Федеральное государственное образовательное

бюджетное учреждение высшего образования

**«ФИНАНСОВЫЙ УНИВЕРСИТЕТ**

**ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

**ИНСТИТУТ ОТКРЫТОГО ОБРАЗОВАНИЯ**

Кафедра «Информационная безопасность»

**Доклад**

**по дисциплине «Информационная безопасность»**

**на тему: «Подходы к оценке рисков нарушения информационной безопасности»**

Направление подготовки - 09.03.03 «Прикладная информатика»

Студент: Дервук Максим Анатольевич е

(Ф.И.О.)

Курс 5 № группы ЗБ-ПИ20-1 е

Преподаватель: Жарова А. К.

(Ф.И.О.)

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc176333203)

[1. Основные угрозы информационной безопасности 5](#_Toc176333204)

[1.1. Типы угроз 5](#_Toc176333205)

[1.1.1. Кибератаки 5](#_Toc176333206)

[1.1.2. Внутренние угрозы 6](#_Toc176333207)

[1.1.3. Физические угрозы 6](#_Toc176333208)

[1.2. Риски и последствия 7](#_Toc176333209)

[1.2.1. Финансовые потери 7](#_Toc176333210)

[1.2.2. Репутационные риски 7](#_Toc176333211)

[1.2.3. Юридические последствия 8](#_Toc176333212)

[2. Подходы к оценке затрат на обеспечение безопасности информации 8](#_Toc176333213)

[2.1. Анализ рисков 8](#_Toc176333214)

[2.1.1. Оценка вероятности угроз 8](#_Toc176333215)

[2.1.2. Оценка последствий угроз 9](#_Toc176333216)

[2.2. Методы анализа 9](#_Toc176333217)

[2.2.1. Качественный анализ рисков 9](#_Toc176333218)

[1.2.2. Количественный анализ рисков 10](#_Toc176333219)

[2.3. Методы оценки ущерба 10](#_Toc176333220)

[3. Определение целесообразных затрат на безопасность 10](#_Toc176333221)

[3.1. Баланс между затратами и рисками 11](#_Toc176333222)

[3.2. Методы оптимизации затрат 11](#_Toc176333223)

[3.2.1. Анализ стоимости-выгоды (Cost-Benefit Analysis). 11](#_Toc176333224)

[3.2.2. Возврат на инвестиции (ROI). 12](#_Toc176333225)

[3.2.3. Управление остаточным риском: Оценка допустимого уровня риска и решение, какие угрозы можно оставить без внимания. 12](#_Toc176333226)

[ЗАКЛЮЧЕНИЕ 13](#_Toc176333227)

[СПИСОК ЛИТЕРАТУРЫ 16](#_Toc176333228)

**ВВЕДЕНИЕ**

Современная цифровая эпоха характеризуется стремительным ростом объема данных и развитием информационных технологий, что неизбежно увеличивает значимость вопросов информационной безопасности. В условиях глобальной цифровизации, когда все больше бизнес-процессов, коммуникаций и даже критически важных инфраструктурных систем зависят от информационных технологий, обеспечение защиты информации становится одной из главных задач для любой организации. Нарушение информационной безопасности может привести к серьезным последствиям, включая финансовые потери, утрату конфиденциальности данных, а также значительные репутационные риски.

**Проблема** заключается в необходимости определения оптимального уровня затрат на обеспечение безопасности, который должен обеспечивать защиту от угроз, не создавая при этом чрезмерного финансового бремени для организации. Избыточные затраты могут снизить конкурентоспособность компании, тогда как недостаточные меры безопасности могут привести к катастрофическим последствиям.

**Цель** данного доклада — всесторонне рассмотреть методы и подходы к определению целесообразных затрат на информационную безопасность. В процессе исследования будет проанализировано, как можно достичь оптимального баланса между затратами на безопасность и рисками, с которыми сталкивается организация. Также будут рассмотрены методы оптимизации затрат, такие как анализ стоимости-выгоды, расчет возврата на инвестиции и управление остаточным риском.

**Задачи** доклада включают:

* Исследование принципов и методов анализа рисков в контексте информационной безопасности.
* Оценка методов оптимизации затрат, обеспечивающих максимальную эффективность при минимальных ресурсных затратах.
* Предложение рекомендаций по улучшению процессов определения и управления затратами на информационную безопасность.

Данный доклад призван дать четкое понимание того, как организациям следует подходить к планированию и распределению ресурсов на защиту своих информационных систем, чтобы эффективно противостоять современным угрозам и минимизировать возможные риски.

# Основные угрозы информационной безопасности

## Типы угроз

Обеспечение информационной безопасности в организации — это многоуровневый процесс, который сталкивается с множеством различных угроз. Эти угрозы можно классифицировать на несколько категорий в зависимости от их источника и характера.

### Кибератаки

Кибератаки представляют собой одно из наиболее значительных и распространенных направлений угроз для информационной безопасности. Сюда относятся:

* Фишинг: Фишинговые атаки направлены на получение конфиденциальной информации (например, паролей или данных банковских карт) путём обмана пользователя. Злоумышленники создают поддельные веб-сайты или отправляют электронные письма, имитирующие легитимные источники, что побуждает жертву раскрыть свои данные.
* DDoS-атаки (Distributed Denial of Service): В случае DDoS-атак злоумышленники перегружают систему или сеть организации огромным количеством запросов, что приводит к её недоступности для обычных пользователей. Это может существенно повлиять на бизнес-процессы, особенно если атака направлена на онлайн-сервисы, от которых зависит работа компании.
* Вирусы и вредоносное ПО (Malware): Вирусы, черви, трояны и прочие виды вредоносного ПО могут наносить различный ущерб. Они могут похищать данные, нарушать работу систем, шпионить за пользователями или создавать задние двери для последующих атак. Некоторые типы вредоносного ПО, такие как рансомвар (ransomware), шифруют данные и требуют выкуп за их восстановление, что может привести к значительным финансовым потерям.

### Внутренние угрозы

Не все угрозы исходят извне. Внутренние угрозы представляют собой серьёзный риск, поскольку они исходят от лиц, уже имеющих доступ к критически важным системам и данным:

* Недобросовестные сотрудники: Сотрудники могут сознательно или по неосторожности нанести ущерб информационной системе организации. Например, они могут похитить конфиденциальные данные, продав их конкурентам, или несанкционированно использовать служебную информацию в личных целях. В некоторых случаях сотрудники могут случайно удалить важные данные или установить вредоносное ПО на корпоративные устройства.
* Партнёры и подрядчики: Третьи стороны, с которыми сотрудничает организация, также могут представлять угрозу. Например, если подрядчик имеет доступ к внутренним системам компании, то уязвимости в его защите могут быть использованы злоумышленниками для атаки на основную организацию.

### Физические угрозы

Информационная безопасность связана не только с цифровыми, но и с физическими угрозами. К ним относятся:

* Кража оборудования: Если злоумышленники похитят устройства, содержащие конфиденциальные данные (например, ноутбуки, серверы или внешние накопители), это может привести к утечке информации. Несмотря на то, что данные могут быть зашифрованы, физический доступ к устройству предоставляет возможность для их взлома.
* Несанкционированный доступ к помещениям: Физический доступ к серверам, компьютерам или другим устройствам также является угрозой. Злоумышленники могут получить доступ к критически важной информации, если проникнут в офис или дата-центр компании.
* Физическое повреждение оборудования: Пожары, наводнения, и другие стихийные бедствия или умышленные акты вандализма могут уничтожить оборудование, содержащее критически важные данные. Хотя физическое резервирование данных и установка систем защиты помогают минимизировать риск, полное предотвращение таких угроз невозможно.

## Риски и последствия

Последствия угроз информационной безопасности могут быть катастрофическими для организации. Они затрагивают не только её финансовое состояние, но и репутацию, юридический статус и многие другие аспекты.

### Финансовые потери

Финансовые убытки от инцидентов в сфере информационной безопасности могут быть значительными. Они включают:

1. Прямые убытки - это затраты на восстановление после атаки, например, оплата выкупа при ransomware-атаках, затраты на восстановление данных, покупку нового оборудования или программного обеспечения.
2. Упущенная выгода, а именно простой систем или полная их недоступность могут привести к потере прибыли. Например, если интернет-магазин становится недоступен из-за DDoS-атаки, это может привести к потере доходов от продаж.
3. Штрафы и компенсации, если из-за утечки данных пострадали клиенты, организация может быть обязана выплатить компенсации или заплатить штрафы в соответствии с законодательством о защите данных, например, GDPR в Европе.

### Репутационные риски

Репутация компании — один из наиболее ценных её активов. Утечки данных или успешные атаки могут серьёзно подорвать доверие клиентов, партнеров и инвесторов:

* Потеря доверия клиентов: Если клиенты потеряют уверенность в безопасности своих данных, они могут перейти к конкурентам. Восстановление доверия может занять годы и потребовать значительных инвестиций в PR и маркетинг.
* Потеря партнёров и инвесторов: Партнёры и инвесторы могут отказаться от сотрудничества с организацией, если считают её ненадёжной с точки зрения безопасности.

### Юридические последствия

Правовые аспекты безопасности данных становятся всё более жёсткими, и нарушение норм может привести к серьёзным юридическим последствиям:

* Судебные иски: Пострадавшие клиенты или партнёры могут подать иски против компании, если она не обеспечила должную защиту их данных.
* Штрафы за нарушение законодательства: Во многих странах действует жёсткое законодательство в области защиты данных, и нарушение этих норм может привести к значительным штрафам. Например, штрафы по GDPR могут достигать миллионов евро.

# Подходы к оценке затрат на обеспечение безопасности информации

Оценка затрат на обеспечение информационной безопасности требует тщательного анализа рисков, которые могут возникнуть в организации, а также применения различных методов анализа и оценки ущерба. Этот раздел поможет понять, как правильно оценить и оптимизировать расходы на защиту данных и систем.

## Анализ рисков

Анализ рисков является основополагающим этапом в процессе определения целесообразных затрат на безопасность информации. Он направлен на оценку вероятности возникновения различных угроз и их возможных последствий для организации. Это позволяет более точно определить, какие риски требуют приоритетного внимания и какие меры следует принять для их минимизации.

### Оценка вероятности угроз

Для оценки вероятности угроз используются различные методы, которые могут включать как качественные, так и количественные подходы. Основной целью этого этапа является понимание того, какие угрозы наиболее вероятны, чтобы сфокусировать усилия на их предотвращении.

Пример оценки вероятности угрозы можно выразить следующей формулой:

Угроза = Количество случаев реализации угрозы / Общее количество возможных случаев, где угроза – это вероятность того, что угроза реализуется в определённый период времени.

### Оценка последствий угроз

Оценка последствий угроз включает анализ того, какие убытки могут быть понесены в случае реализации той или иной угрозы. Эти убытки могут включать финансовые потери, репутационные ущербы, юридические последствия и другие виды ущерба.

Пример расчета возможного ущерба можно выразить формулой:

Угроза = Активы \* Воздействие, где

Угроза – это потенциальный ущерб, Активы – стоимость затронутых активов, а Воздействие – это коэффициент, отражающий степень воздействия угрозы на активы

## Методы анализа

Существуют различные методы анализа рисков, которые помогают понять, каким образом угрозы могут повлиять на организацию и как их можно предотвратить. Эти методы делятся на качественные и количественные.

### Качественный анализ рисков

Качественный анализ рисков основывается на экспертных оценках и сценарном планировании. Этот метод не требует сложных математических расчётов, но позволяет систематизировать ключевые угрозы и уязвимости.

Сценарное планирование — это процесс, при котором разрабатываются различные гипотетические сценарии, описывающие возможное развитие событий в случае реализации угрозы. Для каждого сценария эксперты оценивают потенциальные последствия и вероятность его реализации.

### Количественный анализ рисков

Количественный анализ рисков предполагает использование математических моделей и статистических методов для вычисления вероятностей и возможных убытков.

Один из методов количественного анализа — это использование модели Монте-Карло, которая позволяет оценить распределение возможных убытков при заданных входных параметрах (вероятность угрозы и возможный ущерб). Формула расчета ожидаемых убытков:

Ожидаемые убытка = Вероятность угрозы \* Возможный ущерб

## Методы оценки ущерба

Методы оценки ущерба играют ключевую роль в определении того, какие финансовые последствия могут возникнуть в случае реализации угроз, и как это отразится на бюджете организации.

##### Прямые финансовые потери

Прямые финансовые потери — это расходы, которые организация несёт непосредственно в результате реализации угрозы. К ним относятся затраты на восстановление систем, замена оборудования, ликвидация последствий утечек данных и т.д. Пример расчета прямых потерь:

Общие финансовые потери = Затраты на восстановление + Затраты на замену оборудования + Затраты на устранение последствий инцидента.

Затраты на восстановление включают расходы на восстановление работы системы после инцидента, например, восстановление данных, восстановление операционных систем и программного обеспечения, а также работу IT-специалистов.

# Определение целесообразных затрат на безопасность

Определение целесообразных затрат на обеспечение информационной безопасности является ключевым элементом стратегического управления рисками. Необходимо найти баланс между затратами на безопасность и возможными рисками, а также использовать методы оптимизации затрат, чтобы максимизировать защиту при минимальных расходах.

## Баланс между затратами и рисками

Одним из основных принципов управления информационной безопасностью является поиск оптимального баланса между затратами на защиту и рисками, которые могут возникнуть в случае недостаточной безопасности. Перерасход средств на меры безопасности может привести к неэффективному использованию ресурсов, тогда как недостаток инвестиций может увеличить вероятность серьезных инцидентов. Для достижения этого баланса важно учитывать следующие факторы:

1. Уровень риска: Анализ вероятности реализации угроз и их последствий для бизнеса.
2. Стоимость мер безопасности: Оценка затрат на внедрение и поддержание различных мер защиты.
3. Допустимый уровень остаточного риска: Определение уровня риска, который организация готова принять, учитывая экономические и стратегические цели.

Пример математического выражения баланса между затратами и рисками может быть представлен через функцию полезности, где организация стремится минимизировать общие расходы:

Затраты на меры безопасности + Ожидаемые убытки, связанные с остаточным риском.

## Методы оптимизации затрат

Для оптимизации затрат на обеспечение безопасности применяются различные методы, которые помогают оценить эффективность мер безопасности и найти наилучшее соотношение между затратами и выгодами.

### Анализ стоимости-выгоды (Cost-Benefit Analysis).

Анализ стоимости-выгоды (CBA) — это метод, который позволяет соотнести затраты на внедрение мер безопасности с предполагаемой выгодой от предотвращения потенциальных инцидентов. Этот анализ помогает определить, стоит ли внедрение определенных мер защиты затрат, которые потребуются для их реализации.

Формула анализа стоимости-выгоды:

*,* где

V – общая выгода от внедрения мер безопасности;

С – затраты на реализацию мер безопасности.

Если CBA>1, то выгоды превышают затраты, и мера безопасности считается целесообразной для внедрения.

### Возврат на инвестиции (ROI).

Возврат на инвестиции (ROI) — это финансовый показатель, который оценивает, насколько вложенные в безопасность средства окупаются за счет предотвращения убытков. Этот показатель важен для принятия решений о выделении средств на информационную безопасность.

Формула расчета ROI:

ROI = (предотвращенные убытки – затраты на меры безопасности)/Затраты на меры безопасности \* 100%

Высокий ROI указывает на то, что затраты на безопасность окупаются и приносят значительную экономическую выгоду

### Управление остаточным риском: Оценка допустимого уровня риска и решение, какие угрозы можно оставить без внимания.

Управление остаточным риском включает оценку допустимого уровня риска, который организация готова принять после внедрения мер безопасности. Этот подход предполагает осознанное решение о том, какие угрозы могут быть оставлены без внимания, если затраты на их устранение превышают допустимые уровни.

Для определения остаточного риска используется следующая формула:

Остаточный риск, который остается после внедрения мер безопасности = общий риск до внедрения мер безопасности – эффективность принятых мер защиты.

Организации должны тщательно взвешивать, какие риски они могут позволить себе оставить без внимания, основываясь на финансовых, операционных и стратегических соображениях.

# ЗАКЛЮЧЕНИЕ

Обеспечение информационной безопасности в современном цифровом мире — это задача, требующая не только значительных ресурсов, но и тщательного планирования и анализа. В условиях постоянно меняющихся технологий и растущих угроз организациям необходимо принимать взвешенные решения, чтобы оптимизировать затраты на безопасность и минимизировать риски, связанные с утечками данных, кибератаками и другими инцидентами.

В рамках данного доклада были рассмотрены ключевые аспекты определения целесообразных затрат на информационную безопасность. Анализ рисков, как качественный, так и количественный, позволяет организациям оценить вероятность возникновения различных угроз и их возможные последствия. Методы оптимизации затрат, такие как анализ стоимости-выгоды, расчет возврата на инвестиции и управление остаточным риском, помогают найти оптимальный баланс между защитой информации и экономической эффективностью.

Существует необходимость в постоянной адаптации и совершенствовании подходов к управлению информационной безопасностью. Важно учитывать не только текущие угрозы, но и прогнозировать будущие риски, чтобы своевременно внедрять необходимые меры защиты.

Таким образом, эффективное управление затратами на информационную безопасность должно быть основано на глубоком понимании рисков и использовании проверенных методов оптимизации. Это позволит организациям не только защитить свои данные и системы, но и обеспечить стабильность и устойчивость в условиях цифровой экономики, минимизируя при этом издержки и повышая общую эффективность.

# **СПИСОК ЛИТЕРАТУРЫ**

1. ФЗ-187 "О безопасности критической информационной инфраструктуры Российской Федерации" от 26 июля 2017 г.
2. ISO/IEC 27001:2022. **Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования.** Международная организация по стандартизации (ISO).
3. Gordon, L. A., & Loeb, M. P. (2020). **Managing Cybersecurity Resources: A Cost-Benefit Analysis.**
4. Артеменко, Е. Г., & Воронин, А. В. (2021). Информационная безопасность в цифровую эпоху.
5. Бурков, В. Н., & Новиков, Д. А. (2019). Управление информационной безопасностью: методы и модели.
6. Григорьев, А. В. (2020). Риски информационной безопасности и их оценка в современных условиях.
7. Ильин, И. В. (2022). Правовые аспекты обеспечения информационной безопасности.
8. Климов, В. А. (2018). Методы анализа рисков и управление затратами на информационную безопасность.