Артамонов В.А.
д.т.н., профессор, академик Международной академии информационных технологий, Минск
artamonov@itzashita.ru
Артамонова Е.В.
к.т.н. (PhD), Минск
admin@itzashita.ru
Васильев А.В.
ScienceSoft, г. Минск
alexey_vasilyev96@mail.ru

ЭКОНОМИКА КИБЕРБЕЗОПАСНОСТИ

Ключевые слова: *кибербезопасность, киберпреступность, защита информации, подпольная экономика, здравоохранение, медицинская информация.*
Keywords: *cybersecurity, cybercrime, information protection, underground economy, healthcare, medical information.*

Введение

Современный мир сталкивается с возрастающей распространенностью все более сложных, целенаправленных и злонамеренных кибератак. Эта новая реальность заставляет нас постоянно совершенствовать существующее понимание о киберокружении, переоценивать и обновлять наши представления в области безопасности таким образом, чтобы минимизировать растущие риски для бизнеса, объектов инфраструктуры и нас самих. При этом мы должны признать, что комплексная стратегия кибербезопасности включает в себя не только технические средства. Она также должна включать в себя аспекты, связанные с корпоративным менеджментом, общественной и корпоративной культурой и охватывать более крупные экономические и даже социо-политические элементы (например, национальную безопасность).

Ежегодные глобальные затраты на кибербезопасность приближаются к отметке в $100 миллиардов, в то время как глобальные убытки для бизнеса из-за киберинцидентов приближаются к $1 триллиону.[1] Несомненно, что бизнес недоинвестирует область безопасности, но действительно ли необходимо потратить $1 триллион, чтобы избежать убытков на сумму в $1 триллион? Истина, вероятно, находится где-то посередине, и правильный подход может заключаться не только в увеличении затрат, но и в их более эффективном использовании и грамотном планировании. Это открывает перед бизнесом и обществом более обширный вопрос об «экономике кибербезопасности», который, в свою очередь, распадается на три основных темы:

1) Киберпреступность и подпольная экономика. Что представляет собой реальная подпольная торговая площадка, и как финансово мотивированные киберпреступники на самом деле зарабатывают деньги? Как функционирует хакерская экономика, как происходит «товарооборот» в теневой киберэкономике? Кто является акторами теневой экономики в кибермире, и какова их мотивация?

2) Экономика кибербезопасности. Как воздействуют киберугрозы на бизнес и общество? Сколько бизнес инвестирует в кибербезопасность, какие есть последствия (или риски финансовых потерь) для бизнеса, общества и отдельных лиц? Каким образом оцениваются фактические и потенциальные финансовые потери от последствий кибератак? Какие существуют математические модели и экономические методики для расчета затрат на кибербезопасность? Как применяются методы оценки рисков и положения международных и национальных стандартов в практике департаментов кибербезопасности на предприятиях? Какие есть методики расчета затрат на кибербезопасность?

3) Принятие бизнес-решений. Как руководитель компании может убедиться, что в его бизнесе достаточно инвестируется средств в кибербезопасность? Как оценить фактические риски и выработать меры по их снижению (или устранению)? Каков правильный уровень бюджетирования, технологий, квалификации персонала и страхования от киберрисков? И как обосновать инвестиции в кибербезопасность, когда затраты крайне непрозрачны, а быстрый экономический результат показать не получается?

Основная цель данной статьи – понять существующие риски в области безопасности, а также разобраться в самой экономике кибербезопасности. Понимание принципов функционирования подпольной экономики, оценка потенциальных финансовых последствий от киберугроз, роль топ-менеджмента в вопросах кибербезопасности – все это ключевые факторы для минимизации возможного вреда от киберугроз.

---

[1] FAIR Institute Blog. Cyber Economics: Smarter (vs. More Expensive) Cybersecurity. 2017. – May 30. – www.fairinstitute.org/blog/cyber-economics-smarter-vs-more-expensive-cybersecurity

Как один из примеров оценки последствий киберугроз в отрасли, в статье описывается ситуация с утечками крайне ценной медицинской информации (PHI – protected health information) и относительно высокой уязвимости IT-систем в медицинских учреждениях.

Оценка роли подпольной киберэкономики

Для понимания масштабов подпольной киберэкономики можно обратить внимание на базовые показатели по суммарному количеству созданных вредоносных программ за год. В 2008 году было создано более 1 миллиона вирусов за год. Это число выросло до более 1 миллиона в день к 2016 году.[1] Производство вредоносных программ теперь ведется как настоящих и продуманный бизнес, который включает в себя инструменты для создания, тестирования, обфускации, доставки и управления вредоносных программ. По сути дела, создана целая подпольная индустрия со своими бизнес-потоками и даже маркетингом.

Огромный объем вредоносных программ, а также современные возможности, позволяющие нацеливаться на конкретные приложения отдельно взятой организации, стали новым и крайне серьезным вызовом для большого количества компаний по всему миру. Несмотря на то, что операционные системы Windows и Android являются наиболее распространенными и привлекают больше всего внимания, любая другая операционная система, программное обеспечение баз данных, приложение, экосистема программных продуктов или платформа веб-сайтов могут стать потенциальными целями для кибератаки.

В дополнение к вредоносным программам, подпольная экономика включает в себя рынок всего ценного для продажи: информацию (например, украденные персональные данные, интеллектуальную собственность), инструменты и сами услуги хакеров, уязвимости (особенно ценные и дорогостоящие уязвимости «нулевого дня»[2]), услуги хостинга для атак, распределенные атаки для отказа в обслуживании и услуги, предоставляемые наемными хакерами (то есть киберпреступления как услуга [CaaS][3]).

CaaS кардинально изменил подпольную экономику и киберпреступность. Сегодня любой злонамеренный человек с деньгами, независимо от мотивации, может нанять «умного парня» или воспользоваться готовым пакетом инструментов для осуществления кибератаки.

Также необходимо отметить и такие «подпольные услуги», как покупка-продажа инсайдерской информации в сети Даркнет. Организации сталкиваются с беспрецедентными рисками со стороны инсайдеров – сотрудников и подрядчиков, имеющих действительный доступ в корпоративные сети. Инсайдерский риск растет отчасти из-за растущего влияния Даркнета, теневой части Интернета. Даркнет все чаще используется киберпреступниками для вербовки инсайдеров с целью кражи данных. Этот процесс помогает совершать незаконную торговлю или иным образом получать прибыль от инсайдерской информации. Используя инсайдерскую информацию, злоумышленник пытается получить прибыль с более правильными ставками на фондовом рынке. В результате, инсайдер получает комиссию. Даркнет способствует незаконной торговой деятельности, обеспечивая анонимность, что затрудняет идентификацию участников.

Форумы инсайдерской торговли, которые исследованы в отчете RedOwl и IntSights[4], были эксклюзивными. Похоже, что самая мощная информация и опытные участники теневого рынка находятся в закрытых небольших группах. Эти группы требуют определенной проверки лояльности от потенциальных участников, которые подают заявку на членство, чтобы доказать свои способности и/или доступ к знаниям, поделившись реальной инсайдерской информацией, которая затем будет тщательно проверена и подтверждена. Некоторые подпольные группы активно приглашают «к сотрудничеству» как работников банков, так и кассиров крупных торговых сетей. Злоумышленникам постоянно требуется информация о кредитных картах пользователей с целью последующего кардинга или незаконного получения кредитов в банке. Через инсайдеров активно идет внедрение вредоносного ПО в банковские и корпоративные сети. Вознаграждение инсайдерам выплачивается в криптовалюте.

Согласно последним исследованиям аналитиков компании INFOWATCH[5], проведенном на российских предприятиях как коммерческой, так и государственной форм собственности:

- в 37% случаев причина утечки – умышленные действия сотрудника организации;
- 16% – результат ошибки сотрудников компании;
- 14% случаев – результат совместной работы внешних и внутренних нарушителей;
- 14% случаев – последствия компьютерных атак.

Что могут сделать департаменты информационной безопасности и управления рисками? Чтобы бороться с проблемой инсайдеров, команды по управлению рисками должны активно создавать программы по противодействию инсайдерским угрозам. По иронии судьбы, почти 80 процентов инициатив в области безопасности сосредоточены на защите периметра, в то время как только небольшой процент организаций выделяют средства на программы внутренней защиты. Это означает, что многие инсайдерские угрозы часто остаются совершенно незамеченными.

Отдельно стоит привести примеры глобальных утечек информации в медицинской отрасли. Отчеты, опубликованные за последние несколько лет, указывают, что украденные медицинские записи продаются за цену в 10-20 раз

---

[1] Symantec Corp. 2017 Internet Security Threat Report. – www.symantec.com/security-center/threat-report

[2] PC Tools. What is a Zero-Day Vulnerability? – www.pctools.com/security-news/zero-day-vulnerability

[3] Khandelwal S. Two New Platforms Found Offering Cybercrime-as-a-Service to 'Wannabe Hackers'. 2017. – July 14. – http://thehackernews.com/2017/07/cybercrime-as-as-service.html

[4] Monetizing the Insider. The Growing Symbiosis of Insiders and the Dark Web. – https://intsights.com

[5] Оценка ущерба вследствие утечек информации. – https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie-utechek-informatsii

больше стоимости номера кредитной карты.[1] В действительности, ценообразование на подпольных рынках устроено немного более сложно. Несколько лет назад украденные данные австралийских медицинских карт были оценены в 0,0089 биткойна за пациента, или около $22.[2] Однако в период массовых кибератак за данные пациентов предлагали большие скидки, и конечная стоимость составляла около $1-2 за запись[3]. Таким образом, ценообразование на медицинские записи сильно варьирует в зависимости от намерений продавца и типа доступных данных. Закон спроса и предложения применим и в подпольной экономике.

Табл. 1 демонстрирует оценочную стоимость того или другого типа данных на «черном рынке».

Стоимость простых номеров кредитных карт действительно может быть оценена ниже $1, но более полная информация о карте (т.е. полные данные, информация с магнитной полосы, персональный идентификационный номер) может оцениваться до $100.

Таблица 1

Средняя стоимость данных на «черном рынке»

Тип данных	Средняя стоимость ($)
Банковская карта	0.5-30
Банковская карта с полной информацией	20-60
Магнитная полоса и личный идентификационный номер	60-100
Банковский троян	100
Троян для пароля	25-100
Троян для мобильного банкинга	200
Вредоносное ПО для криптовалют	20-40
Набор для вымогательного ПО	10-1,800
Сервис медиа-стриминга (Netflix)	0.10-10
Бонусы от авиакомпаний (10 000 миль)	5-35
Банковский счет	0.5-10% от баланса счета
Аккаунт облачного хранилища	6-10
Электронная копия паспорта (скан)	1-3

Медицинские данные, как правило, признаются более ценными, чем другие виды данных по следующим причинам:

• Эти данные очень подробные. Медицинские данные могут включать имя потерпевшего, адрес, дату рождения, данные о платежах и финансовых счетах, страховые данные, медицинскую историю и иногда даже данные о ближайших родственниках или фотографии.

• В отличие от номеров кредитных карт, медицинские записи и номера страховки сложнее изменить, а часто они и вовсе не меняются, оставаясь актуальными десятилетиями.

• Такие данные могут быть монетизированы различными способами. Медицинские записи могут использоваться для кражи личности, кражи медицинской страховки, рядового мошенничества, шантажа и вымогательства.[4]

• Медицинская информация ценна для политической разведки. Совмещение информации о вакцинации с данными о занятости в правительстве может указывать на предстоящие зарубежные поездки, можно выявлять государственных служащих с высокими медицинскими счетами, которые могут быть уязвимы для компрометации.

Считается, что стоимость медицинских данных в целом высока. Однако извлечение выгоды из этих объемов данных может быть достаточно затруднительным. Сложность и усилия, необходимые для монетизации медицинских данных, могут отпугнуть хакеров, так как многие из них склонны к быстрой наживе.

Одним из новых трендов в киберпреступности стало вымогательство с использованием вредоносных программ (ransomware). Можно выделить несколько тенденций в использовании вредоносных программ для вымогательства[5]:

• Атаки становятся более целенаправленными, в отличии от бессистемных атак в прошлом, например, «целевые атаки» (APT).

• Рядовые хакеры используют передовые техники для своих операций, аналогичные тем, которые используются в кибершпионажных атаках с привлечением профессионалов.

• Размер выкупных требований увеличивается. Среднее выкупное требование теперь составляет более $1,077, в то время как еще в 2015 году оно составляло $294.

• Рекордные темпы производства вымогательских программ — 98 новых семейств вымогательских программ было обнаружено лишь в 2016 году. К 2023 году их количество увеличилось в десятки раз.

---

[1] Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. – www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[2] Farrell P. The Medicare Machine: Patient Details of 'Any Australian' for sale on Darknet. – www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet

[3] Doe D. 655,000 Patient Records for Sale on The Dark Net after Hacking Victims Refuse Extortion Demands. – www.dailydot.com/layer8/655000-patient-records-dark-net

[4] Cerniauskas S. Lithuania: Cybercriminals Blackmail Plastic Surgery Clinic with Stolen Photos. – www.occrp.org/en/daily/6387-lithuania-cybercriminals-blackmail-plastic-surgery-clinic-with-stolen-photos

[5] Symantec. Ransomware and Businesses 2016. – www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf

• Появление нового вида деятельности — вымогательства с использованием вредоносных программ как услуга (CaaS). Это означает, что все большее число киберпреступников будет участвовать в киберпреступлениях, включая тех, у кого относительно низкий уровень экспертизы.

• Хакеры разрабатывают новые модели и тактики вредоносных атак (например, шифрование уже выкупленных файлов или фальшивое вымогательство, скрывающее более разрушительную кибератаку).[1]

Финансовый ущерб от кибератак

В предыдущие годы главными элементами для обеспечения кибербезопасности были рабочие станции и серверы. Однако с ростом постиндустриальной экономики все большую значимость приобретают именно нематериальные активы: увеличивается значимость бизнес-ценности самих данных (из-за угроз вымогательства). Аналитики начинают рассматривать более сложные сценарии киберугроз, такие как атаки с целью навредить бизнес-операциям (например, в здравоохранении) или нанесения вреда цепям поставок крупных логистических компаний (например, атака с помощью вируса Petya на гиганта судоходства AP Moller-Maersk[2]). Глобальные атаки хакеров существенно повлияли на бизнес (например, подразделения FedEx и TNT, очень долго восстанавливались после сильнейшей кибератаки в июле 2017 года, и их потери в доходах существенно повлияли на итоговые финансовые результаты в конце года[3]).

Происходит рост числа атак на системы промышленной автоматизации и АСУ. Ниже приводим последнюю статистику подобных угроз и атак, полученную в Лаборатории Касперского:

• В первые шесть месяцев 2023 года на 34 процентах компьютеров АСУ, были заблокированы вредоносные объекты (все угрозы).

• Во втором квартале 2023 года в мире этот процент достиг максимального с 2022 года значения за квартал – 26,8%.

• Показатель угроз за полугодие варьирует от 40,3% в Африке до 14,7% в Северной Европе.

• В странах – от 53,3% в Эфиопии до 7,4% в Люксембурге.

Основными источниками угроз являлись: Интернет (19,3% угроз заблокировано на компьютерах АСУ), почтовые клиенты (на 6% компьютерах АСУ), съемные носители (на 3,4% компьютерах АСУ). [4]

Институт Понемона является лидером в изучении затрат на кибербезопасность. Отчет о стоимости кибератак, подготовленный Институтом Понемона в США, подводит итоги финансовых последствий киберпреступности[5]:

• Средняя стоимость утечки или кражи данных достигла исторического максимума в размере $225 за запись.

• Организации в области здравоохранения имели наибольшие убытки в размере $380 за запись.

• Здравоохранение имеет третью по величине степень потери клиентов (5,5%) в результате кибератаки.

• Во всех отраслях экономики атаки хакеров (в сравнении со сбоем в системе или человеческой ошибкой) требуют дольше всего времени для выявления (в среднем 235 дней) и устранения (68 дней).

Однако сложность вопроса целостности данных заключается в том, что злоумышленнику не обязательно фактически манипулировать данными. Для создания неопределенности и даже нарушения работы достаточно просто вызвать сомнения в точности информации.

В табл. 2 представлены потенциальные последствия нарушения защищенной информации о состоянии здоровья.[6-]

Таблица 2

Потенциальные последствия утечки информации в здравоохранении

Репутационные	Финансовые	Судебные/Регуляторные	Операционные
Риск потери пациентов, клиентов, партнеров и/или персонала.	Страховые выплаты и увеличенные отчисления, возможная замена подрядчиков, потеря бизнеса, выплаты пострадавшим.	Судебные издержки и штрафы, потеря аккредитации.	Увольнения и найм новых сотрудников, новое обучение персонала, реорганизация процессов внутри компании.

Оценка того, как киберинцидент влияет на финансовые показатели, является крайне сложным процессом. Помимо реальных затрат в рамках предприятия (например, усилия по обнаружению и ликвидации вредоносного ПО),

---

[1] Krebs B. ‘Petya’ Ransomware Outbreak Goes Global. – https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global

[2] Roberts P. Dear SEC: More Companies Warn on Financial Impact from Petya Infection. – https://securityledger.com/2017/07/dear-sec-more-companies-warn-on-financial-impact-from-petya-infection

[3] Schlangenstein M. FedEx Says TNT Systems May Never Fully Recover From Cyberattack. – www.bloomberg.com/news/articles/2017-07-17/fedex-says-tnt-systems-may-never-fully-recover-from-cyberattack

[4] Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2023. – https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023

[5] The Ponemon Institute. 2017 Cost of Data Breach Study. – www.ibm.com/security/data-breach

[6] American National Standards Institute. The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security. – http://webstore.ansi.org/phi

существуют различные юридические и регуляторные затраты (например, штрафы, судебные иски), а также косвенные затраты, связанные с риском потери бизнеса и репутации.

Методики расчета затрат на кибербезопасность

Для начала определимся с подходами для решения задач по расчету затрат на кибербезопасность. В научной среде и среди практиков существует несколько подходов к решению подобных задач, а именно:

1) На основе бухгалтерского учета и традиционной экономики. Подобный подход базируется на основе учета нематериальных активов.

2) На основе оценки рисков, а также международных стандартов (например, ГОСТ Р ИСО/МЭК 27005-2010).

3) На основе методов математического моделирования, а конкретно, решения задач линейного программирования. Данный метод предполагает постановку экономической задачи, затем построение математической модели, далее идет решение математической модели и проверка ее на устойчивость, допустимость и другие критерии. В конце аналитик проводит экономическую интерпретацию полученного решения.[1]

4) Комплексные методы, которые применяются в бизнесе, ИТ-секторе и экономике.

Вообще, из практики департаментов ИБ следует, что затраты на кибербезопасность должны составлять примерно 30% затрат на ИТ-систему. Далее рассмотрим, какие требования аналитик должен предъявлять к самому методу определения затрат на кибербезопасность:

1) Метод должен обеспечивать количественную оценку затрат на ИБ, но при этом могут быть использованы и качественные показатели.

2) Метод должен быть совершенно «прозрачным» с точки зрения пользователя.

3) Метод должен быть универсальным.

4) Метод должен быть применим в случае существования нескольких видов мер по предотвращению угрозы.

Ниже перечислим некоторые методы из математического моделирования и экономики, которые вполне можно применять при расчете затрат на кибербезопасность:

- Прикладной информационный анализ Applied Information Economics (AIE).
- Потребительский индекс Customer Index (CI).
- Добавленная экономическая стоимость Economic Value Added (EVA).
- Управление портфелем активов Portfolio Management (PM).
- Оценка действительных возможностей Real Option Valuation (ROV).
- Метод жизненного цикла искусственных систем System Life Cycle Analysis (SLCA).
- Система сбалансированных показателей Balanced Scorecard (BSC).
- Совокупная стоимость владения Total Cost of Ownership (TCO).
- Функционально-стоимостной анализ Activity Based Costing (ABC).[2]

Описание каждого из методов и практические примеры решения экономических задач – это тема для отдельной большой статьи. Поэтому в данной статье остановимся на практической задаче вычисления показателей ROI (Return on Investment – отдача от инвестиций), ROSI (отдача от инвестиций в информационную безопасность), показателя TCO (совокупная стоимость владения Total Cost of Ownership) и Payback (окупаемость, период времени, необходимый чтобы доходы, полученные в результате инвестиций, покрыли затраты на эти инвестиции).

Формула для расчета ROI:

$$ROI = \frac{\text{Доходы} - \text{Расходы}}{\text{Инвестиции}}. \quad (1)$$

В экономике показатель ROI является интегральным критерием, который отражает насколько эффективно работают инвестиции, вложенные в бизнес. ROI считают экономисты, а не сотрудники подразделения ИБ, поэтому для ИБ необходимо посчитать свой специфический индекс ROSI:

$$ROSI = \frac{\Delta\text{Доходы} - \Delta\text{Расходы}}{\Delta\text{Инвестиции}}, \quad (2),$$

где ROSI — показатель изменения ROI из-за инвестиций в ИБ;

ΔДоходы — изменение в доходах, которое произошло из-за инвестиций в ИБ;

ΔРасходы — изменение в расходах, которое произошло из-за инвестиций в ИБ;

ΔИнвестиции — инвестиции, сделанные в ИБ.

После подсчета ROSI необходимо оценить эффективность внедренного проекта в сфере ИБ:

1) Если ROSI < 0, то проект убыточен и эффективность его отрицательная.

2) Если ROI > ROSI > 0, то внедрение проекта по ИБ приведет к уменьшению общего ROI в компании.

3) Если ROSI > ROI > 0, то внедрение проекта по ИБ приведет к увеличению общего ROI в компании.

Однако бизнесменам и экономистам необходимо понимать, что внедрение решения по кибербезопасности не приведет напрямую ни к увеличениям продаж, ни к прибыльности основного бизнеса. ROSI только косвенно влияет на основной бизнес компании.

---

[1] Ищук В. Линейное программирование в экономике // Образовательный портал «Справочник». – https://spravochnick.ru/ekonometrika/lineynoe_programmirovanie_v_ekonomike

[2] Петренко С.А. Оценка затрат на кибербезопасность // Труды ИСА РАН. – М., 2006. – Т. 27. – С. 234-265.

Дополнительно, стоит рассмотреть такой показатель, как TCO, который является суммой прямых и косвенных затрат, которые несет владелец информационной системы на протяжении всего жизненного цикла этой системы. Средний срок жизни системы – примерно 3 года (до модернизации или замены на новую). Этот параметр является очень важным, руководителям департаментов ИБ он позволяет экономически обосновать расходы на информационную безопасность, мало того, выразить это в количественных показателях, что важно для экономистов, бухгалтеров и бизнесменов. Но для окончательной оценки проекта по ИБ, необходимо применить еще один показатель: Payback (окупаемость) – показывает период времени, который нужен, чтобы доходы, вырученные в результате инвестиций, покрыли затраты на вложенные инвестиции. Чем больше период окупаемости, тем больше риски вложений в данный проект. В общем, при расчете затрат на кибербезопасность в компании необходимо использовать комплексные методы и различные экономические показатели.[1] Далее будет описано, как опираясь на грамотные экономические расчеты, руководителю принимать верные бизнес-решения.

Принятие верных бизнес-решений в области кибербезопасности

Значимость кибербезопасности еще не полностью дошла до сознания управленческого состава большинства компаний. Многие руководители остаются застрявшими в фазах «отрицания» или «беспокойства». Или, что еще хуже, они могут занять позицию ложной уверенности.[2] Некоторые руководители не могут воспринимать кибербезопасность как составляющую добавочной стоимости для своего бизнеса, потому что кибербезопасность требует фиксируемых затрат, но приносит лишь косвенные выгоды.[3] Это делает сложным демонстрацию возврата вложений в кибербезопасность. Однако здесь руководителю помогут простые правила и прозрачные формулы для планирования затрат на кибербезопасность. Всю работу по внедрению проекта ИБ в организации можно разделить на административные мероприятия, технические мероприятия и меры по ликвидации последствий инцидента ИБ. Таким образом, вырисовывается простая формула для определения общих затрат на ИБ:

$$З_{ИБ} = З_{о} + З_{т} + З_{л}, \quad (3)$$

где:

$З_{ИБ}$ – ежегодные суммарные затраты на безопасность,

$З_{о}$ – затраты на административные мероприятия,

$З_{т}$ – затраты на технические мероприятия,

$З_{л}$ – затраты на ликвидацию последствий инцидентов ИБ.

Но менеджменту компаний также нужно понимать и важность оценки рисков при ведении бизнеса и планирования затрат на кибербезопасность. Также руководителям компаний необходимо осмыслить основные понятия по оценке рисков, для этого необходимо полагаться на ГОСТ Р ИСО/МЭК 27005-2010. Менеджмент рисков ИБ предусматривает следующие меры:

- идентификация рисков;
- оценка рисков;
- информирование о вероятности и последствиях рисков;
- приоритизация в рамках обработки рисков;
- приоритизация мероприятий по снижению имеющих место рисков;
- регулярный мониторинг и пересмотр процесса менеджмента риска;
- подготовка менеджеров в сфере оценки рисков.

Процесс менеджмента риска ИБ состоит из установления контекста, оценки риска, обработки риска, принятия риска, коммуникаций риска, а также мониторинга и переоценки риска ИБ. На рис. 1 изображен процесс менеджмента риска информационной безопасности в виде итераций.[4]

Стоит отметить, что вложение инвестиций в кибербезопасность требует тщательного анализа и профессионализма.[5]

Ключевыми правилами для менеджмента компаний будут:

1. Понимание и подход к кибербезопасности как к вопросу управления рисками на уровне предприятия согласно международным нормативным документам и требованиям регуляторов.

2. Осознание не только технических, но и юридических последствий кибератак для бизнес-процессов компании.

3. Регулярное обсуждение вопросов управления рисками и кибербезопасности на заседаниях руководящего состава любого бизнеса или организации.

---

[1] Пискунов И. Планирование затрат на информационную безопасность. – https://www.anti-malware.ru/analytics/Technology_Analysis/economic_planning

[2] Burkitt-Gray A. Executives 'in Denial' about Cyber Security Threat. – www.globaltelecomsbusiness.com/article/b13rsw1zvm8mnw/executives-39in-denial39-about-cyber-security-threat

[3] Magee K. Why Cybersecurity Is Financially Undervalued. – ww2.cfo.com/cyber-security-technology/2017/06/cybersecurity-financially-undervalued

[4] ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Information technology. Security techniques. Information security risk management. – https://docs.cntd.ru/document/1200084141

[5] Blau A. The Behavioral Economics of Why Executives Underinvest in Cybersecurity. – https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity

4. Создание специального департамента ИБ на уровне предприятия с адекватным штатным расписанием и бюджетом.

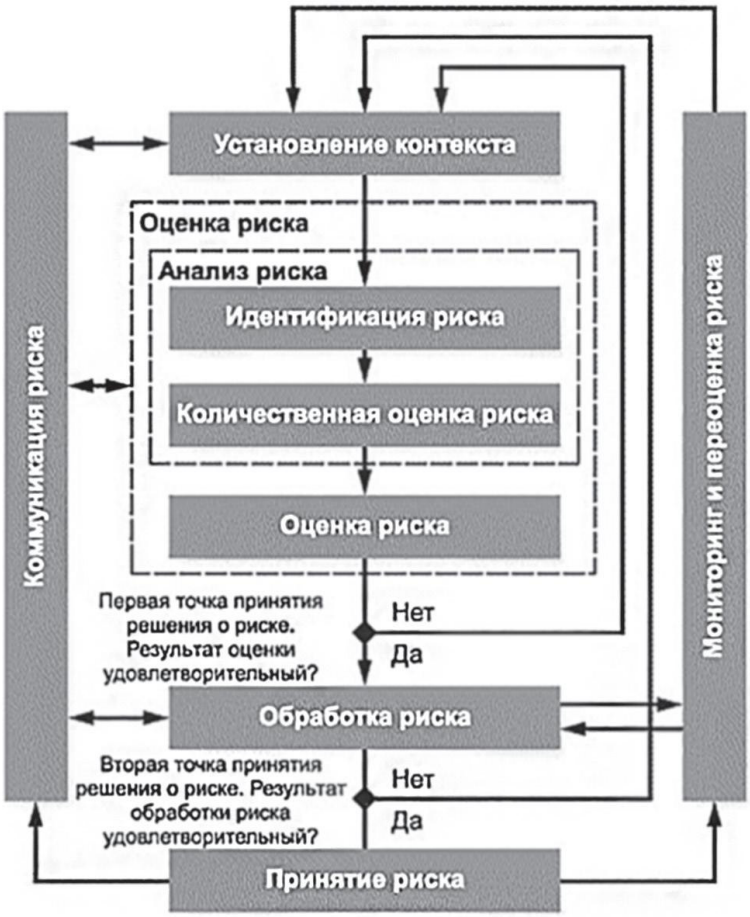

Рисунок 1.
Процесс менеджмента риска информационной безопасности

Выводы

Руководство компаний и государственных организаций должно понимать, что соответствие техническим регламентам, международным и национальным стандартам, а также требованиям регуляторов по ИБ, т.е. комплаенс (англ. compliance), и практическая кибербезопасность – это две связанные, но все же отдельные цели. В каких-то организациях (например, в финансовых компаниях и банках) на первое место выходит комплаенс, но департаменты ИБ банков не забывают и о технических и программных методах защиты чувствительной информации. Однако есть негативные примеры, когда комплаенс и систему ИБ разворачивают только ради прохождения аудита у регулятора.

В реальном мире компании и организации противостоят целой индустрии киберпреступности, поэтому такие задачи, как комплаенс, разработка политики безопасности компании, построение эффективной системы киберзащиты на основе моделей угроз и алгоритмов оценки рисков являются первоочередными целями для менеджмента компаний.