организации как нематериальный актив (НМА), который с точки зрения ведения бухгалтерского учета относится к внеоборотным активам.

В бухгалтерском учете учет НМА регулирует ПБУ 14/2007 «Учет нематериальных активов». Главное отличие НМА от других видом имущества — это отсутствие материально-вещественной формы.

В составе НМА при определенных условиях можно учесть объекты интеллектуальной собственности (или результаты интеллектуальной деятельности). На рисунке 1 приведены такие объекты.

Рис. 1. Виды объектов интеллектуальной собственности

Источник: составлено авторами.

ПБУ 14/200 предусматривает также отнесения к НМА деловой репутации организации [1].

Следует отметить, что никаких стоимостных ограничений при признании объектом в составе нематериальных активов в бухгалтерском учете не существует, однако для целей ведения налогового учета объект относится к амортизируемому имуществу, в том числе и нематериальному, если его стоимость превышает сто тысяч рублей.

Объект интеллектуальной собственности можно учесть в составе нематериальных активов при одновременном выполнении определенных условий, которые приведены на рисунке 2

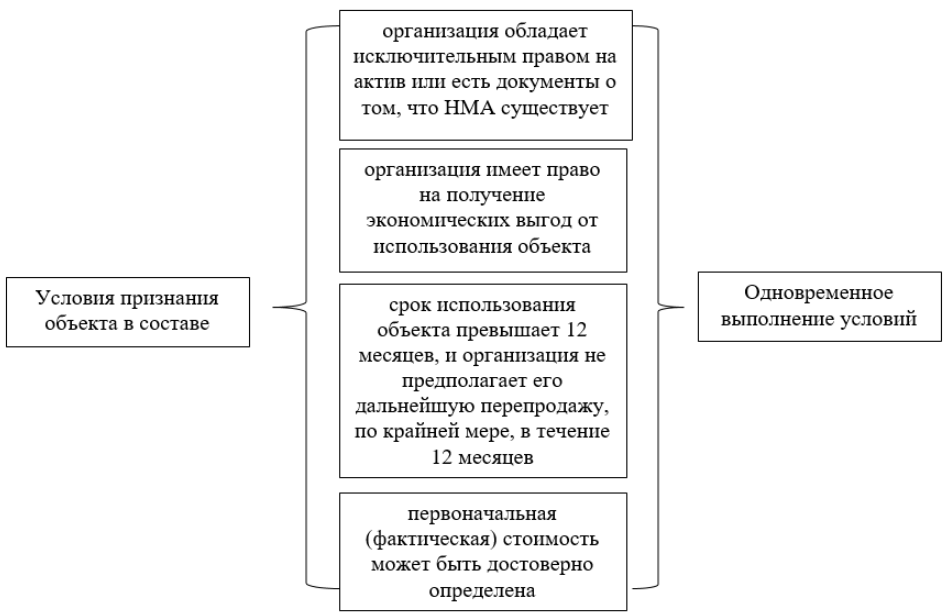

Рис. 2. Условия признания объектов в составе НМА

Источник: составлено авторами по данным [2].

При невыполнении хотя бы одного условия, указанного на рисунке 2, стоимость имущества учитывают в составе:

– расходов на научно-исследовательские, опытно-конструкторские и технологические работы (НИОКР);

– расходов будущих периодов;

– текущих расходов [3].

При создании НМА собственными силами организации, необходимо подтвердить исключительные права на данный актив документально.

Многие объекты интеллектуальной деятельности должны быть зарегистрированы в Роспатенте или в Госкомиссии по испытанию и охране селекционных достижений. Тогда документами, подтверждающими исключительные права на созданный объект, являются:

– свидетельство на товарный знак (знак обслуживания) (ст. 1480 и 1481 ГК);

– свидетельство об исключительном праве на наименование места происхождения товара (п. 2 ст. 1518 и ст. 1530 ГК);

– патент на изобретение, промышленный образец, полезную модель (ст. 1353 и 1354 ГК);

– патент на селекционное достижение (ст. 1414 и 1415 ГК) [4].

Если организация получила необходимые охранные документы, созданный объект интеллектуальной собственности можно учесть в составе НМА. Некоторые объекты интеллектуальной собственности регистрируются в добровольном порядке, например, исключительное право на компьютерную программу (ст. 1262 ГК) [4].

Таким образом, интеллектуальная собственность — это нематериальный актив, который несет в себе ценную информацию или право обладания ею, способный приносить экономическую выгоду хозяйствующему субъекту в течение определенного периода времени.

Интеллектуальная собственность (ИС) невещественный актив, который находится в информационном пространстве. В частности, речь идет об облачных моделях и их информационной безопасности. Около двух лет назад в период пандемии компании были вынуждены задействовать облака и аутсорсинг, что придает значимость работы с ИС. Сейчас это различные хранилища данных, которые помещены в нематериальное пространство и имеют свои способы функционирования и взаимодействия между пользователями [2].

Для идентификации и защиты ИС применяют различие правовые меры, которые не всегда обеспечивают сохранность доступа к такой экономически значимой информации. Введение режима коммерческой тайны, товарные знаки и патентирование дает лишь право на определение последствий и ответственности в следствии хищения информации на законодательном уровне, но не дает гарантий на обеспечение безопасности и реальной конфиденциальности доступа к такой собственности. В действительности представляется важными обеспечение информационной безопасности хозяйствующего субъекта — состояние информационной системы субъекта, способствующее реализации его экономических интересов в материальном и цифровом пространстве.

«Вся ваша коммерчески значимая информация — теперь не только ваша. Ее обладатель в любой момент может потерять к ней доступ до лучших времен или она просто будет стерта» [5].

В декабре 2021 г. на VII SOS-Форуме, организованном ФСБ России и ФСТЭК России в партнерстве в «Ростелкком-Солар» лидеры экономического сообщества подтвердили данное высказывание.

На данный момент кибербезопасность считается уязвимой точкой развития в сфере технологий. По мнению экспертов, последние 1,5 года ускорился процесс внедрения цифровых технологий во всех сферах жизни человека. Киберпезопасность в то же время развивалась более замедленно и равномерно, однако любые нововведения требуют дополнительных мер защиты. Ситуация развивается таким образом, что с появлением новых форм появляются недоработанные участки, следовательно, это ведет к риску киберугроз.

Например, для эффективной цифровизации компании все чаще используют облачную модель и аутсорсинг ИТ и ИБ. Но облака сильно изменили баланс ответственности за безопасность. Или другой быстро развивающийся тренд — атаки через подрядчиков: по сути, у компаний сейчас нет возможности ни проверить защищенность аутсорсеров, ни разделить с ними ответственность в случае киберинцидента.

Уже сейчас очевидно, что запрос на экспертизу и в части технологий, и в части сотрудников SOC вырос существенно, что создает потребность всерьез пересматривать ландшафт создаваемых ранее экосистем безопасности.

Таким образом, необходимо более детально рассмотреть понятие кибербезопасности и киберугроз.

Понятие кибербезопасность включает в себя защиту сетей, компьютеров, софта и самих данных. Защита от кибератак заключается как в налаженной работе антивирусных программ и исключении уязвимостей в системах, так и во взаимодействии людей. Основная цель защиты информации: предотвратить или снизить риски кибератак, исключить утечки или повреждение данных, а также минимизировать сбои в работе систем.

Кибератаки проводят для незаконного доступа к устройству, сети, инфраструктуре. Они ведут к потере конфиденциальной информации, хищению денежных средств, нарушению бизнес-процессов и, в итоге, к репутационному и прямому финансовому ущербу.

Критические проблемы кибербезопасности приведены на рисунке 3.

Самые распространенные существующие виды кибератак:

1. Вредоносное программное обеспечение (Malware) получает доступ к информационной системе без разрешения пользователя. Это группа программ-вымогателей, также называемых шифровальщиками вирусов, троянов, червей и иных шпионских рекламных программ.

2. Программы-вымогатели предлагают пользователю заплатить определенную сумму, шантажируя его потерей определенный файлов или элементов системы. Доступ к данным может быть не восстановлен даже после перечисления суммы, так как программа не дает никаких гарантий.

3. Социальная инженерия — мошенническая схема, предлагающая пользователю за определенную сумму приобрести доступ к конфиденциальной информации. Обманным путем киберпреступники получают данные пользователей, не давая никаких гарантий раскрытия информации.

4. Фишинг — письмо или набор текста, ссылка, в основном распространяется через электронную почту, массовые рассылки или социальные сети и мессенджеры. Переход на которые влечет за собой утечку конфиденциальных данных: логинов, паролей, номеров и кодов банковских карт [6].

Рис. 3. Критические проблемы кибербезопасности

Источник: составлено авторами.

Технологии обеспечения кибербезопасности приходится задействовать в разных сферах деятельности, так как необходимо защищать секретные сведения. С каждым годом попытки кражи данных злоумышленниками увеличивается во всем мире. Это устойчивая тенденция. В отчете RiskBased Security приводятся шокирующие сведения: за 9 месяцев 2019 г. зафиксированное число утечек информации приблизилось к 8 млрд случаев, что на 112% больше по сравнению с аналогичным периодом предыдущего года [6].

В основном хакеры заинтересованы в атаках ритейлерских коммерческих организаций, однако лидерами являются компании государственного сектора, в частности медицинские. Злоумышленники имеют личные интересы в отношении баз данных и добытых сведений, это дает возможность их реализации в преступных и неправомерных методах конкуренции.

В последние месяцы все острее становится вопрос о защите собственности организаций в информационном пространстве в связи с уходом большинства ИТ-компаний и информационного обеспечения с российского рынка. Потеря ИТ- поддержки пришлась на такие зарубежные компании, как Microsoft, Adobe, DXC Technology, Oracle, Forcepoint, Fortinet, Mikrotik, Lenovo, Samsung, Dell, Spotify, HP и Cisco [7].

Для пользователей уход с рынка приведет к серьезным проблемам с кибербезопасностью, поскольку перестанет работать исправление и обновление программного обеспечения, а также заблокируются все подписки. Судя по текущей ситуации, обновления для российского рынка выпускаться не будут, что, скорее всего, подстегнет пиратство. Более того, рынок в реальном времени может наблюдать за совершением хакерских атак. По данным новостных порталов 1 марта 2022 г. компания «Яндекс Еда» сообщила об утечке данных пользователей — телефонов клиентов и информации о заказах, времени доставки, адресов и других. Архив с тремя SQL-дампами, суммарно содержащими 49 441 507 строк с заказами, включая данные:

- имена и фамилии клиентов, как они записаны в профиле пользователя;
- номера телефонов из РФ (6 882 230), Казахстана и Беларуси (206 725);
- полный адрес доставки клиента;
- комментарии к заказу;
- даты заказов с 19.06.2021 по 04.02.2022 [8].

Кибератаке средней мощности подвергся крупнейший торговый маркетплейс Wildberries. 16 марта 2022 г. началось внутреннее расследование сбоя в работе сервисов. По информации Forbes часть сервисов выведена из строя. Однако злоумышленники не получили данные пользователей, а данные систем украдены с возможностью восстановления. Начальник отдела информационной безопасности Андрей Дрозд из «СёрчИнформ» обозначает данный случай как один из масштабных показательных инцидентов кибератак. По его мнению, серьезно пострадала именно внутренняя система безопасности маркетплейса, остальные аспекты можно определить только по косвенным признакам [9].

Таким образом обеспечение кибербезопасности актуально для направлений работы с базами данных:

1. Компьютерных сетей.
2. Приложений для мобильных устройств.
3. Личная и коммерческая информация.
4. Операционная безопасность.
5. Аварийное восстановление.
6. Подготовка пользователей в области обеспечения кибербезопасности.

Необходимо рассмотреть альтернативные варианты ПО, так как западные IT-сервисы в текущих условиях несут киберопасность. В моменты нестабильности увеличивается количество хакерских атак и внедрение вредоносных программ, а уровень защиты не справляется. В Едином реестре российского ПО существуют аккредитованные IT-сервисы, служащие достойной заменой зарубежным системам. За новизну и актуальность содержащихся данных несет ответственность Министерство цифрового развития.

В пример можно привести систему «Первая форма», содержащуюся в обои реестрах. Она так же эффективно справляется с бизнес-задачами, с ее помощью организуются видеоконференции, общение в мессенджерах, организуется контроль деятельности сотрудников, процесс управления проектами. автоматизация бизнес-процессов, а также другие важные организационные элементы.

При размещении данных на серверах заказчика, а также облачных ресурсов российских разработчиков можно быть уверенным в сохранении информации, вне зависимости от политической обстановки. Так как нет никаких влияний и решений менеджеров зарубежных IT-компаний. Клиентами «Первой формы» можно считать — «ВкусВилл», Спортмастер, «Сколково», ПАО «Банк Уралсиб», Страховой Дом ВСК и десятки других компаний. «Первая форма» входит в топ-10 российских разработчиков BPM-систем по версии TAdviser [5].

На данный момент единственной возможностью обезопасить конфиденциальную и коммерчески значимую информацию компаний можно только с переходом на российское ПО.

Таким образом в мерах по защите от киберугроз можно выделить три элемента:

1. Персонал компании.
2. Инструменты обеспечения безопасности нуждающихся в защите устройств.
3. Выстроенный процесс защиты информационной среды.

Таким образом, проблема кибербезопасности активов является чрезвычайно актуальной. От рисков не застрахованы не только обычные пользователи, но и все субъекты экономики. С каждым годом случаи киберпреступности возрастают. Это требует постоянного развития и разработки методов защиты. Для того, чтобы сократить утечку и кражу приватных данных каждому члену сообщества необходимо идти в ногу с технологическим прогрессом, внедряя инновационные технологии защиты информационного пространства. Если не находить выходы из сложившейся ситуации, и не опережать киберпреступников в внедрении и использовании методов защиты, можно столкнуться с наихудшими последствиями. Это может нанести серьезный ущерб экономическому сектору российского рынка, а в глобальном смысле всему обществу.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Об утверждении Положения по бухгалтерскому учету «Учет нематериальных активов» (ПБУ 14/2007): Приказ Минфина России от 27.12.2007 № 153н (ред. от 16.05.2016) // КонсультантПлюс: надежная правовая поддержка: [официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_63465/adf2cfd636e9e799777ca5e7c8add8b722dced71/ (дата обращения: 05.04.2022).
2. Попова Е.Ю. Что относится к нематериальным активам. // Система Главбух: [сайт] [дата публ. 01.01.2019]. URL: https://www.1gl.ru/#/document/16/58138/bssPhr46/?of=copy-9c173aab12/ (дата обращения: 05.04.2022).
3. Разгулин С.В. Как оформить и учесть приобретение компьютерной программы. // Система Главбух: [сайт] [дата публ. 01.01.2021]. URL: https://www.1gl.ru/#/document/16/71963/bssPhr2/?of=copy-79817e0c80/ (дата обращения: 05.04.2022).
4. Гражданский Кодекс Российской Федерации? Часть третья, принят Государственной Думой 1 ноября 2001 г. // КонсультантПлюс: надежная правовая поддержка:

[официальный сайт]. 1997-2022. URL: http://www.consultant.ru/document/cons_doc_LAW_34154/ (дата обращения: 06.04.2022).
5. Западные ИТ-компании уходят из России. Отечественный аналог Zoom, Jira и Slack. Сколько времени нужно для перехода // [сайт] [дата публ. 31.03.2022]. URL: https://vc.ru/u/1122982-pervaya-forma/391903-zapadnye-it-kompanii-uhodyat-iz-rossii-otechestvennyy-analog-zoom-jira-i-slack-skolko-vremeni-nuzhno-dlya-perehoda/ (дата обращения: 12.04.2022).
6. Что такое кибербезопасность: основные угрозы // GeekBrains [сайт] [дата публ. 05.12.2021]. URL: https://gb.ru/blog/cto-takoe-kiberbezopasnost / (дата обращения: 12.04.2022).
7. SOC-Форум 2021 — кибербезопасность по-новому // Коммерсант [сайт] [дата публ. 08.12.2021]. URL: https://www.kommersant.ru/doc/5118384/ (дата обращения: 12.04.2022).
8. В сети опубликовали карту с данными клиентов «Яндекс.Еды» — именами, номерами и тратами за полгода // VC.RU [сайт] [дата публ. 22.03.2022]. URL: https://vc.ru/food/385375-v-seti-opublikovali-kartu-s-dannymi-klientov-yandeks-edy-imenami-nomerami-i-tratami-za-polgoda/ (дата обращения: 12.04.2022).
9. Кибератака или инсайдер: почему произошел сбой в работе Wildberries // Forbes [сайт] [дата публ. 19.22.2022]. URL: https://www.forbes.ru/biznes/459557-kiberataka-ili-insajder-pocemu-proizosel-sboj-v-rabote-wildberries/ (дата обращения: 14.04.2022).