Министерство цифрового развития, связи и
массовых коммуникаций Российской Федерации

Сибирский Государственный Университет Телекоммуникаций и Информатики

Межрегиональный центр переподготовки специалистов

Реферат (контрольная работа)

По дисциплине: информационная безопасность

Тема: экономический аспект информационной безопасности

Новосибирск, 2023г

Оглавление

ВВЕДЕНИЕ

В современном мире информация становится стратегическим ресурсом, одним из основных богатств экономически развитого государства. Быстрое совершенствование информатизации в России, проникновение ее во все сферы жизненно важных интересов личности, общества и государства вызвали помимо несомненных преимуществ и появление ряда существенных проблем. Одной из них стала необходимость защиты информации. Учитывая, что в настоящее время экономический потенциал все в большей степени определяется уровнем развития информационной структуры, пропорционально растет потенциальная уязвимость экономики от информационных воздействий.

Каждый сбой работы компьютерной сети — это не только «моральный» ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей, «безбумажного» документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем на сегодняшний день.

Решению этой проблемы экономистами уделяется огромное значение. Предложено большое количество методик и разработок для расчета стоимостных показателей информационной безопасности.

Как правило, они сводятся к двум основным направлениям:

– Определение степени значимости (секретности) той или иной информации, исходя из требований законодательных документов и/или решений руководства фирмы;

– Установление соответственно определенных весов тем или иным угрозам.

Тема контрольной работы является актуальной в современном мире, так как интерес к вопросам защиты информации в последнее время вырос, что связывают с возрастанием роли информационных ресурсов в конкурентной борьбе, расширением использования сетей, а, следовательно, и возможностей несанкционированного доступа к хранимой и передаваемой информации.

Развитие средств, методов и форм автоматизации процессов хранения и обработки информации и массовое применение персональных компьютеров делают информацию гораздо более уязвимой. Информация, циркулирующая в них, может быть незаконно изменена, похищена или уничтожена.

Информатизация на современном этапе развития человечества является наиболее динамично развивающейся сферой мировой экономики, способной конкурировать по доходности с топливно-энергетическим комплексом, автомобилестроением, производством сельскохозяйственной продукции, и определяет наукоемкость промышленной продукции, ее конкурентоспособность на мировом рынке.

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляюших системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия, что угрожает экономической безопасности.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сторон деятельности, конфиденциальная коммерческая и персональная информация, была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения,

фальсификации, незаконного тиражирования, блокирования или уничтожения.

1. Понятие и сущность информационной безопасности

Понятие информации первоначально было следующим: это сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и т.д.). С середины XX века появляется общенаучное понятие информации, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом.

Сформулированные к настоящему времени строгие научные определения концентрируют внимание на одном из основных аспектов этого многозначного понятия — соотношении информации и материи.

Понятие «информационная безопасность» неоднозначно трактуется в современной научной литературе. Можно выделить три принципиально различных подхода к пониманию его содержания.

В первом случае информационная безопасность рассматривается как комплекс мероприятий по защите информации и средств ее передачи, хранения, обработки и накопления.

Во втором – как обеспечение защиты от информационных воздействий различного рода или как комплекс мер по противодействию акциям информационной войны.

В третьем случае проблематика информационной безопасности распространяется практически на все сферы жизнедеятельности личности, общества и государства, связанные с производством, преобразованием, потреблением, накоплением и хранением информации независимо от способов и средств осуществления этих процессов (это так называемое расширительное толкование).

Таким образом, информационная безопасность – это невозможность нанесения вреда свойствам объекта безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз).

Объектом информационной безопасности может быть коммерческое предприятие. Тогда содержание "информационной безопасности" будет заключаться в защищенности интересов собственника данного предприятия, удовлетворяемых с помощью информации, либо связанных с защитой от несанкционированного доступа тех сведений, которые представляются собственнику достаточно важными.

Интересы проявляются через объекты, способные служить для их удовлетворения, и действия, предпринимаемые для обладания этими объектами. Соответственно интересы как объект безопасности могут быть представлены совокупностью информации, способной удовлетворять интерес собственника, и его действий, направленных на овладение информацией или сокрытие информации. Эти составляющие объекта информационной безопасности и защищаются от внешних и внутренних угроз.

К объектам информационной безопасности на предприятии относят:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде информационных массивов и баз данных;
- средства и системы информатизации - средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления предприятиями, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля.

При осуществлении коммерческой деятельности возникает информация, известность которой другим участникам рынка может существенно снизить доходность этой деятельности. В деятельности государства порождается информация, раскрытие которой может снизить эффективность проводимой политики. Подобная информация закрывается, и устанавливаемый режим ее использования призван предупредить

возможность несанкционированного ознакомления с ней. В этом случае объектом безопасности выступает режим доступа к информации, а информационная безопасность заключается в невозможности нарушения этого режима.

Примером могут служить информационно-телекоммуникационные системы и средства связи, предназначенные для обработки и передачи сведений, составляющих государственную тайну. Основным объектом безопасности в них является режим доступа к секретной информации. Информационная безопасность таких систем заключается в защищенности этой информации от несанкционированного доступа, уничтожения, изменения и других действий. Система обеспечения безопасности информации включает подсистемы:

- компьютерную безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности, связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашении.

Безопасное программное обеспечение представляет собой общесистемные и прикладные программы и средства, осуществляющие безопасную обработку данных и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается принятием мер по предотвращению предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

Политика безопасности включает в себя анализ возможных угроз и выбор соответствующих мер противодействия, являющихся совокупностью тех норм, правил поведения, которыми пользуется конкретная организация при обработке информации и ее защите.

Угроза безопасности информации - события или действия, которые могут привести к искажению, неразрешенному использованию или к разрушению информационных ресурсов управления системы, а также программных и аппаратных средств.

2. Экономические аспекты информационной безопасности

Сегодня высшее руководство любой компании при осуществлении управления, по существу имеет дело только с информацией - и на ее основе принимает решения. Информация в настоящее время решает все.

Информация уже давно стала товаром, который можно покупать и продавать на рынке, иногда - за достаточно большие деньги. Как и любой товар, информация имеет свою цену, за которую она покупается и продается, и как любой ценный ресурс - подлежит защите.

Российский ИТ-рынок по итогам 2021 года показал положительную динамику. По оценке TAdviser (https://www.tadviser.ru/), озвученной в июне 2022 года, рост рынка составил 20%, а его объем достиг 2,22 трлн рублей. Главными драйверами роста стали факторы, связанные с пандемией – массовая цифровизация компаний и переориентация на гибридный формат работы, увеличение спроса на решения в сфере информационной безопасности. Также заметно увеличился спрос на отечественные ИТ-решения.

Такой рост определяется в основном двумя факторами: возросшим вниманием руководства к обеспечению ИБ и недостаточным уровнем ИБ в существующих информационных системах (ИС). Понятно, что долго такие темпы роста сектора ИБ сохраняться не смогут, они замедлятся, и вопросы оценки эффективности затрат в области ИБ встанут весьма остро.

Уже сейчас в отечественных ИС с повышенными требованиями в области ИБ (банковские системы, ответственные производства, и т.д.) затраты на обеспечение режима ИБ составляют до 30% всех затрат на ИС. Владельцы информационных ресурсов серьезно рассматривают экономические аспекты обеспечения ИБ. Даже в тех ИС, уровень ИБ, которых явно не достаточен, у технических специалистов зачастую возникают проблемы обоснования перед руководством (владельцами информационных ресурсов) затрат на повышение этого уровня. Начальники

служб автоматизации, исполнительные директора, начальники служб информационной безопасности должны иметь понятные для бизнеса аргументы для обоснования инвестиций в ИБ, т.е., по сути, представлять обоснование стоимости системы ИБ для бизнеса.

Таким образом, в настоящее время комплексное управление процессами обеспечения ИБ подразумевает не просто бесцельное внедрение совокупности средств и систем защиты. ИБ превратилась в науку о реализации адекватного и эффективного по качеству и стоимости подхода к обеспечению защищенности всех элементов информационных технологий (IT). Такой взгляд на проблему ИБ неизбежно требует определения показателей и метрик, позволяющих сравнивать защищенность различных систем IT, сравнивать эффективность контрмер, ранжировать угрозы и уязвимости по своей важности.

Для любых компаний очень важно деньги в защиту информации (ЗИ) вкладывать обоснованно. В информационной безопасности известен принцип разумной достаточности, который гласит следующее: "Создание 100% надежной системы защиты информации (СЗИ) невозможно в принципе, в любых случаях остается ненулевая возможность реализации какой-либо угрозы либо уязвимости". Любая система ЗИ может быть взломана, это вопрос только времени и потраченных злоумышленником средств. Поэтому бесконечно вкладывать деньги в обеспечение ИБ бессмысленно, необходимо когда-то остановиться (вопрос только в выборе этого порога). Согласно принципу разумной достаточности, стойкость СЗИ считается достаточной, если время взлома злоумышленником СЗИ превосходит время старения информации (либо некоторый разумный предел), либо стоимость взлома системы защиты информации превосходит стоимость полученной злоумышленником выгоды от взлома. В последнем случае, если злоумышленник является нормальным экономическим субъектом, то он, конечно, не будет работать себе в убыток.

Существует, как минимум, два подхода к обоснованию стоимости корпоративной системы защиты.

Первый подход - наукообразный, который заключается в том, чтобы применить на практике необходимый инструментарий получения метрики и меры безопасности, а для этого привлечь руководство компании (как ее собственника) к оценке стоимости защищаемой информации, определению возможностей реализации потенциальных угроз и уязвимостей, а также потенциального ущерба. Наиболее известный показатель, позволяющий характеризовать меру безопасности, сравнивать защищенность различных систем IT, сравнивать эффективность контрмер - есть риск ИБ. Через риск достаточно эффективно считается наиболее экономичный вариант реализации контрмер.

Второй подход - практический состоит в следующем: можно попробовать найти инвариант разумной стоимости корпоративной системы защиты информации. Ведь существуют аналогичные инварианты в других областях, где значимые для бизнеса события носят вероятностный характер. Например, на рынке автострахования некоторая общая оценка разумной стоимости такой услуги, как страхование собственного автомобиля, составляет от 5 до 15% его рыночной цены - в зависимости от локальных условий эксплуатации, культуры и опыта вождения водителя, интенсивности движения, состояния дорог и т.д.

Эксперты-практики в области защиты информации нашли некий оптимум, позволяющий чувствовать себя относительно уверенно, - стоимость системы ИБ должна составлять примерно 10-20% от стоимости корпоративной информационной системы (КИС) - в зависимости от уровня конфиденциальности информации (но надо их еще правильно вложить). Это и есть та самая оценка на основе практического опыта (best practice), на которую можно положиться. И на вопрос "А почему для создания адекватной целям и задачам бизнеса комплексной системы защиты информации (КСЗИ) требуется сто тысяч долларов?" отвечать "Потому что на сегодняшний день

стоимость нашей КИС составила один миллион долларов!". Очевидно, что второй подход не лишен недостатков. Здесь, скорее всего, не удастся заставить руководство глубоко осознать проблемы ИБ. Но зато можно смело прогнозировать объем бюджета на ИБ и существенно сэкономить на услугах внешних консультантов.

2.1 Пример оценки затрат на ИБ

В качестве примера использования методики совокупной стоимости владения (ССВ) для обоснования инвестиций в ИБ рассмотрим проект модернизации корпоративной системы антивирусной защиты и системы управления доступом на объекте информатизации (физическая защита).

Для этого сначала условно определим три возможных состояния системы защиты КИС от вирусов и вредоносного ПО, а именно: базовое, среднее и высокое.

Базовое: Стационарные и мобильные рабочие станции обладают локальной защитой от вирусов. Антивирусное программное обеспечение и базы сигнатур регулярно обновляются для успешного распознавания и парирования новых вирусов. Установлена программа автоматического уничтожения наиболее опасных вирусов. Основная цель уровня – организация минимальной защиты от вирусов и вредоносного ПО при небольших затратах.

Среднее: Установлена сетевая программа обнаружения вирусов. Управление программными обновлениями на сервере автоматизировано. Системный контроль над событиями оповещает о случаях появления вирусов и предоставляет информацию по предотвращению дальнейшего распространения вирусов. Превентивная защита от вирусов предполагает выработку и следование определённой политики защиты информации, передаваемой по открытым каналам связи Интернет. Дополнительно к техническим мерам используются организационные меры защиты информации.

Высокое: Антивирусная защита воспринимается как один из основных компонентов корпоративной системы защиты. Система антивирусной защиты тесно интегрирована в комплексную систему централизованного управления ИБ компании и обладает максимальной степенью автоматизации. При этом организационные меры по защите информации преобладают над техническими мерами. Стратегия защиты информации определяется исключительно стратегией развития бизнеса компании.

Также условно выделим три состояния развития системы контроля и управления доступом в КИС (обеспечение физической безопасности): базовое, среднее, высокое.

Базовое: ведётся учет как минимум рабочих станций и серверов, инвентаризационные таблички крепятся на соответствующее аппаратное обеспечение. Введена процедура контроля перемещения аппаратных средств КИС. Проводятся постоянные и периодические инструктажи персонала компании. Особое внимание уделяется мобильным компонентам КИС.

Среднее: используются механические и электронные замки, шлюзовые кабины и турникеты. Организованы контрольно-пропускные пункты и проходные. Осуществляется видеонаблюдение на объекте информатизации. Требования к персоналу определены и доведены под роспись. Разработаны инструкции по действию в штатных и внештатных ситуациях. Задействованы частные и государственные охранные предприятия и структуры.

Высокое: Обеспечение физической безопасности аппаратных средств является частью единой политики безопасности, утверждённой руководством компании. Активно используются весь комплекс мер защиты информации, начиная с организационного и заканчивая техническим уровнями.

Проект по модернизации корпоративной системы в части ИБ предполагает модернизацию двух элементов: антивирусной защиты и системы управления ИБ. Необходимо обосновать переход от базового уровня к повышенному (среднему или высокому). В табл. 1 приводятся требования к элементам защиты, сформулированные в задании на модернизацию КИС.

Элемент системы ИБ	Задача	Исходный (базовый) уровень	Повышенный уровень
Антивирусная защита	Каким образом распространяются обновления механизма антивирусной защиты?	Ничего не делается или нет информации	Используется автоматическое обновление антивирусного обеспечения
Антивирусная защита	Какая степень защиты от вирусов является допустимой?	Нет механизма защиты от вирусов	Защита от вирусов устанавливается ИС службой и не доступна пользователям для изменений
Антивирусная защита	Какой процент клиентских мест поддерживается серверной антивирусной защитой?	Нет данных	100 %
Антивирусная защита	Как устраняются последствия вирусных атак (в процентном отношении к числу вирусных событий)?	Пользователь самостоятельно восстанавливает поврежденные файлы и систему, протокол событий не ведется	ИС персонал уведомляется об инциденте, проводятся исследования и предпринимаются нейтрализующие меры, на местах поддерживается БД вирусных событий
Управление ИБ	Что делается для гарантии безопасности критичных данных (информация, которая является критичной по отношению к миссии каждого отдельного предприятия)	Не регламентирован	Средства шифрования и резервного копирования на серверах
Управление ИБ	Что делается для гарантии физической безопасности помещений с целью предотвращения случаев воровства и преступного использования оборудования?	Применяются сигналы тревоги о нарушении безопасности	Дополнительное использование таких средств безопасности, как смарт-карты или биометрические устройства

Таблица 1- характеристики исходного и повышенного уровня защиты

Возможно несколько вариантов реализации этих требований, характеризующихся разными экономическими показателями. Рассмотрим типичную структуру расходов по выбранным элементам системы ИБ «среднего западного» предприятия на модернизацию ИС (табл.2) для обеспечения «среднего» уровня защиты.

Статья затрат	Антивирусная защита	Управление ИБ
Подготовительные процедуры и операции по инсталляции		
Услуги по инсталляции ПО:		
С учетом поддержки уровня 2	2,600 %	0,000 %
С учетом поддержки уровня 3	1,300 %	0,000 %
Администрирование пользователей	0,000 %	6,500 %
Установка аппаратного обеспечения	0,000 %	2,600 %
Резервное копирование, архивирование и восстановление	2,600 %	0,000 %
Планирование и управление процессами восстановления		
Общие процедуры управления, планирование и изучение рынка продуктов	1,300 %	1,300 %
Закупка программно-технических средств	18,200 %	2,600 %
Процедуры по восстановлению	19,500 %	0,000 %
Сервисное обслуживание		
Ежедневные процедуры поддержки пользователей	5,200 %	2,600 %
Административные расходы		
Финансовые службы и администрация	1,268 %	0,618 %
Административная поддержка ИС	0,429 %	0,169 %
Закупка, снабжение	0,000 %	5,200 %
Аудит	0,000 %	1,300 %
Управление контрактами, работа с поставщиками	0,000 %	2,600 %
Затраты рабочего времени конечных пользователей на решение задач ИБ		
Затраты времени на управление файлами, данными и резервным копированием	6,500 %	0,000 %
Затрата на взаимодействие со службами поддержки	6,500 %	0,000 %
Затрата на взаимопомощь пользователей	6,500 %	0,000 %
Затраты на самоподдержку (решение проблем своими силами)	6,500 %	2,600 %
Незапланированные простои по причинам, относящимся к данным средствам защиты	10,400 %	10,400 %

Таблица 2 - статьи расходов среднего уровня защиты

В табл. 3 и на рис. 1 показаны расчеты совокупной стоимости владения при различных вариантах проведения модернизации КИС. Данные приводятся для «среднего западного» предприятия. Расчетная стоимость снижения ССВ для третьего варианта около 230 тыс. долл. в год позволяют обосновать инвестиции в размере около 600 тыс. долл. на рассматриваемые компоненты защиты. При этом расчётный период окупаемости составляет не более 3 лет.

Расходы на ИТ	Базовый вариант защиты: Антивирусная защита – низкий уровень Управление ИБ – низкий уровень	Вариант 1: Антивирусная защита – средний уровень Управление ИБ – низкий уровень	Вариант 2: Антивирусная защита – низкий уровень Управление ИБ – средний уровень	Вариант 3: Антивирусная защита – средний уровень Управление ИБ – средний уровень
Совокупная стоимость владения (ССВ)	$14,905,090	$14,659,236	$14,796,746	$14,563,990
Расходы на СВТ и ПО	$9,183,334	$9,212,787	$9,211,699	$9,241,232
Расходы на операции ИС	$1,402,287	$1,376,061	$1,394,232	$1,368,450
Административные расходы	$426,758	$425,554	$423,952	$422,748
Расходы на операции конечных пользователей	$2,772,377	$2,636,870	$2,758,898	$2,624,287
Расходы, связанные с простоями	$1,120,334	$1,007,965	$1,007,965	$907,273

Таблица 3 - совокупная стоимость владения

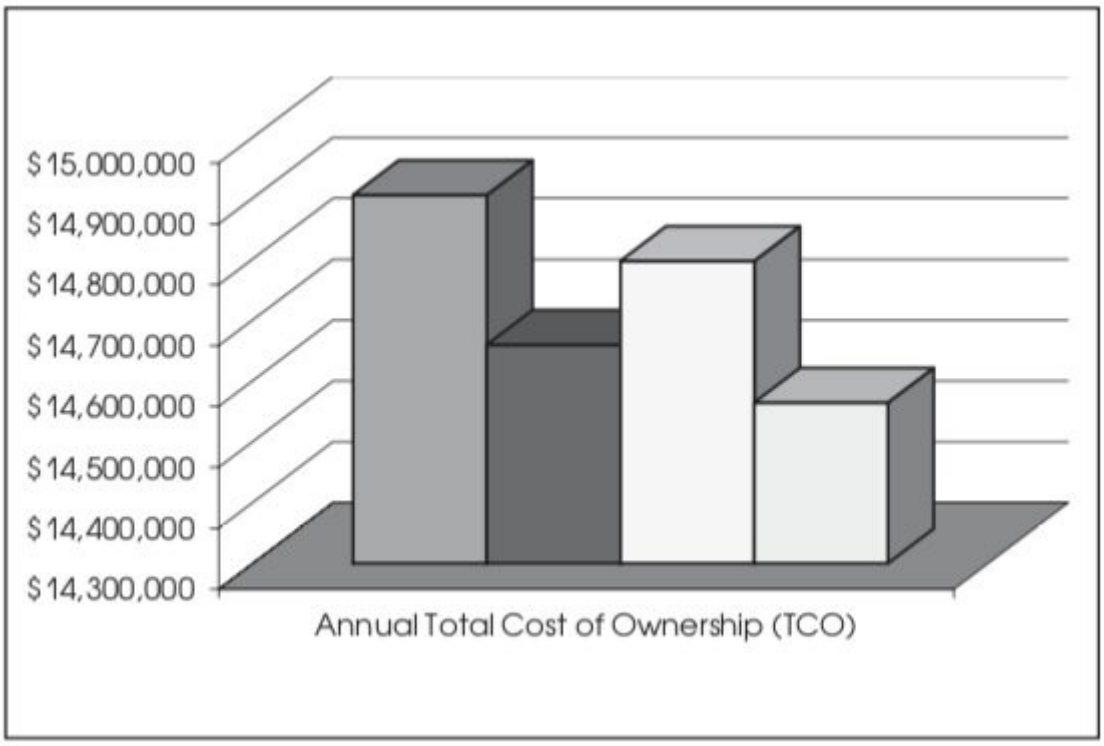


Рисунок 1 - изменение ССВ при различных вариантах проведения модернизации ИБ

Расходы на аппаратные средства и программное обеспечение. Эта категория модели ССВ включает серверы, компьютеры клиентов (настольные и мобильные компьютеры), периферийные устройства и сетевые компоненты.

Также в эту категорию входят расходы на аппаратно-программные средства ИБ.

Расходы на операции ИС.

Прямые затраты на содержание персонала, стоимость работ и аутсорсинг, произведенные компанией в целом, бизнес-подразделениями или ИС службой для осуществления технической поддержки и операций по поддержанию инфраструктуры для пользователей распределенных вычислений.

Административные расходы.

Прямые затраты на персонал, обеспечение деятельности и расходы внутренних/внешних поставщиков (вендоров) на поддержку ИС операций, включающих управление, финансирование, приобретение и обучение ИС.

Расходы на операции конечных пользователей.

Это затраты на само поддержку конечных пользователей, а также на поддержку пользователями друг друга в противовес официальной поддержке ИТ. Затраты включают: самостоятельную поддержку, официальное обучение конечных пользователей, нерегулярное (неофициальное) обучение, самостоятельные прикладные разработки, поддержку локальной файловой системы.

Расходы на простои.

Данная категория учитывает ежегодные потери производительности конечных пользователей от запланированных и незапланированных отключений сетевых ресурсов, включая клиентские компьютеры, совместно используемые серверы, принтеры, прикладные программы, коммуникационные ресурсы и ПО для связи. Для анализа фактической стоимости простоев, которые связаны с перебоями в работе сети и которые оказывают влияние на производительность, исходные данные получают из обзора по конечным пользователям. Рассматриваются только те простои, которые ведут к потерям в основной деятельности организации.

Отметим, что для применения методики ССВ требуются данные о потерях, связанных с простоями и другими негативными последствиях

реализации угроз ИБ. Получить экономические оценки потерь можно на этапе анализа информационных рисков.

2.2 Разработка методик оценки затрат на ИБ

Рассмотрим, как можно определить прямые (бюджетные) и косвенные затраты на ИБ с учетом специфики российских компаний.

Предположим, что руководство компании проводит работы по внедрению на предприятии системы защиты информации (СЗИ). Уже определены объекты и цели защиты, угрозы информационной безопасности и меры по противодействию им, приобретены и установлены необходимые средства защиты информации.

Затраты на информационную безопасность.

Как правило, затраты на информационную безопасность подразделяются на следующие категории:

- Затраты на формирование и поддержание звена управления системой защиты информации (организационные затраты).
- Затраты на контроль, то есть на определение и подтверждение достигнутого уровня защищенности ресурсов предприятия.
- Внутренние затраты на ликвидацию последствий нарушения политики информационной безопасности (НПБ) – затраты, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут.
- Внешние затраты на ликвидацию последствий нарушения политики информационной безопасности – компенсация потерь при нарушениях политики безопасности в случаях, связанных с утечкой информации, потерей имиджа компании, утратой доверия партнеров и потребителей и т. п.

- Затраты на техническое обслуживание системы защиты информации и мероприятия по предотвращению нарушений политики безопасности предприятия (затраты на предупредительные мероприятия).

При этом обычно выделяют единовременные и систематические затраты. К единовременным относятся затраты на формирование политики безопасности предприятия: организационные затраты и затраты на приобретение и установку средств защиты.

Классификация затрат условна, так как сбор, классификация и анализ затрат на информационную безопасность – внутренняя деятельность предприятий, и детальная разработка перечня зависят от особенностей конкретной организации. Самое главное при определении затрат на систему безопасности – взаимопонимание и согласие по статьям расходов внутри предприятия. Кроме того, категории затрат должны быть постоянными и не должны дублировать друг друга.

Невозможно полностью исключить затраты на безопасность, однако они могут быть приведены к приемлемому уровню. Некоторые виды затрат на безопасность являются абсолютно необходимыми, а некоторые могут быть существенно уменьшены или исключены. Последние – это те, которые могут исчезнуть при отсутствии нарушений политики безопасности или сократятся, если количество и разрушающее воздействие нарушений уменьшатся.

При соблюдении политики безопасности и проведении профилактики нарушений можно исключить или существенно уменьшить следующие затраты:

- На восстановление системы безопасности до соответствия требованиям политики безопасности.
- На восстановление ресурсов информационной среды предприятия.
- На переделки внутри системы безопасности.
- На юридические споры и выплаты компенсаций.

- На выявление причин нарушения политики безопасности.

Необходимые затраты – это те, которые необходимы даже если уровень угроз безопасности достаточно низкий. Это затраты на поддержание достигнутого уровня защищенности информационной среды предприятия.

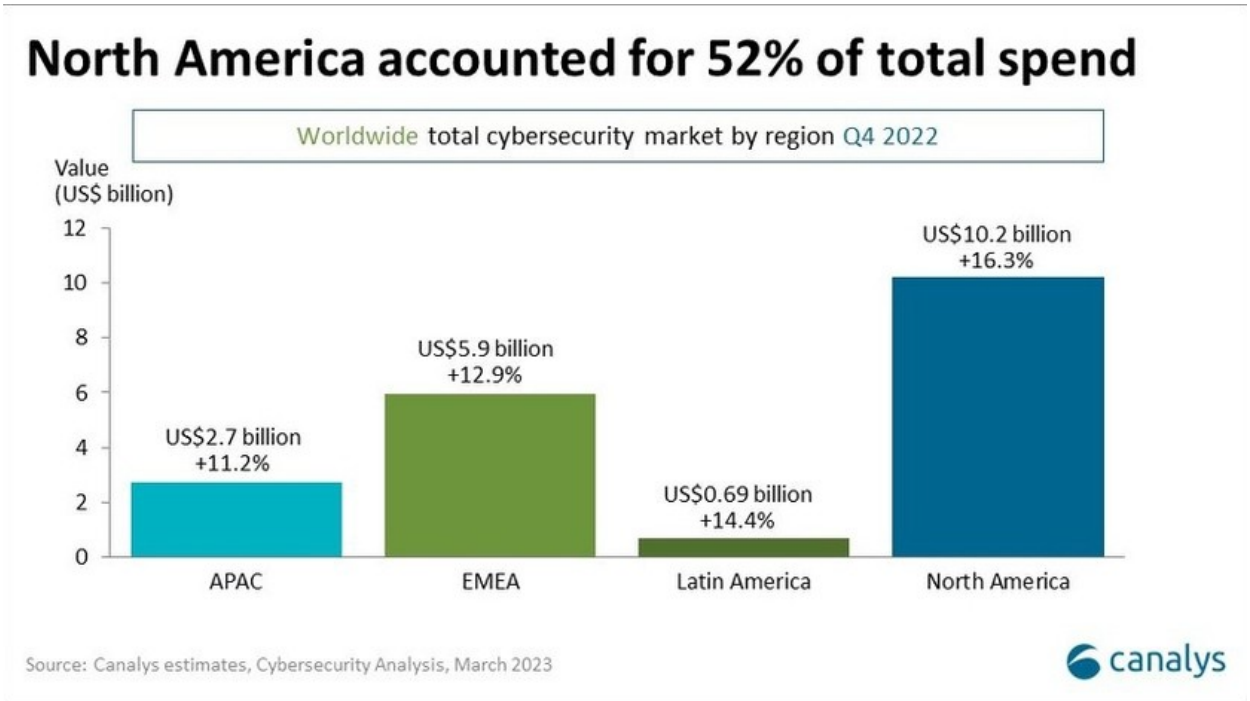
Неизбежные затраты могут включать:

- Обслуживание технических средств защиты.
- Конфиденциальное делопроизводство.
- Функционирование и аудит системы безопасности.
- Минимальный уровень проверок и контроля с привлечением специализированных организаций.
- Обучение персонала методам информационной безопасности.

3. Экономические проблемы информационных ресурсов и защиты информации

Расходы на технологии кибербезопасности в мировом масштабе устойчиво растут. В 2022 году затраты в соответствующем сегменте поднялись на 15,8% по сравнению с предыдущим годом, достигнув $71,1 млрд. Об этом 23 марта 2023-го сообщила аналитическая компания Canalys (https://canalys.com/).

В исследовании учитываются показатели по шести ключевым сегментам рынка ИБ-технологий. Это средства обеспечения безопасности конечных точек, инструменты сетевой защиты, безопасность данных, веб-безопасность и защита электронной почты, софт для поиска и анализа уязвимостей, а также системы управления доступом к идентификационным



данным.

Поставки ИБ-продуктов через каналы продаж за год выросли на 16,1% — до $64,6 млрд, что составляет 91% от общего объёма глобального рынка.

На непосредственные сделки между заказчиками и поставщиками защитных решений пришлись оставшиеся 9%. К концу 2022-го средства обеспечения сетевой безопасности стали самой крупной категорией с точки зрения затрат клиентов. Далее следуют инструменты для обнаружения уязвимостей и программное обеспечение для управления доступом к идентификационным данным.

Оптимистичные результаты компенсируются растущими бюджетными ограничениями на ИТ, которые вынуждают заказчиков расставлять приоритеты в проектах, в то время как дополнительные уровни контроля ещё больше удлиняют циклы продаж. Ведущие поставщики боролись за позиции на сильно фрагментированном рынке. В центре внимания остаются средства контроля доступа, облачная защита и модернизация центров управления безопасностью, — говорится в отчёте Canalys (https://canalys.com/).

По состоянию на конец 2022 года 12 ведущих поставщиков инструментов кибербезопасности контролировали практически половину мирового рынка в плане расходов — 47,1%.

Лидером отрасли стала Palo Alto Networks с долей около 7,9%. На втором месте находится Fortinet с 6,8%, а замыкает тройку Cisco с 6,1%. Далее идут Check Point и CrowdStrike, показатель которых составляет соответственно 3,8% и 3,2%. На шестой строке располагается IBM с 3,1%, на седьмой — Okta с 3%. Затем идут Microsoft, Trellix и Symantec — 2,9%, 2,9% и 2,6%. Одиннадцатое и двенадцатое места достались Splunk и Trend Micro, доли которых составили 2,4% и 2,3%. Все прочие поставщики вместе взятые контролируют 52,9% отрасли.

Worldwide cybersecurity leading vendors

Canalys Cybersecurity Market Pulse: Q4 2022

Vendor	Q4 2021 market share	Q4 2022 market share	Revenue growth
Palo Alto Networks	7.3%	7.9%	24.8%
Fortinet	6.1%	6.8%	26.6%
Cisco	7.0%	6.1%	0.1%
Check Point	4.1%	3.8%	6.7%
CrowdStrike	2.5%	3.2%	45.5%
IBM	3.4%	3.1%	4.0%
Okta	2.6%	3.0%	34.0%
Microsoft	2.5%	2.9%	37.1%
Trellix	3.2%	2.9%	5.1%
Symantec	2.9%	2.6%	1.9%
Splunk	2.1%	2.4%	35.5%
Trend Micro	2.5%	2.3%	9.0%
Others	54.0%	52.9%	12.0%
All vendors	**100%**	**100%**	**14.5%**

Необходимость в защите информации от постороннего вмешательства и наблюдения давно осознана, разработаны и продолжают разрабатываться соответствующие технологии. Однако увлечение отдельными решениями из области информационной безопасности заслоняет сохраняющуюся фундаментальную проблему, а именно достаточность и эффективность систем защиты с точки зрения пользователя.

Мерилом потребительских качеств подобных систем может служить соотношение «стоимость/эффективность», т.е., в конечном счете, баланс между возможным ущербом от несанкционированных действий и размером вложений, которые необходимо потратить для обеспечения защищенности информационных ресурсов.

Инвестиции в разработку проектов защиты объекта, закупку необходимых элементов безопасности и эксплуатацию систем защиты для владельца информации есть ни что иное, как материализованный экономический ущерб. Идя на эти траты, пользователь надеется избежать большего ущерба, связанного с возможным нарушением конфиденциальности. Возникает дилемма: внести плату (частично реализовав ущерб) за возможность уклонения с долей вероятности или допустить возможность ущерба в полной мере, не тратя ничего. Разумное решение состоит в определении оптимальных вложений в системы защиты, обеспечивающих минимальные финансовые потери владельца информации при несанкционированных действиях с нею.

Перед пользователем стоит задача создания оптимальной, с экономической точки зрения, системы защиты информации. Эта задача не так характерна для государственных организаций, однако весьма актуальна для хозяйственно самостоятельных субъектов, ориентированных на деятельность в рыночных условиях.

Наиболее надежными системами защиты информации (СЗИ) являются те, в которых комплексно реализованы все возможные и доступные меры — морально-этические, законодательные, организационные, экономические и технические. Однако комплексные решения очень дороги и могут быть реализованы далеко не всегда. Кроме того, ущерб от утраты защищаемой информации или от разного рода несанкционированных действий с ней может быть гораздо меньше стоимости СЗИ. Поэтому уровень финансовых средств, выделяемых на создание и эксплуатацию СЗИ, должен быть сбалансированным и соответствовать масштабу угроз. Если стоимость СЗИ

по сравнению с предполагаемым ущербом мала, то основным фактором риска собственника являются экономические потери от несанкционированных действий с принадлежащей ему информацией. В противоположной ситуации основные потери связаны с чрезмерно высокой стоимостью СЗИ. Необходимо при этом отметить, что затраты на СЗИ носят детерминированный характер, поскольку они уже материализованы в конкретные меры, способы и средства защиты, а вот ущерб, который может быть нанесен при несанкционированных действиях, — величина случайная.

Такой качественный анализ позволяет предполагать, что существует область экономически оптимальных СЗИ, обеспечивающих наименьший риск собственника информации. В качестве меры риска понимаются ожидаемые суммарные потери в процессе защиты информации в течение определенного периода времени. Проведенное автором исследование, основанное на количественном моделировании риска, подтвердило это предположение, обеспечив оценку параметров экономически оптимальных СЗИ.

Результаты численного моделирования подтвердили, что экономически оптимальная СЗИ не является самой безопасной. Более того, вероятность ущерба от несанкционированных действий при реализации такой системы может превышать в несколько раз минимально возможные значения показателей безопасности защиты информации. Поэтому применение изложенного подхода ограничено областью экономической целесообразности. В случаях, когда доминирующим требованием является обеспечение абсолютной безопасности информации, реализация концепции экономически оптимальной СЗИ не применима. Это относится, например, к сведениям, составляющим государственную тайну. Тем не менее, оптимальные СЗИ обеспечивают адаптацию требований безопасности к размеру возможного ущерба.

Изложенные результаты базируются на вполне логичном предположении о том, что более высокий уровень безопасности достигается за счет увеличения стоимости СЗИ.

4. Развитие услуг информационной безопасности

По оценке Accenture (https://www.accenture.com/) мировой рынок услуг в сфере кибербезопасности будет расти на 13% в год и достигнет объема в $94 млрд к 2025 г. Об этом компания сообщила 4 февраля 2022 года. Главными направлениями развития станут кибербезопасность как сервис и автоматизация операций ИБ, особое внимание будет уделено защите критической инфраструктуры и приложений.

По мнению Accenture, рост расходов на кибербезопасность обусловлен различными факторами, в частности постоянным увеличением объема вредоносного ПО. Непрерывно эволюционируют методы злоумышленников. Услуги хакеров становятся более доступны и часто используются как средство конкурентной борьбы или легкого заработка, что привело к формированию модели Cybercrime-as-a-Service (киберпреступление как услуга).

Киберпреступность – незаконные, противоправные действия, которые осуществляются людьми, использующими информационно-телекоммуникационные технологии, компьютеры и компьютерные сети для преступных целей.

Зависимость бизнес-экосистем от стабильной работы цифровой инфраструктуры делает компании крайне уязвимыми перед ИБ-угрозами. Эффективность атак при этом растет, так как киберпреступники вооружаются цифровыми технологиями, включая ML/AI-решения.

Симметричным ответом мошенникам на использование ИИ станет развитие решений с применением ML/AI для защиты сетей, данных, конечных устройств, доступа, приложений, облаков и пр. По прогнозам,

сегмент ИБ-решений с применением ИИ к 2027 году может составить $46 млрд.

В построении информационной защиты у компаний остается множество узких мест. Так, атаки ведутся комплексно – на экосистемы и цепочки поставок – и противостоять им организованно вместе с партнерами предстоит научиться.

Масштабная цифровизация экономики требует молниеносного time-to-market: в итоге многие приложения и решения выходят в «сыром» небезопасном виде.

В итоге темпы цифровой трансформации опережают развитие ИБ. Сказывается и нехватка специалистов: в мире около 3,5 млн незакрытых вакансий ИБ-специалистов.

Ответом на эти вызовы станет развитие модели «Security-as-a-service» (безопасность как сервис) – эта модель позволяет быстро решить актуальные задачи даже в условиях дефицита кадров. Также для реализации комплексных ИБ-стратегий и защиты экосистем бизнеса будут создаваться объединенные киберцентры — Cyber Fusion Center, объединяющие за одним столом компетенции по ИТ, ИБ, рискам, комплаенсу, экономической безопасности и различным направлениям бизнеса для быстрого реагирования на цифровые риски и угрозы.

Инструменты аналитики будут применяться в сфере информационной безопасности все более активно: это даст возможность эффективнее находить «узкие» места в ИТ-инфраструктуре, быстрее предвосхищать атаки и точнее ранжировать риски.

Развиваются инструменты аналитики киберугроз (Cyber Threat Intelligence и Threat Hunting) и выявления аномалий (Anomaly Detection). Для тестирования гипотез, проверки надежности инфраструктуры и повышения эффективности выявления и прогнозирования кибератак будут создаваться различные варианты кибердвойников ИТ и ИБ инфраструктуры и систем компании.

Киберугроза – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных, целей.

Вырастет востребованность услуг по развитию ИБ-компетенций, включая проведение киберучений и киберполигоны, повышение осведомленности, развитие знаний и навыков пользователей в области ИБ.

Киберполигон - учебно-тренировочная платформа для обучения методам обнаружения, анализа и устранения последствий компьютерных атак.

Также это касается инструментов обеспечения безопасности удаленной работы: инфраструктуры, удаленного подключения и облаков.

ЗАКЛЮЧЕНИЕ

В своей работе я рассмотрела основные аспекты информационной безопасности, привела пример оценки затрат ИБ. Изучила нормативную литературу, а также дополнительные источники информации. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем. Ценность изучения данной темы определена бурным развитием информационных и телекоммуникационных технологий, их активным внедрением в деятельность предприятий и организаций, и вытекающей из этого потребностью защиты информации.

В заключение отмечу, что оптимальные СЗИ наиболее целесообразны для экономически самостоятельных субъектов, которые в своей деятельности вынуждены соблюдать баланс между затратами на СЗИ и возможным ущербом. Реализация таких систем защиты информации возможна при тщательном учете всех аспектов, включая количественную оценку безопасности и размера ожидаемых потерь. Оценка экономически оптимальных параметров должна являться основой формирования конкретного технического облика СЗИ. К сожалению, сегодня проектирование СЗИ обычно осуществляется с ориентацией на произвольно выделяемый бюджет, не имеющий объективного обоснования по системе критериев «стоимость информации — размер возможного ущерба — риски». При этом владелец информационных ресурсов, если не проводит тщательного анализа и не оптимизирует размер выделяемых на СЗИ средств, практически всегда оказывается в экономическом проигрыше.

Экономические аспекты информационной безопасности проявляются при составлении сметы расходов на обеспечение данного типа безопасности, или же при возникновении инцидентов в системе информационной

безопасности, которые приводят к заметным убыткам на предприятии. Оптимальным вариантом является учет всех аспектов при планировании всех мероприятий в сфере защиты информации. На современном этапе методы и решения позволяют создать высокий уровень безопасности, при этом затраты на данные мероприятия могут составлять весьма значительную долю от ИТ-бюджета (для крупных компаний это около 20-30%).

БИБЛИОГРАФИЯ

1. Экономика в информационной безопасности // Справочник от автор 24 URL: https://spravochnick.ru/ (дата обращения: 30.04.2023).

2. Тахтаева Р.Ш., Аргынбеков И.Б., Самыжан К.Н. ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА МИРОВОЙ АРЕНЕ // Фундаментальные исследования. - 2018. - №5. - С. 114-118.

3. ИНФОРМАЦИЯ И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ // Образовательный портал URL: https://obrazovanie-gid.ru/ (дата обращения: 30.04.2023).

4. Туганова Э.А., Мызрова К.А., Захарова Ю.Н., Качагина О.В. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ДРАЙВЕР РАЗВИТИЯ ЭКОНОМИЧЕСКИХ ПРОЦЕССОВ РЕГИОНА В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ // Вестник Алтайской академии экономики и права. - 2023. - №5 (Часть 2). - С. 319-326.