Анализ угроз информационной безопасности

Учебник



БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ
ИМЕНИ И. Д. ПУТИЛИНА

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебник

Санкт-Петербург
Наукоемкие технологии
2026

УДК 004.056.5
ББК 16.8
А64

Авторы:
Е. Г. Ковалева, канд. техн. наук;
В. Л. Акапьев, канд. пед. наук;
А. В. Борисенко, канд. физ.-мат. наук;
Р. А. Дунаев, канд. филос. наук;
А. В. Кузнецов, доктор филос. наук

Рецензенты:
Л. Д. Матросова, кандидат юридических наук, доцент, полковник полиции,
начальник кафедры информационных технологий в деятельности ОВД Орловского юридического института МВД России имени В. В. Лукьянова;
Ю. А. Гончаров, заместитель начальника отдела специальной связи ЦИТСиЗИ УМВД России по Белгородской области

Ковалева, **Е. Г.**
А64 Анализ угроз информационной безопасности: учебник / Е. Г. Ковалева, В. Л. Акапьев, А. В. Борисенко, Р. А. Дунаев, А. В. Кузнецов. – СПб.: Наукоемкие технологии, 2026. – 120 с.

ISBN 978-5-00271-066-9

Учебник посвящен актуальной теме угроз информационной безопасности, отражая ее многообразие и значимость. В первой главе рассматривается понятие угрозы информационной безопасности и ее основные характеристики, что позволяет сформировать общее представление о природе и типах угроз. Вторая глава освещает ключевые принципы классификации угроз информационной безопасности, что помогает понять, как систематизировать угрозы. Третья глава предоставляет обзор универсальных и отраслевых классификаций угроз, а также включает сравнительный анализ существующих систем классификации, что позволяет выявить преимущества и недостатки различных подходов. В заключительной главе учебника представлены формальные модели представления угроз информационной безопасности.

Предназначен для курсантов и слушателей, профессорско-преподавательского состава, слушателей факультета заочного обучения, слушателей факультета переподготовки и повышения квалификации образовательных организаций системы МВД России, лиц рядового состава и младшего начальствующего состава, впервые принятых на службу в органы внутренних дел Российской Федерации по должности служащего «Полицейский», лиц среднего и старшего начальствующего состава, впервые принятых на службу в органы внутренних дел Российской Федерации по должности служащего «Полицейский», имеющих высшее или среднее профессиональное (неюридическое) образование.

Учебное издание

Ковалева Екатерина Геннадьевна
Акапьев Виктор Львович
Борисенко Александр Васильевич
Дунаев Роман Алексеевич
Кузнецов Андрей Владимирович

Анализ угроз информационной безопасности

Учебник

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел Групп»
https://publishing.intelgr.com
E-mail: publishing@intelgr.com
Тел.: +7 (812) 945-50-63

Подписано в печать 01.01.2026.
Формат 60×84/16
Объем 7,5 п.л.
Тираж 500 экз.

ISBN 978-5-00271-066-9

© Ковалева Е. Г., Акапьев В. Л., Борисенко А. В., Дунаев Р. А., Кузнецов А. В., 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ …….. 5
1. ПОНЯТИЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ …….. 7
1.1. Основные термины и определения ……... 7
1.2. Информация, подлежащая защите …… 10
1.3. Перечень объектов информационной безопасности ……... 12
1.4. Нормативные требования по обеспечению информационной безопасности по законодательству Российской Федерации ……. 14
1.5. Анализ концепции угрозы информационной безопасности в различных правовых и технологических экосистемах ……... 26
1.6. Практические примеры анализа угроз информационной безопасности в ЕС, Китае и России ……. 36
1.7. Объектно-ориентированные угрозы информационной безопасности…….. 40
1.8. Источники угроз по классификации MITRE ATT&CK …….. 42
Глоссарий ……... 54
Вопросы и задания для самоконтроля……. 56

2. КЛЮЧЕВЫЕ ПРИНЦИПЫ КЛАССИФИКАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ …….. 58
2.1. Угрозы безопасности информации: понятие и классификация ……. 58
2.2. Угроза ИБ по источнику возникновения …….. 62
2.3. Угроза ИБ по характеру воздействия ……..... 64
2.4. Угроза ИБ по аспекту защищаемой информации ……..... 70
2.5. Угроза ИБ по объекту воздействия …….. 71
Глоссарий…… 74
Вопросы и задания для самоконтроля ……. 76

3. УНИВЕРСАЛЬНЫЕ И ОТРАСЛЕВЫЕ ТАКСОНОМИИ УГРОЗ: ОБЗОР И СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ КЛАССИФИКАЦИИ……... 78
3.1. Введение в таксономии угроз……. 78
3.2. Универсальные таксономии угроз информационной безопасности.. 82
3.3. Отраслевые таксономии и стандарты информационной безопасности……... 84
3.4. Российские таксономические подходы в информационной безопасности……... 88
3.5. Практическое применение таксономий угроз информационной безопасности……... 90
3.6. Перспективы развития таксономий……... 92
Глоссарий…… 94
Вопросы и задания для самоконтроля……. 97

4. ФОРМАЛЬНЫЕ МОДЕЛИ ПРЕДСТАВЛЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: НАЗНАЧЕНИЕ И ПРИМЕРЫ ……... 99
4.1. Назначение и методологическая база формальных моделей информационной безопасности ……... 99
4.2. Модель цепочки кибератаки (Cyber Kill Chain®): таксономия и противодействие многоэтапным угрозам ……... 101
4.3. Матрица MITRE ATT&CK®: таксономия поведения противника как основа проактивной обороны …… 103
4.4. Модель STRIDE: таксономия угроз на этапе проектирования …….. 105
Глоссарий ……... 107
Вопросы и задания для самоконтроля …… 109
ЗАКЛЮЧЕНИЕ ……... 111
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ …….. 113
ПРИЛОЖЕНИЕ 1. Практикум: Разработка модели угроз (Threat Model) для мобильного приложения банка с учётом требований ФСТЭК …….. 119

ВВЕДЕНИЕ

Динамика современного цифрового мира и рост числа кибератак на объекты различного масштаба и назначения (от персональных устройств до критической инфраструктуры) формирует актуальную повестку систематизации знаний о подходах и инструментах для комплексного управления угрозами информационной безопасности (ИБ).

Информационная безопасность необходима для защиты конфиденциальных и ценных данных от несанкционированного доступа, использования, раскрытия, нарушения целостности, изменения или уничтожения.

Информационная безопасность помогает гарантировать, что критически важные функциональные операции будут продолжены в случае чрезвычайной ситуации, например, кибератаки или стихийного бедствия. Без надлежащих мер безопасности данные и системы организации могут быть скомпрометированы, что приведет к значительным простоям и снижению эффективности правоохранительной деятельности.

Кибератаки, такие как заражение вирусами, вредоносным программным обеспечением (ПО), фишинг и программы-вымогатели, становятся всё более изощрёнными и частыми. Информационная безопасность помогает предотвращать указанные атаки и минимизировать их последствия в случае их возникновения.

Организации также обязаны защищать данные о сотрудниках, такие как сведения о заработной плате, состоянии здоровья и личные данные. Эта информация часто становится целью киберпреступников, а ее кража может привести к краже личных данных и финансовому мошенничеству.

В мире цифровых технологий защита конфиденциальной информации стала не просто желательной, а необходимой. Информационная безопасность - это стратегии и технологии, используемые для предотвращения несанкционированного доступа, нарушения работы или кражи данных. Будь то здравоохранение, финансы, образование или государственное управление, организации полагаются на защищённые системы для поддержания доверия и операционной целостности. Но что такое информационная безопасность на практике и почему она так важна сегодня?

Информационная безопасность защищает цифровую и физическую информацию от несанкционированного доступа, использования, раскрытия, нарушения работы, изменения или уничтожения. Она направлена на защиту конфиденциальной информации путём обеспечения её конфиденциальности, целостности и доступности. Сфера её применения включает сетевую, прикладную и операционную безопасность, а также физический и административный контроль. Такой комплексный подход позволяет противостоять угрозам, начиная от кибератак и заканчивая человеческим фактором. Четкое понимание того, что такое информационная безопасность,

помогает организациям применять эффективные меры для защиты активов и поддержания доверия.

Не менее важно соблюдение политики информационной безопасности правоохранительных органов, которая имеет решающее значение для защиты персональных данных, обеспечения бесперебойной работы и укрепления доверия общественности.

Информационная безопасность стала ключевым элементом работы правоохранительных органов. Рост числа киберпреступлений, распространение цифровых доказательств и растущая зависимость полиции от технологий сделали информационную безопасность критически важным компонентом защиты правоохранительных органов и их способности служить обществу и защищать его.

По мере того, как киберпреступники становятся всё более изощрёнными, правоохранительные органы должны укреплять собственную цифровую защиту, чтобы быть на шаг впереди, а также использовать информационную безопасность для борьбы с растущим числом киберугроз.

Информационная безопасность играет важнейшую роль в работе современных правоохранительных органов в эпоху цифровых технологий. Поскольку правоохранительные органы сталкиваются с растущим числом киберугроз и всё больше полагаются на цифровые инструменты и данные, информационная безопасность обеспечивает основу для стабильной работы, эффективности расследований информационных инцидентов, улучшения информационного обеспечения правоохранительной деятельности и защиты конфиденциальной информации.

Настоящее учебное издание посвящено рассмотрению общих положений обеспечения информационной безопасности и нормативных требований по ее обеспечению, а также определению возможных угроз для объектов информатизации подразделений органов внутренних дел (ОВД), методике оценки защищенности данной категории объектов и организации их комплексной защиты.

Учебник разработан в соответствии с Федеральным государственным образовательным стандартом высшего образования, основными образовательными и рабочими программами учебных дисциплин «Информационные системы, технологии и основы информационной безопасности органов внутренних дел» и «Основы кибербезопасности».

ГЛАВА 1. ПОНЯТИЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

1.1. Основные термины и определения

Конфиденциальная данные, включая личную информацию, финансовую отчётность, коммерческие секреты и интеллектуальную собственность, должны быть надёжно защищены от несанкционированного доступа. Эта информация имеет высокую ценность и может быть использована для кражи личных данных, мошенничества или других злонамеренных целей.

Многие сектора экономики, такие как здравоохранение, финансы и государственное управление, подчиняются строгим нормативным требованиям и законам, которые обязывают их защищать конфиденциальные данные. Несоблюдение этих требований может привести к юридическим и финансовым санкциям, а также нанести ущерб репутации организации.

Правоохранительные органы всё чаще подвергаются атакам со стороны киберпреступников и недружественных государственных структур. Программы-вымогатели могут выводить из строя диспетчерские системы, утечка данных может поставить под угрозу конфиденциальных информаторов, а фишинговые атаки могут лишить сотрудников доступа к критически важным инструментам управления делами.

В связи с тем, что для эффективной защиты информации необходимо, чтобы и законодатель (разработчик руководящих документов в заданной области) и лицо, ответственное за защиту информации на конкретных объектах, и контролирующий орган «говорили на одном языке». Для этого целесообразно определить и рассмотреть понятийную область, используемую в работе, на примере основных терминов и определений [67].

Информационная безопасность (InfoSec) - это защита важной информации от несанкционированного доступа, раскрытия, использования, изменения или нарушения. Она помогает обеспечить доступ к конфиденциальным данным организации для уполномоченных пользователей, а также сохранить конфиденциальность и целостность данных [27].

Нам необходимо защищать информационные активы, которые могут включать в себя финансовые, конфиденциальные, персональные данные, сведения ограниченного распространения или содержащие государственную тайну. Эти активы могут представлять собой цифровые файлы и данные, бумажные документы, физические носители и даже человеческую речь. На протяжении всего жизненного цикла данных InfoSec контролирует такие функции, как инфраструктура, программное обеспечение, тестирование, аудит и архивирование [25].

Информационная безопасность, основанная на принципах, которым уже несколько десятков лет, постоянно развивается, чтобы обеспечить защиту все более гибридных и мультиоблачных сред в условиях постоянно меняющегося ландшафта угроз. Учитывая, что характер этих угроз меняется, для

обновления технологий и процессов, используемых для защиты, необходимо взаимодействие нескольких команд [28].

Защита информации - это целенаправленная деятельность по предотвращению утечки защищаемой информации, а также по недопущению несанкционированных и непреднамеренных воздействий на нее [36].

Защита информации (или информационная безопасность, согласно определению Национального института безопасности и стандартов) - это защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения работы, изменения или уничтожения [4].

Технический канал утечки информации (ТКУИ) - представляет собой совокупность объекта разведки, технического средства разведки (ТСР), используемого для получения информации об этом объекте, и физической среды, в которой происходит распространение информационного сигнала [21].

Несанкционированный доступ к информации - это доступ к информации, осуществляемый с нарушением установленных правил разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Защита информации от утечки - это комплекс мер, направленных на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на создание существенных препятствий для получения защищаемой информации иностранными разведками и другими заинтересованными субъектами.

Защита информации от несанкционированного доступа - это защита информации, нацеленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами прав или правил разграничения доступа к защищаемой информации [31].

Техническая защита информации - это защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [73].

Физическая защита информации - это защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты [39].

Безопасность информации (данных) - это состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Безопасность данных представляет собой практику защиты цифровой информации от несанкционированного доступа, повреждения или хищения на протяжении всего жизненного цикла данных. Она включает физическую

защиту оборудования и устройств хранения данных, а также административный контроль и управление доступом. Кроме того, она охватывает логическую защиту программных приложений, организационные политики и процедуры [38].

Защищаемая информация - это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Объект информатизации - это совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [19].

Защищаемый объект информатизации - это объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

Объект защиты информации - это информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Угроза (безопасности информации) - это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Охраняемые сведения - это сведения, содержащие государственную тайну или сведения, отнесенные к другой категории конфиденциальной информации.

Технический демаскирующий признак объекта - это характерное свойство объекта защиты, которое может быть использовано технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем.

Автоматизированная система (АС) - это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций [20].

Средства вычислительной техники (СВТ) - это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Штатные средства - это совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Выделенное помещение (ВП) - это специальное помещение, предназначенное для проведения собраний, совещаний, бесед и других мероприятий речевого характера по секретным или конфиденциальным вопросам.

Способ защиты информации - это порядок и правила применения определенных принципов и средств защиты информации [75].

Фактор, воздействующий на защищаемую информацию - это явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Термины «информационная безопасность», «ИТ-безопасность», «кибербезопасность» и «защита данных» часто (и не совсем корректно) используются как взаимозаменяемые. Хотя эти области имеют точки пересечения и дополняют друг друга, они различаются, в первую очередь, по охвату решаемых задач.

Информационная безопасность - это общий термин, обозначающий меры, принимаемые организацией для защиты информации. Он включает физическую защиту ИТ-активов, защиту конечных устройств, шифрование данных, сетевую безопасность и многое другое [77].

Информационная безопасность также подразумевает защиту физических и цифровых ИТ-активов и центров обработки данных, но не включает защиту бумажных документов и других аналоговых носителей информации. Она ориентирована на защиту технологических активов, а не самой информации как таковой [24].

Кибербезопасность сосредоточена на защите цифровых информационных систем. Основная цель состоит в защите цифровых данных и активов от киберугроз. Несмотря на масштабность решаемых задач, сфера применения кибербезопасности ограничена, поскольку она не связана с защитой бумажных или аналоговых данных [74].

1.2. Информация, подлежащая защите

Для обеспечения эффективной защиты информации, с которой ведется работа в органах внутренних дел, необходимо, прежде всего, определить, какая же из всей циркулирующей в ОВД информации подлежит защите. При этом основные требования по защите информации будут непосредственно определяться степенью ее конфиденциальности [4].

Существуют различные признаки, по которым осуществляется классификация информации. С точки зрения организации защиты целесообразно начать с ее классификации по категории доступа [57].

В статье 5 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ указано: «Информация в зависимости от категории доступа к ней подразделяется на **общедоступную информацию**, а также на информацию, доступ к которой ограничен федеральными законами **(информация ограниченного доступа)**»[1].

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную (в том числе, имеющую пометку «для служебного пользования»). Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «О государственной тайне». Перечень сведений, отнесенных к государственной тайне, опубликован в ст.5 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне»[2]. Конкретные перечни сведений, подлежащих засекречиванию, разрабатываются и вводятся в действие соответствующими ведомственными приказами. Существует три степени секретности такой информации:

- особой важности;
- совершенно секретно;
- секретно.

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Определение состава защищаемой информации представляет собой первоначальный этап построения системы защиты. От точности его выполнения зависит эффективность функционирования разрабатываемой системы. Общий подход состоит в том, что защите подлежит вся конфиденциальная информация, то есть сведения, составляющие государственную тайну, информация, составляющая коммерческую тайну, и служебная информация. При этом конфиденциальная информация должна защищаться от утечки и утраты [64].

К информации, нашедшей свое отражение в различных физических полях, относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Это, как правило, **информация ограниченного доступа**, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера или служебные сведения.

[2] Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (последняя редакция) // СПС «КонсультантПлюс».

1.3. Перечень объектов информационной безопасности

Перечень объектов информационной безопасности необходимо рассматривать как систему, которую лучше всего анализировать с двух ключевых точек зрения:

- законодательной (нормативно-правовой);
- практической (бизнес-ориентированной).

С точки зрения законодательства Российской Федерации[3] выделяются следующие объекты, требующие особой защиты и подчиняющиеся строгим нормам:

1. Персональные данные (ПДн).

Объект: любая информация, относящаяся к прямо или косвенно определенному физическому лицу.

Примеры: ФИО, паспортные данные, место работы, биометрия, медицинская информация, переписка, история покупок, IP-адрес (в некоторых случаях).

2. Объекты критической информационной инфраструктуры (КИИ).

Объект: автоматизированные системы управления и информационные системы, используемые в критически важных сферах государства.

Сферы-примеры (по ФЗ-187):

- здравоохранение;
- транспорт;
- связь;
- финансовый рынок;
- топливно-энергетический комплекс;
- атомная энергетика;
- оборонная промышленность;
- космическая деятельность и др.

3. Государственная тайна.

Объект: защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной деятельности, распространение которых может нанести ущерб безопасности РФ.

4. Коммерческая тайна (ноу-хау).

Объект: сведения любого характера (производственные, технические, экономические, организационные и иные), которые имеют действительную или потенциальную коммерческую ценность, неизвестны третьим лицам и к которым нет свободного доступа.

С практической (бизнес-ориентированной) точки зрения, определяя объекты информационной безопасности, необходимо ответить на вопрос: «Что мы защищаем внутри организации?».

[3] ФЗ-152 «О персональных данных», ФЗ-187 «О безопасности КИИ» и др.

Категория 1. Информационные активы (сама информация).

Конфиденциальная информация:

– персональные данные клиентов и сотрудников;
– финансовая отчетность, бизнес-планы, бюджеты;
– договоры, коммерческие предложения, переговоры;
– патенты, чертежи, исходный код, технологии (ноу-хау);
– внутренняя переписка руководства.

Информация, представляющая операционную ценность:

– базы данных клиентов, поставщиков.
– архивы проектов, документация.
– маркетинговые исследования, аналитика.
– расписания, планы работ.

Публичная информация требует защиты от несанкционированного изменения (дефейс сайта, подмена данных).

Категория 2. Технические активы (носители и системы обработки).

Аппаратное обеспечение:

– серверы, рабочие станции, ноутбуки, мобильные устройства;
– сетевое оборудование (маршрутизаторы, коммутаторы, МФУ);
– системы хранения данных (NAS, SAN);
– средства криптографической защиты (СЗИ, HSM).

Программное обеспечение:

– операционные системы, системы управления базами данных (СУБД);
– прикладное ПО (1С, CRM, ERP, офисные пакеты);
– средства разработки, системы автоматизации;
– прошивки (firmware) оборудования.

Инфраструктурные компоненты:

– каналы связи (оптоволокно, спутниковые, радиоканалы);
– центры обработки данных (ЦОД);
– системы электропитания и кондиционирования.

Категория 3. Человеческий фактор (субъекты информации).

Сотрудники организации:

– ошибки (неаккуратные действия могут привести к утечке информации или другим угрозам);

– социальная инженерия (манипуляция сотрудниками для получения доступа к защищенным ресурсам).

Партнеры и контрагенты, которые имеют ограниченный доступ к ресурсам компании (уровень доступа, безопасность взаимодействия).

Клиенты и пользователи. Данные клиентов должны быть защищены, а их действия – контролируемы в рамках предоставленного доступа.

Категория 4. Процессы и услуги.

Бизнес-процессы:

– процессы, зависимые от ИТ (например, онлайн-платежи, логистика, управление производством).

Услуги:

– доступ в интернет, электронная почта, облачные сервисы (SAAS);
– веб-сайты, порталы государственных услуг;
– системы дистанционного банковского обслуживания.

Классическая триада CIA (целостность, доступность, конфиденциальность) является основополагающей концепцией защиты информации. Все рассмотренные объекты, подлежащие защите, должны обеспечить три обязательных свойства:

1. Конфиденциальность (Confidentiality).

Обеспечивает доступ к информации исключительно авторизованным пользователям.

2. Целостность (Integrity).

Гарантирует точность и полноту информации, защиту от несанкционированного изменения. Поддержание целостности важно для их надежности и достоверности.

3. Доступность (Availability).

Обеспечивает доступ авторизованных пользователей к информации и связанным с ней активам в любое время, когда это необходимо.

Полный перечень объектов ИБ в организации формируется на стыке требований закона (что защищать обязаны) и бизнес-потребностей (что защищать необходимо для выживания и развития). Он включает в себя не только файлы с данными, но и всю технологическую цепочку их обработки, а также людей и процессы, с ними связанные [5].

1.4. Нормативные требования к обеспечению информационной безопасности по законодательству Российской Федерации

В процессе реализации действующих требований по обеспечению информационной безопасности (ИБ) на практике возникает один вопрос: какой результат мы получим, так как наша задача состоит не в выполнении бумажных требований, а в том, чтобы информационные системы компании или организации не были взломаны и действия по обеспечению информационной безопасности приносили необходимый результат? А этот результат был оптимально достижим с тем, чтобы затраты на выполнение нормативных требований по ИБ не превышали тот потенциальный ущерб, который может быть в случае невыполнения этих требований. Основная задача: найти баланс между нормативными требованиями и результативной ИБ [65].

В так называемом «трехглавом» законе «Об информации, информационных технологиях и защите информации» четко оговаривается, что обладатель информации обязан принимать меры по защите информации. И только в отдельных случаях, которые установлены законодательством Российской Федерации, мы обязаны защищать информацию или какие-то иные информационные активы, как нам это предписывает государство, тот

или иной государственный орган – регулятор, который определяет правила по ИБ[4].

Во всех остальных случаях, когда государство не устанавливает обязательных требований, обладатели информации вольны самостоятельно выбирать те стандарты, подходы, которыми они будут руководствоваться при построении, мониторинге, эксплуатации системы информационной безопасности в своей организации или предприятии[5].

Таким образом, требования по защите выбираются:

- на основе законодательных актов;
- на основе ведомственных стандартов и приказов;
- самостоятельно.

Основных законов по защите информации, принятых в Российской Федерации, на самом деле не так и много, потому что векторов регулирования всего семь [10]. В составе законодательных актов, устанавливающих обязательные требования по кибербезопасности, в первую очередь необходимо выделить Федеральный закон «О персональных данных» № 152-ФЗ, регламентирующий обязательные требования по защите персональных данных субъектов информационного взаимодействия[6]. Под него разработаны соответствующие подзаконные акты, а именно - постановления Правительства, ведомственные приказы и т.д. Причем необходимо обратить внимание на тот факт, что этот закон о персональных данных, а не о защите персональных данных.

Очень часто наши регуляторы подменяют два понятия: защита прав субъектов персональных данных и защита самих персональных данных. Защита персональных данных - это только небольшая часть от всего набора мероприятий, которые защищают наши права, ведь мы все субъекты персональных данных. Но иногда имеет место некий перекос: ведь защищать права у нас не всегда любят, умеют и хотят, а вот защитить некую сущность, установить какие-то ограничительные требования по защите самих персональных данных и ответственность за утечки, связанные с персональными данными, законодатель всегда готов, поэтому буйным цветом расцветает наше законодательство [74].

При этом иногда регуляторы и законодатели подменяют некоторые термины, но специалисты в области информационной безопасности должны четко разбираться, в чём отличие защиты прав субъектов от защиты самих персональных данных [66].

Федеральный закон «Об информации, информационных технологиях и о защите информации» выступает основополагающим нормативным актом в

---

[4] Ст. 6 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // СПС «КонсультантПлюс».
[5] Ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // СПС «КонсультантПлюс».
[6] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

том, что касается защиты информации. Он задает правовое направление, касающееся охраны информации в государственных информационных системах (ГИС) и государственных информационных ресурсов. На основе закона разрабатываются ключевые подзаконные акты, такие как Приказ ФСТЭК России от 11.02.2013 № 17[7] и Постановление Правительства РФ №676 по вводу в эксплуатацию государственных информационных систем[8]. Кроме того, данный закон предшествует разработке моделей угроз, их согласованию с ФСТЭК и ФСБ[9], а также формированию технических заданий по требованиям защиты информации. Это стало основой для развития открытых конкурсов по поиску уязвимостей, известных как баг-баунти (от англ. bug bounty). Все публичные государственные информационные системы обязаны участвовать в программе баг-баунти, прежде чем они будут введены в эксплуатацию [50].

Также необходимо выделить Федеральный закон № 187[10] со значительным количеством подзаконных актов по безопасности критической инфраструктуры[11]. Имеет место Федеральный закон № 161 по национальной платежной системе[12] и в его составе статья 27, посвященная обеспечению защиты в платежных системах. Стоит отметить закон № 395-1 «О банках

[7] Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // СПС «КонсультантПлюс».

[8] Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // СПС «КонсультантПлюс».

[9] Постановление Правительства РФ от 18.09.2012 № 940 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю» // СПС «КонсультантПлюс».

[10] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ // СПС «КонсультантПлюс».

[11] Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»; Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изм. и доп., вступ. в силу с 21.03.2023) // СПС «КонсультантПлюс».

[12] Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

банковской деятельности»[13], который наделяет Центральный банк правом регулировать вопросы защиты информации в кредитных организациях, а в кредитной организации обязаны эти требования выполнять. Закон о Центральном банке[14] обязывает выполнять и некредитные финансовые организации требования ЦБ, согласованные с ФСТЭК и ФСБ по вопросам защиты информации [49].

Нельзя обойти стороной и нашумевший майский указ Президента №250[15], который установил и новые требования по практической результативной ИБ, и требования по наличию заместителей генеральных директоров и руководителей организации, которые отвечают за кибербезопасность в организации, тем самым подняв тему информационной безопасности на более высокий уровень.

Имеется закон о коммерческой тайне[16], но он очень по касательной затрагивает проблему защиты информации, потому что, с одной стороны, да, есть коммерческая тайна и её надо соблюдать, защищать и т.д., но в законе чётко прописано, что требования по защите информации устанавливает сам обладатель, владелец этой самой коммерческой тайны. И хотя раньше в 2006 году были приняты для служебного пользования (ДСП) требования ФСТЭК по защите коммерческой тайны[17], они не получили широкого распространения. Складывается странная ситуация: есть коммерческая тайна и правообладатель готов защищать свои права в суде в случае ее утечки, но ему придётся самостоятельно реализовывать режим коммерческой тайны и самостоятельно разрабатывать меры по защите этой самой коммерческой тайны, хотя можно ориентироваться и на существующие приказы ФСТЭК и ФСБ, взяв из них то, что лучше всего подходит для решения конкретных задач [47].

Важный и необходимый, для тех специалистов, которые обрабатывает сведения, составляющие государственную тайну - закон № 5485-1 «О государственной тайне»[18]. Стоит упомянуть про разработку указа Президента

---

[13] Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1 (последняя редакция) // СПС «КонсультантПлюс».

[14] Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 № 86-ФЗ// СПС «КонсультантПлюс».

[15] Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

[16] Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ (последняя редакция) // СПС «КонсультантПлюс».

[17] «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006 г. // СПС «КонсультантПлюс».

[18] Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (последняя редакция) // СПС «КонсультантПлюс».

РФ по государственной системе защиты информации в РФ[19]. В случае его принятия законодательная сфера в области информационной безопасности получит дополнительное ускорение, потому что Проект распространяется не только на организации, которые являются государственными (госкорпорации, госорганы, муниципальные организации и др.), но и распространяет требования по защите информации на все организации, обрабатывающие информацию, обладателям которой является государство, то есть и на коммерческие в том числе. Соответственно, в состав этих требование войдет и аттестация, и обязательная сертификация.

Идет речь если не о переделе рынка информационных услуг, то о необходимости коммерческих организаций, которые сотрудничали с государством, но защищали информацию так как считали нужным, кардинально пересматривать свои отдельные подходы и требования по защите информации.

Необходимо остановиться на основополагающих приказах, детально описывающих требования по информационной безопасности. Стоит начать с приказа № 17 ФСТЭК по защите государственных и муниципальных информационных систем. Документ публичный и доступен как на сайте ФСТЭК, так и на сайтах различных правовых систем. Практика подсказывает, что лучше ориентироваться на сайты правовых систем, так как на них документы размещены в более актуальной версии, не содержащие каких-либо ошибок. Нужно признать, что на сайтах регуляторов далеко не всегда документы своевременно и оперативно обновляются, и там иногда встречаются отдельные ошибки [5].

Приказ № 21 ФСТЭК регулирует защиту персональных данных, обрабатываемых в информационных системах персональных данных[20]. Он применяется для всех коммерческих операторов персональных данных, потому что для государственных структур, в которых персональные данные обрабатываются в ГИС, применяются требования приказа № 17 ФСТЭК.

Помимо приказа № 21 ФСТЭК по линии персональных данных действует еще ряд документов других регуляторов. Например, у Министерства цифрового развития, связи и массовых коммуникаций РФ по биометрическим персональным данным издан приказ № 930[21].

---

[19] Проект Указа Президента РФ «Об утверждении Положения о государственной системе защиты информации в Российской Федерации» (размещен на Федеральном портале проектов нормативных правовых актов 23.01.2023)

[20] Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс».

[21] Приказ Минцифры России № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических

Приказ № 31 ФСТЭК[22] по защите информации в информационных системах, связанных с оборонно-промышленным комплексом. В отличие от трех предыдущих документов, которые являются открытыми, этот приказ относится к категории ограниченного доступа.

Приказы № 235[23] и № 239[24] ФСТЭК России устанавливают требования к созданию субъектами критической информационной инфраструктуры (КИИ) Российской Федерации систем безопасности значимых объектов КИИ и по обеспечению их устойчивого функционирования.

Приказ № 378 ФСБ России по криптографической защите персональных данных[25].

Приказ № 524 ФСБ по криптографической защите информации в государственных информационных системах[26]. Необходимо обратить внимание на нестыковки данного документа с приказом № 17 ФСТЭК в части классификации информационных систем, поэтому на практике не просто сочетать эти два документа.

Отдельную группу представляют национальные стандарты в области кибербезопасности, разработанные банком России. Начнем с ГОСТ 57580.1[27], устанавливающего базовый набор защитных мер для финансовых кредитных

лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» // СПС «КонсультантПлюс».

[22] Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // СПС «КонсультантПлюс».

[23] Приказ Федеральной службы по техническому и экспортному контролю от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» // СПС «КонсультантПлюс».

[24] Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

[25] Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» // СПС «КонсультантПлюс».

[26] Приказ ФСБ РФ от 24.10.2022 № 524 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» // СПС «КонсультантПлюс».

[27] ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200146534 (дата обращения: 04.03.2025).

и некредитных организаций. По своей сути и идеологически он не имеет значительных отличий от требований ФСТЭК и расходится только в количестве этих требований: в приказах ФСТЭК их насчитывается порядка полутора сотен, в зависимости от приказа, а у ЦБ их около четырех сот. Сами требования почти идентичны, но различия заключаются в уровне детализации и разъяснениях по реализации заявленных требований [9].

Также имеют место отдельные положения Банка России по частным вопросам защиты информации в различных контурах: при переводе денежных средств, в рамках национальной платёжной системы, в кредитных и не кредитных финансовых организациях, на участке платежной системы банка России и т.д. В таких документах, которых достаточно много, указаны базовые требования, обязательные для всех, и отсылка на выполнение требований ГОСТа 571780.1.

Есть основания считать, что в текущем году многие документы ЦБ обновятся в части обязательных ссылок на принятые в конце декабря 2022 года два ГОСТа 57580.3[28] и 575804[29], соответственно регулирующие вопросы операционной надежности и нейтрализации рисков реализации информационных угроз. Указанные ГОСТ формируют, с точки зрения Центрального Банка, две линии обеспечения кибербезопасности.

Нельзя не упомянуть международные требования стандарта PCI DSS[30] от PCI council, требования SWIFT Cyber Security Program, которые распространяются на финансовые организации, подключенные к SWIFT, и другие очень узкие или отраслевые требования, которые нельзя отнести к всеобъемлющим и представляющим интерес только для организаций, работающим в конкретной сфере деятельности [5].

Таких подходов, стандартов и проектов передового опыта может быть достаточно много. Это могут быть и российские требования, и зарубежные, которых значительно больше, потому что за рубежом подход к организации информационной безопасности отличается от отечественного: помимо чисто обязательной истории, применимой к отдельным видам организаций, есть и большой пласт энтузиастов - коммерческих и некоммерческих организаций, которые разрабатывают какие-то лучшие практики[31] и учат их сочетать с

---

[28] Национальный стандарт РФ ГОСТ Р 57580.3-2022 «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения» // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200194981 (дата обращения: 18.03.2025).

[29] ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер» // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200194982 (дата обращения: 22.03.2025).

[30] PCI DSS (Payment Card Industry Data Security Standard) - стандарт безопасности данных индустрии платежных карт.

[31] Лучшая практика (англ. best practice) - формализация уникального успешного практического опыта.

требованиями законодательства. Так сложилось исторически, что в России инициативных разработчиков, да и самих общепризнанных стандартов, не так много [11].

Хотя в последнее время в отрасли ИБ наметилась тенденция использования России платформ подобных Github для совместной работы появляются сообщества, которые ставят перед собой задачу разработки проектов в области информационной безопасности, которые не противоречат требованиям российского законодательства, так как в текущей геополитической ситуации западные стандарты нам не всегда подходят[32].

Все в значительной степени зависит от развивающейся в мире ситуации, но необходимо помнить, что, если государство не установило какие-то обязательные требования, либо эти требования не полны, специалисты и руководители должны ориентироваться на иные практики и рекомендации в области ИБ, которые существуют в мире.

К лучшим практикам (стандартам) с требованиями по защите принято относить:

ISO 270xx[33];
NIST CSF[34];
ASD 4 / 8 / 37 защитных мер;
CIS Controls (Top 20)[35];
CoBIT;
ITIL;
O-ISM3 и другие.

Исторически одними их первых в России появились Требования по защите информации в государственных информационных системах[36], которые в дальнейшем были расширены на муниципальные информационные системы и на все системы, обрабатывающие информацию, собственником которых является государство. Такие действия указывают на то, что государство хочет контролировать и устанавливать требования в отношении тех информационных активов, которыми оно обладает. При этом не важно, где эти

[32]Гитхабификация Информационной Безопасности // https://habr.com/ru/companies/microsoft/articles/487584/

[33] ISO/IEC 27000 - серия международных стандартов, включающая стандарты по информационной безопасности, опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC).

[34] NIST Cybersecurity Framework (CSF) - это добровольная платформа, которая состоит из стандартов, рекомендаций и рекомендаций по управлению рисками, связанными с кибербезопасности.

[35] CIS TOP 20 Controls - это базовый набор действий, которые в совокупности нацелены на защиту от наиболее распространенных атак на предприятия и их системы безопасности.

[36] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (в редакции приказа ФСТЭК России от 15.02.2017 № 27, от 28.05.2019 № 106) // СПС «КонсультантПлюс».

активы располагаются: в государственных органах, муниципальных структурах или коммерческих организациях [5].

При наличии требований и стандартов возникает вопрос о том, как определить требования по защите. Проблема в том, что регулирующие документы не содержат только сплошной перечень требований, так как их набор зависит от ряда условий. В основном определяющими, какие требования по защите необходимо реализовать, являются два условия:

- актуальные угрозы;
- значимость или ценность информационной системы или обрабатываемой в ней информации.

Соответственно, в зависимости от того, как будут определены актуальность угроз и значимость информации, будет получен класс, уровень или категория информационной системы или объекта информационной инфраструктуры. Если речь идет о персональных данных, то это Постановление Правительства № 1119[37], в котором говорится о том, что существуют уровни защищённости персональных данных. В случае со 149-ФЗ и, соответственно, с приказом № 17 ФСТЭК речь идет о классах защищённости, например, ГИС, АСУТП. В ГОСТах Центрального Банка речь также идет о классах защищенности. В отношении информационных систем персональных данных (ИСПДн) – это уровни защищенности.

Когда речь заходит об объектах критической информационной инфраструктуры, то, опираясь на Постановление Правительства № 127[38], необходимо определять категории значимости объектов критической информационной структуры (КИИ) от одной до трёх. Существует и четвертая категория, к которой относят незначимые объекты, на которые каких-то обязательных требований в области законодательства по информации защите не распространяется, но, если этот объект относится и к ИСПДн, и к какому-либо классу АСУТП или ГИС, на него будут в обязательном порядке распространяться соответствующие требования к ИСПДн, АСУТП, ГИС, либо требование ГОСТа Банка России.

Соответственно, в каждом из ранее упомянутых приказов или иных уровней нормативных актов описана процедура определения актуальности угрозы. Это может быть либо высокоуровневая процедура, как в Постановлении Правительства № 1019, либо детальная процедура как в методике оценки угроз ФСТЭК, либо пока не очень детальная процедура оценки рисков как в документах Центрального банка [5].

---

[37] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СПС «КонсультантПлюс».

[38] Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СПС «КонсультантПлюс».

Но каждая из этих процедур позволяет определить перечень того, что является для нас недопустимым, то есть какие недопустимые события требуется сделать невозможными в нашей организации. В дальнейшем можно будет определить, как эти недопустимые события, эти угрозы могут быть реализованы в нашей инфраструктуре и какие элементы инфраструктуры будут задействованы, то есть какие целевые ключевые системы может задействовать хакер, чтобы осуществить несанкционированное воздействие в отношении конкретной инфраструктуры, бизнеса или госуправления [8].

Затем по простой процедуре, описанной в документах регуляторов, определяется значимость или ценность систем или информации и, опираясь на эти два параметра, регуляторы предлагают очень простую формулу определения конкретного уровня защищенности или класса защищенности, для которого предлагается (не требуется, а предлагается) выбирать защитные меры.

И это достаточно важный момент, который следует рассмотреть отдельно, так как описанные выше четыре или три класса защищенности информационных систем – это очень грубая трактовка. Очевидно, что на практике системы очень разные. И, даже работающие в одной сфере системы, могут иметь различную реализацию, использовать разные информационные технологии, разные правила политики ИБ и т.д. Поэтому невозможно унифицировать все действия по обеспечению информационной безопасности, как невозможно заставлять всех их выполнять. В этом как раз и заключается некая свобода творчества, которую предоставили все регуляторы администрации и специалистам в области информационной безопасности [10].

Раньше такого не было и где-то до 2012 года действовали жесткие требования, которые надо было реализовывать в любых случаях. Например, действовало правило ФСТЭК, по которому пароль должен быть не менее восьми символов. Возникала проблема: как на смартфоне или телефоне, с помощью которых ведется обработка персональных данных, имеющих пин, максимум, из четырех символов, выполнить требование на восемь символов? То есть физически выполнить это требование на подобных устройствах было невозможно. Естественно, что перечень таких примеров можно продолжать очень долго. Возникали десятки-сотни различных ситуаций, поэтому регуляторы пошли навстречу и приняли решение, согласно которому будет предложен каталог защитных мер, из которого можно выбирать то, что важно, нужно, полезно и позволит выполнить требования законодательства и защититься от угроз недопустимых событий [82].

Но, поскольку далеко не все обладают нужной квалификацией, чтобы самостоятельно выбрать из двухсот или четырехсот, если речь идет о Центральном Банке, защитных мер релевантные, регуляторы пошли по пути разработки базового, или рекомендуемого, набора защитных мер, тем самым оказывая помощь, на что стоит ориентироваться, если субъект ИБ не готов тратить время, ресурсы на составление своего уникального перечня защитных мер, которые подходят именно ему.

Поэтому в настоящее время сформировалось два пути выбора защитных мер. Первый заключается в том, чтобы взять базовый набор средств ИБ и его реализовывать. Второй вариант - сделать нечто под себя и реализовывать то, что адекватно для конкретной структуры. Тем самым находится некий баланс между требованиями законодательства и затратами на его реализацию [5].

Но есть и второй вопрос. Практически во всех документах говорится о необходимости включения в базовый набор защитных мер защиту Wi-Fi, но, если нет Wi-Fi, зачем его туда включать? Зачем реализовывать мероприятия по мониторингу беспроводного эфира, внедрению беспроводных систем обнаружения вторжения, разграничения доступа и так далее?

Приведенные примеры показывают, почему не всегда срабатывает базовый набор, поэтому в ряде случаев, а, может быть, и в большинстве случаев, рекомендуется самостоятельно разработать набор защитных мер и, в случае с Wi-Fi, его просто исключают из базового набора, потому что такая технология не используется [81].

Возможны различные решения и, главное, все действующие сегодня приказы, стандарты, требования позволяют реализовать этот подход. Ошибочно рассуждать о том, что регулирующие документы не позволяют реализовать те или иные меры защиты информации. Это не так. Документы позволяют реализовать всё, что необходимо, просто с ними надо внимательно работать и с их помощью реализовать защитную меру. Не внедрить какой-то продукт, а реализовать защитную меру, а она может быть реализована по-разному: и с помощью продуктов, и сервисов, и т.д. Конечно, проще всего применять готовый инструментарий, который автоматизирует рутинные задачи и обладает всеми необходимыми регалиями от регуляторов, либо по линии ФСТЭК, либо по линии ВСБ, либо по линии Минобороны в зависимости от какие требования на принимаемые решения распространяются.

Данное решение принимается на усмотрение субъекта ИБ, который может использовать любой из описанных сценариев за редким исключением, когда устанавливается, что для решения той или иной задачи необходимо применять определенный класс продуктов или этот класс продуктов должен соответствовать определенным требованиям и требуется подтверждение выполнения указанных требований.

Такое подтверждение может быть реализовано самостоятельно в виде добровольной сертификации, или оценки соответствия, или испытания. Либо это обязательная сертификация, когда необходимо сдать в испытательную лабораторию, имеющую аккредитацию ФСТЭК, либо Минобороны, либо ФСБ, и будут проведены все необходимые испытания и выдан сертификат о соответствии предъявляемым требованиям.

Необходимо учитывать требования различных устанавливающих документов. В некоторых предъявляются требования к реализации той или иной защитной меры, но, в большинстве случаев, принятие решения остается за субъектом ИБ, потому что заранее не всегда можно жестко прописать

способы защиты той или иной информации, информационной системы, того или иного процесса и в этом плане творческий подход помогает реализовывать, с одной стороны, требования законодательства, с другой стороны, сделать это сбалансировано с учетом имеющихся ресурсов и возможностей хакеров, которые против вас действуют [11].

И, наконец, а что, если ничего не делать? Этот закономерный вопрос, который в Российской Федерации звучит не только в части кибербезопасности, имеет также очевидный ответ: все под ответственность субъекта ИБ.

Действующее законодательство предусматривает:

- административную ответственность (ст.13.11, 13.12, 19.5, 19.7 КоАП РФ);
- уголовную ответственность (ст.137, 138, 159, 183, 272-274, 171 УК РФ);
- дисциплинарную ответственность (ст. 81, 90, 195, 237 ТК РФ);
- гражданскую ответственность (ст. 1095 ГК РФ).

На практике самый распространенный вариант связан с наступлением административной ответственности. В Кодексе Российской Федерации об административных правонарушениях имеются отдельные статьи, которые за невыполнение требований по информационной безопасности предусматривают штрафные санкции. В настоящее время планируется введение оборотных штрафов за, например, утечки персональных данных, что может радикально изменить сложившуюся ситуацию.

Существует уголовная ответственность за нарушение правил эксплуатации объектов КИИ при нанесении ущерба таким объектам, за утечки информации, за нарушения финансовой, налоговой, банковской и иных видов тайн. Имеет место дисциплинарная ответственность, но это уже внутренняя дело каждой организации. Законодательством предусмотрена гражданская ответственность, которая не так часто применяется в области информационной безопасности.

При этом надо понимать, что существует законодательство, а есть правоприменительная практика, которая имеет свою специфику. Поэтому необходимо учитывать все факторы для построения сбалансированной, как с точки зрения законодательства, так и с точки зрения фактической результативной действенности, системы информационной безопасности [81].

Специалисты в области ИБ для построения эффективной системы безопасности предлагают дорожные карты, включающие в свой состав следующие элементы:

- определение недопустимых событий;
- определение целевых и ключевых систем;
- усиление защищенности с целью снижения рисков от возможных угроз (харденинг) инфраструктуры;
- модернизация бизнес-процессов;
- выстраивание мониторинга и реагирования;
- обучение работников;

- проведение регулярных киберучений, которые проверяют насколько процесс обучения был эффективен и появились ли у сотрудников навыки безопасности;

- внедрение программы непрерывного измерения эффективности и оптимальности информационной безопасности;

- поддержание цифровой устойчивости;

- внешняя оценка системы (через Bug Bounty).

С одной стороны, такая дорожная карта позволит выполнить требования законодательства и защитить себя от таких недопустимых событий, как административное и уголовное наказание, а, с другой, создаст условия для развития собственного бизнеса и сегмента оказания электронных услуг государством юридическим и физическим лицам, то есть баланса между двумя сторонами.

Вопреки сложившемуся мнению в действующем законодательстве имеется немалое количество примеров, отражающих не «бумажную», а реальную информационную безопасность. В нем отражаются требования определить самое важное с точки зрения реализации системы ИБ, требования по построению центра противодействия киберугрозам. Не просто SOC[39], который в основном занимается мониторингом, а именно центр противодействия, который помимо мониторинга включает в себя и харденинг, и защиту, и реагирования.

В разных документах прописаны эти требования и, конечно же, требования по оценке результативности ИБ в виде киберучений, в виде планов реагирования, в виде пентестов, поисков уязвимости, непрерывного мониторинга и так далее. Необходимо обратить внимание, что рассмотренные нормы и документы, в том числе измененные в 2022 году и, которые будут еще изменяться в дальнейшем, уже содержат немалое количество пунктов и требований по результативной ИБ.

Знание нормативной базы, регламентирующей реализацию мероприятий по обеспечению информационной безопасности, позволит решить проблему кибербезопасности организации наиболее эффективно и с наименьшими затратами [43].

1.5. Анализ концепции угрозы информационной безопасности

Понятие угрозы ИБ в глобальном контексте определяется политэкономическими факторами. Для специалиста ИБ критично понимать эти различия при проектировании транснациональных систем защиты. Каждый подход учитывает специфические юридические, социальные и культурные аспекты, что влияет на реализацию IT-решений.

Глобальная цифровая трансформация сопровождается дивергенцией подходов к информационной безопасности в ключевых юрисдикциях. Это

[39] Центр мониторинга информационной безопасности (Security Operations Center, SOC).

означает, что специалисты по информационной безопасности должны адаптироваться к различным требованиям и стандартам, которые могут значительно варьироваться в зависимости от региона (табл. 1.1).

Таблица 1.1

Анализ концепции угрозы информационной безопасности в различных правовых и технологических экосистемах

Аспект анализа	Европейский союз (ЕС)	Китай	Россия
Ключевой концептуальный подход	Защита приватности и киберустойчивости	Киберсуверенитет и социальная стабильность	Цифровой суверенитет и технологическая независимость
Базовые нормативные акты	GDPR (General Data Protection Regulation) Директива NIS2 (по безопасности сетей и информационных систем)	Закон о кибербезопасности GB/T 22239-2019	Закон о «суверенном Рунете» Политика импортозамещения ПО
Приоритеты в защите	1. Права граждан на приватность. 2. Устойчивость критической инфраструктуры. 3. Сквозная безопасность цепочек поставок.	1. Государственная безопасность в киберпространстве. 2. Социальная стабильность. 3. Контроль над данными.	1. Технологический суверенитет. 2. Независимость от иностранных технологий. 3. Контроль интернет-инфраструктуры.
Основные субъекты защиты	Физические лица (персональные данные), бизнес, критическая инфраструктура	Государство, общественные интересы, социальная стабильность	Государство, национальная безопасность, отечественный ИТ-сектор
Подход к данным	Свободное перемещение с защитой приватности (GDPR)	Государственный контроль и локализация	Постепенный переход к суверенному управлению и локализации
Технологические приоритеты	Стандартизация и кросс-граничная безопасность	Развитие национальных технологий	Активное импортозамещение и развитие отечественных решений
Восприятие угроз	Угрозы приватности, нарушения работы критической инфраструктуры	Угрозы государственной безопасности и социальной стабильности	Угрозы цифровому суверенитету и технологической зависимости

Российский сегмент интернета (Рунет) демонстрирует уникальные черты, обусловленные геополитическими, регуляторными и технологическими факторами. Ключевыми особенностями являются:

- инфраструктурная трансформация – масштабные проекты (например, федеральный проект «Инфраструктура доступа к сети интернет» с бюджетом ₽287 млрд[40]);

- регуляторная специфика (законодательные инициативы, направленные на обеспечение цифрового суверенитета, например, закон о свободном доступе провайдеров в МКД).

Теперь выявим семантические, нормативные и операционные различия в трактовке базовых характеристик угроз ИБ и проведем сравнительный анализ понятия «угроза ИБ».

Европейская трактовка (ENISA, GDPR).

Определение: «Любое потенциальное событие, способное нанести ущерб конфиденциальности, целостности или доступности (CIA-триада) информационных активов» (ENISA Threat Landscape).

Ключевые акценты:

- неразрывная связь с *рисками персональных данных* (GDPR Art.4);
- классификация по таксономии *TTPs (Tactics, Techniques, Procedures)* на базе MITRE ATT&CK.

Китайская трактовка (Закон о кибербезопасности, GB/T 22239)[41].

Определение: «Деятельность, создающая опасность для работы сетей, утечки данных, распространения незаконной информации или нарушения национальной безопасности» (Статья 76 Закона КНР).

Ключевые акценты:

- привязка к национальной безопасности и общественным интересам;
- жесткая регламентация критических информационных инфраструктур (КИИ).

Российская модель (ФСТЭК, закон о КИИ).

Определение: «Воздействие на информацию или инфраструктуру, способное нанести ущерб CIA-триаде или национальной безопасности».

Ключевые аспекты:

- фокус на защите критической инфраструктуры (Приказ № 235 ФСТЭК от 21 декабря 2017 года);
- учет требований ФСТЭК и закона о «суверенном Рунете»[42].

---

[40] Проект по развитию быстрого домашнего интернета может обойтись в 287 млрд рублей https://tass.ru/ekonomika/21991957

[41] GB/T 22239-2019. Базовые требования безопасности информационных систем [信息安全技术 信息系统安全等级保护基本要求] / Китайская национальная стандартизация. – Пекин: Standards Press of China, 2019. – 68 p.

[42] Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».

Российская специфика источников угроз.

Внутренние угрозы: рост рисков, связанных с инсайдерами и непреднамеренными действиями персонала (например, ошибочные конфигурации облачных сервисов).

Внешние акторы (преобладают государственно-спонсируемые APT-группы и киберпреступные сообщества, использующие):

– техники атаки на цепочку поставок (вид кибератаки, при которой злоумышленники атакуют не саму компанию, а её поставщиков или партнёров);

– эксплойты уязвимостей в импортозамещенном программном обеспечении (ПО).

Отметим основные цели угроз для каждой из трех юрисдикций.

Цель угрозы.

ЕС:

– основной регламент, регулирующий защиту персональных данных (GDPR);

– сервисы цифровой экономики (стандарт eIDAS, обеспечивающий правовую основу для использования электронных идентификаторов и услуг).

Китай:

– КИИ (энергетика, транспорт);

– платформы с пользовательским контентом (закон «О управлении данными») регулирующий сбор и обработку пользовательских данных на онлайн-платформах).

Россия:

– КИИ и ИСПДн (энергетика, транспорт);

– цифровые платформы (видеосервисы, e-commerce; интернет-трафика);

– IoT/IIoT-системы (29.6 млн устройств в 2021 г., прогноз 62 млн к 2026 г.)[43].

Рассмотренные различия напрямую влияют на подходы к оценке угроз информационной безопасности. Для эффективной защиты информационных систем необходимо учитывать не только внутренние факторы, но и международные аспекты.

В таблице 1.2 приведен алгоритм оценки угроз информационной безопасности в РФ (с учетом ФСТЭК).

Таблица 1.2

Алгоритм оценки угроз информационной безопасности в РФ

№	Ключевой этап	Содержание этапа (действия и характеристики)
1	Выявление угроз	Цель: формирование перечня потенциальных угроз безопасности информации (ИБ).

[43] https://www.tadviser.ru/index.php/Статья:Интернет_вещей,_IoT_(рынок_России)

№	Ключевой этап	Содержание этапа (действия и характеристики)
		Источники данных: базы данных угроз ФСТЭК России, результаты моделирования нарушителя, данные о ранее произошедших инцидентах, анализ уязвимостей (слабых мест) в информационной системе (ИС). Результат: полный и актуальный список угроз ИБ, релевантных для защищаемой информационной системы.
2	Классификация	Цель: систематизация выявленных угроз по заданным критериям для упрощения дальнейшего анализа. Критерии классификации: - по типу нарушителя - по характеру воздействия; - по используемым уязвимостям. Результат: структурированный и категорированный перечень угроз.
3	Оценка рисков	Цель: определение уровня риска для каждой значимой угрозы. Процесс: анализ и оценка двух компонентов: - вероятность реализации угрозы (P); - степень негативных последствий (ущерб) для организации (C). Формула риска: $R = P \times C$ (качественно или количественно). Результат: ранжированный список угроз по уровню риска (высокий, средний, низкий).
4	Применение нормативных стандартов (включая ГОСТ Р 59533-2021)	Цель: сопоставление выявленных и оцененных угроз с требованиями регулирующих документов. Ключевые документы: Приказы ФСТЭК России (например, № 239 о требованиях к СЗИ в ГИС). Действия: проверка полноты перечня угроз, соответствия методов оценки установленным методикам, идентификация угроз, подлежащих обязательному учету. Результат: нормативно выверенный перечень угроз и рисков.
5	Принятие решений по мерам снижения угроз	Цель: выбор и планирование внедрения адекватных мер защиты. Процесс на основе уровня риска и нормативных требований: - для рисков «высокий» и «средний» (принятие решения о внедрении организационных и технических мер защиты, например, СЗИ, политики доступа, обучение сотрудников); - для рисков «низкий» (возможность принятия риска на себя или их мониторинг).

№	Ключевой этап	Содержание этапа (действия и характеристики)
		Результат: план мероприятий по снижению уровня рисков информационной безопасности до приемлемого уровня.

Данная схема является итерационной. После внедрения мер защиты (этап 5) процесс может быть повторен для оценки остаточного риска и эффективности принятых мер, что соответствует принципам непрерывного управления рисками ИБ.

Разберем общие тренды и специфику угроз информационной безопасности.

Общие тренды угроз:

- фишинг (метод обмана, когда злоумышленники пытаются выманить личные данные, такие как пароли и номер кредитной карты, под видом легитимнорго сообщения/ ссылки);

- zero-day атаки (используют уязвимости в программном обеспечении, о которых разработчики еще не знают);

- supply-chain компрометация (проникновение злоумышленника в цепочку поставок, чтобы получить доступ к конечной цели, например у поставщика программного обеспечения есть уязвимость, злоумышленник может использовать это для доступа к клиентам).

Специфика угроз по регионам.

В Европейском Союзе наблюдается рост угроз через API-интеграции в облачных средах. Это означает что системы, взаимодействующие друг с другом через API (интерфейсы программирования приложений), становятся мишенью для атаки. Если злоумышленник получит доступ к API, он может управлять данными и ресурсами приложений.

В Китае фокус на *атаках на IoT*-устройства (умные устройства), что связано со стандартом GB/T 37044. Этот стандарт определяет безопасность таких устройств. Поскольку они чаще используются в повседневной жизни, от уязвимости в их защите могут пострадать многие пользователи [58].

В России специфические угрозы заключаются в атаках на BGP-маршрутизацию, что может привести к сбоям в Интернет-сетях. Также уязвимости могут быть в импортозамещенном оборудовании, например в устройствах LoRa и NB-IoT. Ключевыми секторами остаются критическая инфраструктура: энергетика, транспорт, финансовый сектор.

Инструментарий анализа угроз.

Европейские подходы:

1. Модели:

- фреймворк ENISA Threat Taxonomy представляет собой систему классификации угроз, разработанный агенством по кибербезопасности;

- NIS2 Directive (директива касается безопасности сетей и информационных систем, особенно для инфраструктуры КИИ);

2. Технологии:

- системы AI-driven SIEM, которые используют искусственный интеллект для анализа данных и выявления аномалий в поведении пользователей (UEBA);

3. Соответствие (compliance):

Обязательная оценка воздействия на защиту данных - DPIA (Data Protection Impact Assessment). Эта операция позволяет выяснить, создает ли обработка риск для субъекта и насколько этот риск серьезен.

Китайские подходы:

1. Модели:

Методология оценки рисков GB/T 32919-2016 (методология оценки рисков, которая позволяет определить и управлять угрозами, связанными с информационной безопасностью на уровне организаций);

2. Технологии:

Национальная система мониторинга (проект «Великий киберщит»);

3. Соответствие (compliance):

Система многоуровневой защиты (Multi-Level Protection Scheme) MLPS 2.0 для классификации объектов, которая помогает определить степень защиты, необходимый для различных категорий информации и систем.

Российские подходы.

1.Модели:

- ГОСТ Р 59533-2021 для защиты КИИ (стандарт касается защиты инфраструктуры и определяет требования к обеспечению безопасности данных и систем);

- отраслевые онтологии на базе MITRE ATT&CK (представляет собой базу знаний и тактики злоумышленников, которые помогают организациям понять потенциальные угрозы и защитить свои системы).

2.Технологии:

- импортозамещенные SIEM-системы с ИИ (данные системы могут предсказывать 90% атак к 2030 г[44], что обеспечивает проактивнй подход к кибербезопасности);

- IoT-платформы (например, «Инфраструктурная IoT-платформа» Росатома[45] с сертификацией ФСТЭК, обеспечивает защиту умных устройств и их данных);

- сети LPWAN на базе отечественных стандартов (XNB, NB-Fi). Это технологии для создания сетей для устройств интернет-вещей, обеспечивающие низкое потребление энергии).

[44] Российский рынок SIEM-систем в 2025 году: тенденции, выбор и прогнозы развития https://www.anti-malware.ru/analytics/Technology_Analysis/Russian-SIEM-market-in-2025-AMLive

[45] Интеллектуальный контроль и управление инженерно-технической инфраструктурой зданий и территорий https://iot.rosatom.city

Выводы и тенденции:

- инфраструктурные и регуляторные особенности определяют уникальные требования и стандарты в каждом регионе;

- все три юрисдикции используют понятие длинных атак APT (Advanced Persistent Threat), которое описывает сложные и целенаправленные атаки, но источники этих угроз могут различаться.

В таблице 1.3 представлены технологические фокусы и соответствующие классы киберугроз по странам/регионам.

В приведенной таблице первый столбец «Страна/Регион» задаёт географический контекст, определяя в рамках какой национальной технологической стратегии или рыночной среды рассматриваются угрозы. Второй столбец «ключевая технология», указывает на конкретный технологический приоритет этого региона, который формирует его уникальный, специфический ландшафт киберугроз. Третий столбец «классы угроз», содержит конкретные типы кибератак, наиболее вероятные и критические для указанной технологии в данном контексте: API-атаки, Data Breach, сенсорный шпионаж, DDoS, уязвимости BGP и фишинг.

Таблица 1.3

Технологические фокусы и соответствующие классы киберугроз по странам/регионам

Страна/Регион	**Ключевая технология**	**Характерные классы угроз информационной безопасности**
ЕС	Облачные сервисы (Cloud Services)	- API-атаки. - Утечки данных (Data Breach). - Нарушения конфиденциальности данных в многопользовательских средах.
Китай	Интернет вещей (IoT/5G)	- Сенсорный шпионаж (сбор данных с устройств IoT). - DDoS-атаки через уязвимые устройства. - Компрометация сетей 5G.
Россия	Импортозамещение ПО	- Уязвимости маршрутизации (BGP). - Фишинг и целевые атаки на разработчиков и внедряемые решения. - Уязвимости в новом, недостаточно протестированном ПО.

Представленный перечень характерных классов угроз информационной безопасности является практическим инструментом для решения нескольких важных задач. Во-первых, она полезна для профилактики и анализа рисков. Когла понимая технологические приоритеты страны, организации могут заранее прогнозировать, с какими угрозами с наибольшей вероятностью столкнутся их компании и государственные органы. Во-вторых, она помогает в разработке мер защиты, позволяя сфокусировать ограниченные ресурсы и технические средства на нейтрализации наиболее релевантных и опасных

угроз для конкретной технологической сферы. Наконец, схема является основой для стратегического планирования, помогая при формировании обоснованных и целевых национальных или корпоративных стратегий кибербезопасности [59].

Однако методологические основы классификации угроз ИБ не являются универсальными - они коррелируют с цифровым суверенитетом, технологической специализацией и кризисным опытом каждого сегмента интернета. Таким образом, понятие угрозы ИБ в глобальном контексте остается полисемичным. Полисемия в данном случае означает наличие у термина «информационная безопасность» нескольких взаимосвязанных значений, которые могут различаться в зависимости от контекста или точки зрения исследователя (в разных странах и организациях могут использоваться разные термины и определения). Несмотря на то, что все юрисдикции используют концепции APT и CIA-триады, но применяются они с разными акцентами. Европейская модель фокусируется на защите цифровых прав граждан и бизнеса; китайская – на обеспечении киберсуверенитета, абсолютном приоритете национальной безопасности; российская - технологический суверенитет и адаптация к санкциям. Понимание этих различий критично для проектирования межнациональных систем защиты информации [22].

Угрозы ИБ в российском сегменте интернета характеризуются двойственной природой: с одной стороны – глобальные тренды (APT, ransomware), с другой – уникальные инфраструктурные и регуляторные риски. Ключевой задачей специалистов ИБ является адаптация международных практик (NIST CSF, MITRE ATT&CK) к требованиям ФСТЭК и специфике отечественной телекоммуникационной экосистемы.

Текущая ситуация и тенденции на 2026 год.

Агентство Европейского союза по кибербезопасности (ENISA) обновило методологию «Отчета о ландшафте угроз» (2022-2025гг.), уточнив этапы, инструменты и содержание оценки киберугроз. Нормативно-правовая база отдает предпочтение подходам, основанным на оценке рисков с точки зрения детерминистского подхода «угроза есть/ угрозы нет». Новые законы и директивы направлены на улучшение информирования об инцидентах, координацию между государствами-членами и повышение способности при необходимости переходить от управления на уровне инцидента к управлению на уровне кризиса. Например, система TIBER EU[46] представляет модель «красной команды» на основе анализа угроз и является примером того, как ЕС классифицирует и оценивает угрозы с помощью структурированной методологии, основанной на анализе данных. В настоящее время в ЕС используется стандартизированная методология (ENISA/CTL), регулирование

[46] TIBER-EU framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming
https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

на основе оценки рисков, обязательную отчетность и периодическую переоценку угроз [68].

В Китае намечена тенденция изменения классификации в направлении ее расширения, включая КИИ и узлы цепочек поставок. Это может привести к многоуровневой системе классификации: 1 уровень – критически важная инфраструктура, 2 уровень – системы данных и 3 уровень – общая инфраструктура (подлежащая мониторингу). Классификация будет сосредоточена не только на отраслях, но и на функциях, конфиденциальности данных, трансграничных потоках, точках удаленного доступа. Все это направлено на то, чтобы лучше справляться с угрозами с использованием искусственного интеллекта. В перспективе внедрение мониторинга в режиме, близком к реальному времени, автоматическое обнаружение и классификация угроз.

В России намечено движение от традиционной классификация КИИ к более широкой классификации в сторону суверенитета данных, включив в нее не только физическую инфраструктуру, но и программные платформы, ИТ системы корпоративного уровня, облачные сервисы и системы обработки данных. Все организации, работающие в секторах энергетики, транспорта, здравоохранения, финансов, производства будут регистрироваться, проводить самооценку [80].

Ключевые тренды и прогноз развития методологий классификации угроз ИБ в ЕС, Китае и России (2026-2030 гг.) представлен в табл. 1.4.

Таблица 1.4

Прогноз развития методологий классификации угроз ИБ в ЕС, Китае и России (2026-2030 гг.)

Регион	**Технологический вектор**	**Регуляторные изменения**	**Риски**
ЕС[47]	Конвергенция AI/ML в классификации ATT&CK Стандартизация TTPs для квантовых угроз	Введение «ИИ-акта» Ужесточение NIS3 для cloud/SaaS	Фрагментация моделей из-за GDPR vs. eIDAS
Китай	Национальные классификации для 6G/IoT Интеграция квантовых IDS в GB/T	Закон о суверенном ИИ Обязательное ГОСТ шифрование для КИИ	Технологическая изоляция от global frameworks
Россия[48]	Гибридные модели: MITRE ATT&CK + ГОСТ	ФСТЭК-стандарты для post-quantum crypto	Дефицит электронной

[47] Прогнозируемые угрозы кибербезопасности ENISA до 2030 года https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

[48] «Альфа-Банк» спрогнозировал развитие рынка ИБ до 2030 года https://rspectr.com/novosti/alfa-bank-predstavil-prognoz-razvitiya-rynka-ib-do-2030-goda

Регион	Технологический вектор	Регуляторные изменения	Риски
	Автономные Threat Intelligence платформы	«Закон о киберрезерве» для КИИ	компонентной базы (ЭКБ) для импортозамещенных решений

К 2030 году различия в классификациях угроз достигнут критического уровня. Балансировка между глобальной интероперабельностью (MITRE ATT&CK) и национальным регулированием (GDPR/GB/T/ФСТЭК) станет ключевым вызовом для нового поколения специалистов ИБ.

1.6. Практические примеры анализа угроз информационной безопасности в ЕС, Китае и России

Рассмотрим практические примеры реализации анализа угроз информационной безопасности на примере трех юрисдикций ЕС, Китай и РФ.

Немецкая FinTech-компания, выступающая в качестве обработчика персональных данных в соответствии с Общим регламентом ЕС по защите данных (GDPR) использует Amazon Web Services (AWS) для обработки персональных данных клиентов. В рамках модели общей ответственности облачных сервисов финтех-компания отвечает за внедрение организационных и технических мер безопасности, а AWS обеспечивает безопасную инфраструктуру и базовую защиту.

Ситуация. Компания столкнулась с серьезным инцидентом в сфере безопасности, вызванным целенаправленной атакой на API. Злоумышленник воспользовался уязвимостью в одном из микросервисов, которая не отслеживалась должным образом из-за недостаточного анализа сетевого трафика и слабой оценки безопасности. В результате чего произошла утечка более 500 000 личных записей, что поставило под угрозу конфиденциальность и целостность данных. Согласно GDPR это является серьезным нарушением, поскольку персональные данные были раскрыты без надлежащих мер предосторожности. В результате соответствующий надзорный орган наложил штраф в размере 4% оборота (€8.2 млн по времени фиксации инцидента).

Анализ угроз. Проведенная атака использовала уязвимости на прикладном уровне компании FinTech, в частности через API и микросервисы.

Последствия. Масштабное раскрытие персональных данных с прямыми финансовыми последствиями (штраф со стороны регулятора) и потенциальный ущерб для репутации.

Основные причины:

1. Недостаточная оценка безопасности микросервисов.
2. Слабый мониторинг сетевой активности.
3. Отсутствие проактивных мер по обеспечению конфиденциальности и управлению рисками.

Все это показывает, что технические уязвимости в облачных инфраструктурах, если их не устранять, могут перерасти в серьезные угрозы для бизнеса, если не будут соблюдаться нормативные требования.

Принятые меры (фреймворк ENISA). Для укрепления своей системы управления информационной безопасностью и соблюдения требований GDPR компания внедрила следующие меры:

- усовершенствованное обнаружение угроз и реагирование на них. За счет развертывания системы управления информацией о безопасности и событиями (SIEM), которая была дополнена модулями анализа поведения пользователей и организацией поведенческой аналитики (UEBA), управляемых искусственным интеллектом, для упреждающего выявления необычных действий системы и пользователей.

- обязательная оценка воздействия на защиту данных DPIA (Data Protection Impact Assessment) для всех новых операций по обработке данных. Это обеспечивает проактивное управление рисками в корпоративные процессы.

- реализация сквозного шифрования данных при передаче с использованием CRYSTALS-Kyber[49] (стандартизирован NIST).

Ключевой урок: несоблюдение GDPR ставит под угрозу бизнес-модель, облачная безопасность требует усиленного контроля и важным становится проактивное управление рисками.

Данный случай иллюстрирует как технические уязвимости в сочетании с несоблюдением нормативных требований могут перерасти в серьезные системные риски для современных цифровых организаций. Интеграция юридических, технических и операционных мер (особенно в облачных средах) имеет решающее значение для защиты как персональных данных, так и корпоративной деятельности.

В Шанхае была совершена целенаправленная атака на платформу системы социального кредита (SCS) - критически важного компонента государственной информационной инфраструктуры Китая. SCS функционирует как система обработки персональных данных особой категории, масштаб, конфиденциальность и роль которой в управлении позволяют отнести ее к критически важной информационной инфраструктуре (CII) в соответствии с Законом о кибербезопасности Китайской Народной Республики (CSL) и стандартом многоуровневой схемы защиты (MLPS 2.0 / GB/T 22239).

Ситуация. Атака была совершена группой Advanced Persistent Threat (APT). В отличие от обычных утечек данных, целью этой атаки была подмена данных социального рейтинга, чтобы подорвать доверие к системе и дестабилизировать общественное мнение. Злоумышленники использовали уязвимости в устройствах Интернета вещей, интегрированных в городскую

[49] CRYSTALS-Kyber и другие: постквантовая криптография простым языком https://www.securitylab.ru/blog/personal/Technolady/354956.php

инфраструктуру. Это демонстрирует использование сложной цепочки кибератак, когда злоумышленники используют смежные, менее защищённые системы для достижения важных целей.

Анализ угрозы. Группа APT использовала уязвимости Интернета вещей в городской инфраструктуре для манипулирования рейтинговыми данными системы [61].

Последствия. Нарушение целостности системы, потенциальная социальная дестабилизация и подрыв доверия к механизмам государственного управления.

Основные причины:

1. Сложность взаимосвязанных городских систем Интернета вещей [60].

2. Централизованный характер критически важной информационной инфраструктуры, что усиливает системное воздействие в случае целенаправленной атаки.

3. Зависимость от целостности стратегических данных для управления и социального контроля.

Данный случай демонстрирует системный характер киберугроз в критически важной для государства инфраструктуре, где потенциальный ущерб выходит за рамки технического или экономического и затрагивает социальную и политическую стабильность.

Принятые меры соответствуют стандарту GB/T 22239 и национальным стандартам страны (обусловлены иерархической логикой национальных нормативных и операционных требований:

- активация системы «Великий брандмауэр», функционирующей как национальная система обнаружения вторжений (IDS) с возможностью глубокой проверки пакетов;

- криптографические меры (квантовое распределение ключей между центрами обработки данных для защиты магистральных каналов связи, что обеспечивает долгосрочную криптографическую стабильность и устойчивость к будущим угрозам, связанным с квантовыми вычислениями);

- классификация инцидента Национальным центром реагирования на компьютерные инциденты (CNCERT) как «угрозу социальной стабильности».

Это определение повлекло за собой приоритетное реагирование на государственном уровне, привлечение органов национальной безопасности и полномасштабное расследование с использованием цифровых криминалистических методов [69].

Ключевые уроки: информационная безопасность подчинена государственным целям, операционные системы (IDS) внедряются не только для защиты от технических угроз, но и для обеспечения функционирования критически важных государственных служб.

Этот инцидент показывает, что в Китае информационная безопасность - это инструмент управления, подчинённый национальному контролю, социальной стабильности и киберсуверенитету. Технические стандарты и оперативные меры применяются не только для предотвращения взломов, но и

для обеспечения целостности и доступности критически важных государственных систем, что отражает стратегический подход к киберзащите, основанный на принципе «сверху вниз». Меры по обеспечению кибербезопасности в критически важных для государства системах тесно связаны с политическими и нормативными приоритетами, что подчеркивает более широкий охват информационной безопасности в Китае, выходящий за рамки традиционного управления рисками.

Киберфизическая атака на российский энергетический объект в Арктике. Целенаправленная киберфизическая атака была осуществлена на систему SCADA (система диспетчерского контроля) нефтепровода[50], важнейшего объекта топливно-энергетического комплекса России. Этот объект относится к категории объектов критической информационной инфраструктуры (КИИ) в соответствии с Федеральным законом №187-ФЗ, который определяет правовую базу, оценку серьезности и обязательные меры противодействия в случае подобных инцидентов.

Ситуация. Атака носила гибридный характер и сочетала в себе элементы распределённых атак типа «отказ в обслуживании» (DDoS), направленных на нарушение доступности каналов управления и тактики продвинутых постоянных угроз (APT), предположительно применяемых иностранными субъектами, для проникновения в сеть SCADA. Злоумышленники воспользовались уязвимостью в протоколе пограничного шлюза (BGP) на границе телекоммуникационной сети «Ростелекома». Это позволило перехватить BGP, перенаправить трафик и провести последующий анализ, что дало возможность проникнуть в изолированные сегменты системы управления технологическими процессами. Атака представляет собой классический пример нацеливания на смежную инфраструктуру, когда слабые места в телекоммуникационной инфраструктуре используются для доступа к важным промышленным системам [79].

Анализ угрозы. Гибридная атака, сочетающая методы киберпреступности и возможности иностранных APT-группировок с использованием протокола BGP для нарушения работы сетей SCADA и проникновения в них.

Последствия: потенциальное нарушение работы трубопровода, риск для физической безопасности и компрометация критически важных промышленных систем управления.

Основные причины:

1. взаимосвязанная промышленная и телекоммуникационная инфраструктура создавала возможности для горизонтальных атак;

2. использование отечественных аппаратных и программных компонентов (импортозамещение) создавало физические и технологические уязвимости, особенно в арктических условиях;

[50] Хакеры усилили натиск на нефтегазовую отрасль // https://xakep.ru/2022/09/20/industrial-automation-threats/

3. сложная киберфизическая среда, в которой недостаточная отказоустойчивость может привести к возникновению единой точки отказа.

Этот инцидент показывает, что критически важная инфраструктура в России подвержена рискам, возникающим из-за сочетания уязвимостей в киберпространстве, ограничений физической среды и стратегической операционной политики.

Меры, принятые после инцидента, осуществлены в соответствии с требованиями к обеспечению защиты информации в автоматизированных системах управления производством и технологическими процессами» (Приказ ФСТЭК России от 14.03.2014 № 31):

1. внедрение гибридной VPN для защиты каналов управления, что обеспечивает устойчивость к классическим и будущим вычислительным угрозам при соблюдении политики импортозамещения;

2. усиленная физическая защита и защита периметра (установка термостойких датчиков, оснащенных постквантовым шифрованием для обеспечения целостности аппаратного шифрования в суровых арктических условиях, что позволяет устранить как климатические, так и кибернетические уязвимости);

3. расследование инцидента и криминалистический анализ (Федеральная служба по техническому и экспортному контролю провела полное расследование. Для определения этапов атаки, выявления слабых мест и классификации инцидента как попытки дестабилизации критически важного энергетического объекта была применена адаптированная матрица MITRE ATT&CK).

Ключевые уроки: кибербезопасность тесно связана с физической безопасностью и импортозамещение программных и аппаратных компонентов может привести к появлению технологических и физических уязвимостей, особенно в экстремальных условиях, таких как Арктика, не подходящие для климата компоненты могут создавать единые точки отказа, ставя под угрозу как кибербезопасность, так и операционную устойчивость. Современные гибридные угрозы требуют многоуровневой защиты, а использование постквантовой криптографии (алгоритмы NTRU) обеспечивает долгосрочную криптографическую стабильность [26].

Приведенный случай показывает, что в России киберзащита объектов критической информационной инфраструктуры неразрывно связана со стратегиями импортозамещения (киберсуверенитет), физической безопасностью и управлением системными рисками в киберфизических средах. Для обеспечения устойчивости критически важных промышленных систем к гибридным атакам требуется комплексная интеграция кибер-, аппаратных средств защиты. При этом безопасность не может быть чисто цифровой, она должна охватывать всю технологическую и операционную экосистему [29].

1.7. Объектно-ориентированные угрозы информационной безопасности

Современная ИТ-инфраструктура, построенная на принципах облачной и микросервисной архитектуры, подвергается комплексным объектно-ориентированным угрозам. Эти угрозы нацелены на ключевые абстракции и сервисы (объекты) облака, такие как виртуальные машины, контейнеры, распределённые системы данных и объектные хранилища, требуя в управлении рисками, не изолированных средств защиты, а эшелонированной (многоуровневой) обороны. Критические риски сконцентрированы в точках агрегации данных и управления, где компрометация одного компонента может привести к латеральному перемещению злоумышленника по всей инфраструктуре [30].

Безопасность информационных систем становится одним из приоритетных направлений развития ИТ инфраструктуры организаций. С ростом сложности и масштабов вычислительных систем появляются новые векторы атак и угрозы, требующие комплексного подхода к защите. Современная информационная инфраструктура включает множество компонентов, каждый из которых может стать потенциальной целью для злоумышленников. Рассмотрим основные области риска: виртуализированные среды и облачные инфраструктуры.

Виртуальные машины (VM) остаются первостепенным вектором атак. Наиболее опасным сценарием является внедрение вредоносных или недоверенных образов (image poisoning) на этапе их развертывания, что приводит к созданию изначально скомпрометированных экземпляров. Данная угроза прямо регламентируется в требованиях по обеспечению безопасности значимых объектов критической информационной инфраструктуры (КИИ), где установлены строгие стандарты контроля цепочек поставок и верификации образов для виртуализированных и облачных сред.

Распределённые системы запросов, такие как Cloud Trino, формируют отдельный класс угроз, связанный с безопасностью данных в процессе обработки. Они подвержены рискам инъекций в распределённые SQL-запросы, которые могут привести не к разрушению данных, а к их масштабной несанкционированной выборке (data exfiltration). Для организаций, особенно в финансовом секторе, защита таких систем требует соблюдения профильных стандартов, устанавливающих требования к аудиту транзакций, контролю целостности запросов и защите структурированных информационных массивов на всех этапах жизненного цикла.

Программы, управляющие работой контейнеров (оркестраторы контейнеров), в частности Kubernetes (K8s), сталкиваются с угрозами, связанными с компрометацией среды выполнения. Эксплуатация уязвимостей нулевого дня (zero-day) в контейнерных средах исполнения или компонентах оркестратора (например, CVE-2024-XXXX) позволяет злоумышленникам осуществлять несанкционированный доступ (privilege escalation) к уровню

узла (node) или всего кластера. Противодействие данным угрозам выходит за рамки базовых стандартов и требует реализации специализированных наборов мер, разработанных именно для облачных сред и управления жизненным циклом контейнеризированных приложений.

Объектные хранилища (например, S3-совместимые) регулярно становятся целью для шифровальщиков (ransomware), атак, направленных на блокирование доступности (Availability) данных через их криптографическое преобразование с последующим требованием выкупа. В контексте законодательства о защите персональных данных (ПДн), организация обязана обеспечивать не только их конфиденциальность, но и доступность. Это предписывает внедрение политик неизменяемости, регулярного верифицированного резервного копирования и управления доступом на основе принципа минимальных привилегий (Principle of Least Privilege) [32].

Таким образом, эскалация объектно-ориентированных угроз требует интегрального подхода к безопасности. Он должен комбинировать технические меры защиты (сканирование образов, контроль целостности запросов, сегментация кластеров, WORM-хранилища) со строгим соблюдением отраслевых регуляторных требований и международных стандартов, формируя тем самым комплексную систему управления информационными рисками в распределённой среде (табл. 1.6).

Таблица 1.6

Объектно-ориентированные угрозы информационной безопасности

Компонент	**Критические угрозы**	**Регуляторные требования**
Виртуальные машины	Внедрение вредоносных образов ВМ	ФСТЭК Приказ №17 (контроль ЦОД)
Cloud Trino	Инъекции в SQL-запросы, утечка данных	ГОСТ Р 57580.1-2017 (финансы)
Kubernetes (K8s)	Компрометация контейнеров (CVE-2024-XXXX)	ISO 27017 (облачная безопасность)
S3-хранилища	Ransomware-шифрование объектов	152-ФЗ ст. 19 (защита ПДн)

Эффективная защита современных информационных систем требует комплексного подхода к безопасности, постоянного обновления защитных мер, регулярного анализа новых угроз. Только системный подход может гарантировать защиту от современных киберугроз и минимизировать риски для критически важных объектов инфраструктуры.

1.8. Источники угроз по классификации MITRE ATT&CK

Без систематического подхода к выявлению и классификации угроз невозможно разработать адекватные меры защиты для современных информационных систем. В современной кибербезопасности существует структурированный подход к анализу угроз, основанный на методологии

MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge – дословно с английского – «тактики, приемы и общие знания»). Эта система (среди существующих, является одной из самых авторитетных и широко используется на международном уровне) позволяет упорядочить и систематизировать информацию о потенциальных злоумышленниках и их методах атаки.

MITRE ATT&CK® - это общедоступная база знаний о тактике и методах злоумышленников, основанная на реальных наблюдениях. База знаний ATT&CK используется в качестве основы для разработки конкретных моделей угроз и методологий в частном секторе, государственном управлении, а также в сфере продуктов и услуг в области кибербезопасности (рис.1).

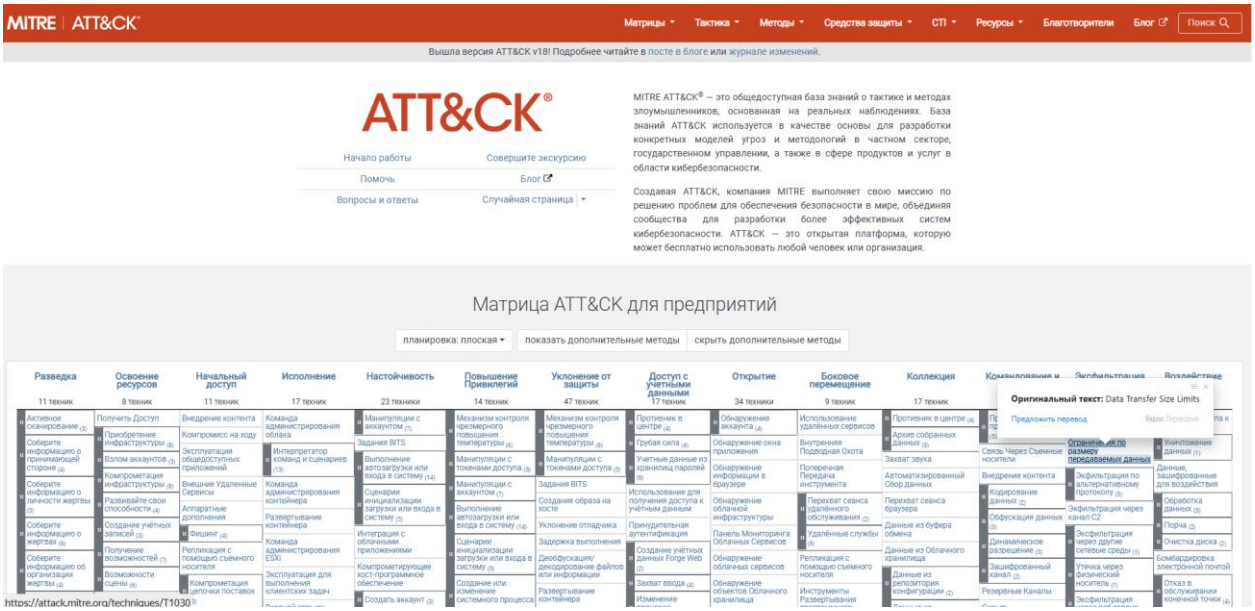


Рис.1 Главная страница MITRE ATT&CK https://attack.mitre.org/

Впервые MITRE презентовала матрицу угроз в 2013 году как способ описания и составления паттернов поведения злоумышленников на основе реальных наблюдений. С тех пор ATT&CK значительно эволюционировала благодаря вкладу сообщества по кибербезопасности: эксперты со всего мира регулярно отправляют в MITRE данные о новых, ранее неизвестных приемах.

В отличии от традиционных классификаций, которые довольно часто описывали угрозы абстрактными терминами (например, «вредоносные программы, «несанкционированный доступ») MITRE ATT&CK систематизирует действия злоумышленников виде структурированной матрицы тактик (целей высокого уровня), техник и подтехник (конкретных методов достижения целей). Эта структура позволяет аналитикам в сфере безопасности, правительствам и организациям понять не только то, что пытается сделать злоумышленник, но и то, как он обычно это делает, используя конкретные наблюдаемые действия.

Одним из важных сегментов экосистемы классификации угроз является классификация групп угроз – APT (Advanced Persistent Threat), которые

осуществляют целенаправленные и продолжительные атаки. APT группы – реальные враждебные объединения, как правило представлены продвинутыми постоянными угрозами на государственном уровне (киберпреступные группировки). Характерным вектором атак для данного источника является компрометация цепочек поставок (supply chain attacks). Примером такой тактики служит внедрение в процесс разработки и распространения программного обеспечения с целью компрометации эталонных образов операционных систем, что позволяет осуществлять скрытное проникновение в инфраструктуру центров обработки данных (ЦОД) [70].

В рамках главы рассмотрим, как MITRE ATT&CK классифицирует источники угроз и как эти классификации можно интерпретировать на примере Европейского Союза, Китае и России.

MITRE ATT&CK и концепция источников угроз.

В сфере информационной безопасности источники угрозы (или субъект угрозы) – это физическое лицо, группа или организация, у которых есть намерение, возможность и шанс нанести ущерб информационным активам.

Распознание источника угрозы важно, потому что разные субъекты используют разные тактики и методы и у субъектов различные мотивы (финансовая выгода, шпионаж, дестабилизация и проч.).

В классическом литературе по информационной безопасности источники угроз часто классифицируют следующим образом:

- случайные (например, ошибки сотрудника);
- естественные (например, пожар);
- злонамеренные (хакеры, инсайдеры, организованная преступность).

В MITRE ATT&CK основное внимание уделяется злонамеренным злоумышленникам. В рамках этой системы интерес представляют источники угроз – группы, выявленные в ходе исследований в области кибербезопасности и анализе инцидентов. Важным является и то, что MITRE ATT&CK не классифицирует группы угроз по географическому положению, вместо этого она каталогизирует их в соответствии с наблюдаемым поведением:

- методы, используемые для первоначального доступа (например, целевой фишинг, компрометация цепочки поставок);
- используемые инструменты и семейства вредоносных программ, операционные схемы, инфраструктура (серверы, загрузчики вредоносных программ);
- документированные кампании.

Группы угроз в ATT&CK обычно делятся на следующие типы:

1. Группы, созданные на уровне государств (спонсируемые государством). Часто называются продвинутыми стойкими угрозами (APT), которые обладают большими ресурсами и способными к долгосрочным целенаправленным операциям.
2. Группы киберпреступников, мотивированные в первую очередь финансовой выгодой, например, группы использующие программы вымогатели. Часто деятельность этого источника часто сводится к

автоматизированной эксплуатации публично известных уязвимостей в компонентах веб-инфраструктуры. Яркой иллюстрацией служат атаки на системы управления базами данных и поисковые движки, где уязвимости в программных интерфейсах (API) позволяют злоумышленникам осуществлять несанкционированный доступ к конфиденциальной информации или получать контроль над системой.

3. Группы мотивированные политическими или идеологическими целями (обозначаемые как «хактивисты»).

4. Группы/лица из числа инсайдеров. Инсайдеры - сотрудники организации, обладающие легитимным доступом к ключевым системам. В контексте систем мониторинга и реагирования, инсайдер, действуя злонамеренно или по неосторожности, может использовать свои привилегии для манипуляции оповещениями и журналами событий, что приводит к сокрытию инцидентов безопасности и блокированию механизмов.

Общие характеристики угроз на примере Европейского Союза (ЕС). Европейский Союз представляет собой уникальную систему информационной безопасности, которая характеризуется высоким уровнем цифровизации финансового и государственного секторов, действием строгим правилам защиты данных (GDPR).

Источники угроз, нацеленные на организации ЕС, включают как внешних, так и внутренних субъектов: государственные APT-группы; устойчивые группы киберпреступников; инсайдерские угрозы в государственном и частном секторах.

Сам ЕС не является единым субъектом угроз, но несколько европейских стран обладают передовыми кибервозможностями, которые часто используются для оборонительных операций и сбора разведданных, а не для крупномасштабных наступательных действий, направленных против иностранной инфраструктуры.

Группы угроз, связанные с ЕС, в MITRE ATT&CK. Хотя в MITRE ATT&CK группы перечислены по отдельности, а не по регионам, несколько хорошо задокументированных APT-групп часто атакуют европейские учреждения: TA505[51] (финансово мотивированная группа, действующая по всему миру и часто наносящая удары по финансовым учреждениям); Evil Corp[52] (группа киберпреступников, проводящая операции с использованием программ-вымогателей и наносящая ущерб предприятиям) и проч.

ЕС как целевой регион сталкивается с разнообразными источниками угроз, описанными в ATT&CK. ЕС как источник угроз (согласно ATT&CK)

В состав MITRE ATT&CK входят группы по борьбе с угрозами, связанные с некоторыми европейскими государствами. Эти группы обычно занимаются: сбором разведывательной информации о борьбе с терроризмом;

[51] https://ptsecurity.com/research/hacker-groups/TA505/
[52] https://www.techtarget.com/searchsecurity/definition/Evil-Corp

киберзащитой и стратегическим шпионажем; промышленным мониторингом; операциями дипломатической разведки.

Исследователи (за пределами самой MITRE) иногда приводят примеры связанных с западными разведками групп, занимающихся кибершпионажем против стратегических иностранных объектов. MITRE ATT&CK фокусируется на поведенческих методах, поэтому такие группы могут быть отнесены к конкретным наборам инструментов или кампаниям, а не к конкретным государствам [78].

Тактики MITRE, часто встречающиеся в контексте ЕС. Угрожающие группы, действующие в ЕС или против него, обычно используют такие методы, как:

- T1566[53] «Целевой фишинг» (нацелен на государственных служащих и дипломатов);
- T1190 «Эксплуатация общедоступных приложений» (часто используется при атаках на критически важную инфраструктуру);
- T1554 «Компрометация инфраструктуры» (используется преступными группировками для распространения программ-вымогателей);
- T1027 «Обфусцированные/зашифрованные файлы (используется в кампаниях по шпионажу и распространению вредоносного ПО).

Таким образом, в контексте ЕС MITRE ATT&CK помогает определить как внутренние возможности европейских государств, так и внешнее давление со стороны иностранных противников.

Источники угроз, связанные с Китаем. Китай выступает одной из самых активных и технически продвинутых стран в глобальном киберпространстве. По многочисленным данным, приоритетными направлениями китайских кибероперациий являются: промышленный и технологический шпионаж, политическая разведка, наблюдение за диаспорами, стратегические военные цели.

Связанные с китайским государством группы (APT) являются одними из наиболее подробно описанных в MITRE ATT&CK[54]. Среди известных примеров можно назвать:

- APT1 (Comment Crew) - одна из первых китайских APT-групп, о которой стало известно общественности; специализируется на промышленном шпионаже;
- APT10 (Stone Panda) - известна компрометацией цепочек поставок глобальных поставщиков управляемых услуг (Managed Service Providers, MSP);
- APT41 (Double Dragon) - примечательна сочетанием спонсируемого государством шпионажа с финансово мотивированными операциями;
- GALLIUM (шпионаж в телекоммуникационном секторе).

[53] Тут и далее классификация MITRE ATT&CK для описания тактик и техник, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру
[54] https://attack.mitre.org/groups/

Эти группы различаются по специализации, инструментам и организационной структуре, но все они имеют общие черты: долгосрочная деятельность, широкий охват целей и глубокая интеграция со стратегическими интересами Китая.

Методы по классификации MITRE, связанные с китайскими APT-операциями. Поведенческие особенности, характерные для субъектов, связанных с Китаем, включают:

- T1078 - действительные учётные записи (использование украденных учётных данных для скрытого долгосрочного доступа);
- T1204 - выполнение команд пользователем (доставка вредоносных вложений, замаскированных под официальные документы);
- T1105 - передача инструментов для входа (развертывание проприетарных и пользовательских вредоносных программ);
- T1482 - обнаружение доверия к домену (исследование корпоративных структур Active Directory для горизонтального перемещения);
- T1041 - кража данных через канал (скрытое извлечение больших массивов данных, включая интеллектуальную собственность, результаты научных исследований и персональные данные).

Эти методы показывают, что китайские кибероперации обычно носят шпионский характер с упором на скрытность, продолжительность и техническую сложность.

Китай является не только субъектом угроз, но и их объектом. Группы, описанные в документе ATT&CK, такие как преступные организации, занимающиеся вымогательством (например, LockBit, ALPHV/BlackCat), атаковали китайские компании, а региональные конфликты привели к шпионским операциям против государственных учреждений Китая.

Источники угроз, связанные с Россией.

Россия широко известна как ведущая кибердержава, и международное сообщество специалистов по кибербезопасности приписывает значительное число APT-атак российским государственным или аффилированным учреждениям. Российские кибероперации обычно направлены на[55]: политический и дипломатический шпионаж; операции по оказанию влияния и информационную войну; нарушение работы критически важной инфраструктуры; нацеливание на военные и правительственные органы НАТО и ЕС.

Киберпространство России включает в себя как спонсируемые государством APT-группы, так и высококвалифицированные киберпреступные сообщества, которые часто действуют в пределах российской юрисдикции. Некоторые связанные с Россией группы в MITRE ATT&CK:

- Sandworm Team (известна разрушительными атаками, в том числе на критически важную инфраструктуру);

[55] Рязанов А.А. Кибероперации как инструмент межгосударственной военно-экономической конкуренции // Вестник Московского университета имени С. Ю. Витте. Серия 1: Экономика и управление. 2021. № 2 (37).

- Gamaredon (группировка, нацеленная на региональные политические объекты).

Методы MITRE, используемые связанными с Россией группами злоумышленников. К наиболее распространенным методам относятся:

- T1059 - Интерпретатор команд и сценариев (использование PowerShell, Python и пользовательских скриптов);

- T1036 - Маскировка (использование законных системных процессов для сокрытия вредоносной активности);

- T1568 - Динамическое разрешение (сложные механизмы управления, позволяющие избежать блокировки);

- T1499 - Отказ в обслуживании конечных точек;

- T1210 - Использование удаленных сервисов (возможности высококлассного шпионажа).

Россия сама подвергается атакам со стороны различных спецслужб и глобальных преступных группировок. Нейтральная классификация ATT&CK позволяет анализировать кампании против России без политической подоплеки:

- использование целевого фишинга (T1566) в качестве начального вектора атаки;

- использование легитимных учётных данных (T1078) для постоянного доступа;

- кража данных по зашифрованным каналам (T1041) и проч.

Ключевые различия между регионами угроз. MITRE ATT&CK предлагает несколько преимуществ для анализа действий злоумышленников:

1. Стандартизированный язык. Команды по обеспечению безопасности во всем мире могут описывать угрозы, используя единую терминологию.

2. Атрибуция на основе поведения. Акцент делается на том, что делают злоумышленники, а не на том, кто они.

3. Всестороннее описание методов. Помогает выявлять закономерности в кампаниях.

4. Поддержка оборонительного планирования. Команды по защите могут создавать сценарии имитации действий противника, проводить учения «красной команды» и разрабатывать правила обнаружения.

5. Нейтралитет. MITRE не делает политических заявлений, она документирует поведение, наблюдаемое несколькими исследователями в области кибербезопасности. Такой нейтралитет крайне важен при изучении источников угроз в политически чувствительных регионах, таких как ЕС, Китай и Россия.

Таким образом, понимание источников угроз с помощью системы MITRE ATT&CK позволяет проводить более глубокий и структурированный анализ глобальных киберугроз. На примерах ЕС, Китая и России мы показали, как различные геополитические субъекты используют разные операционные модели, мотивы и технические методы, которые можно выявить и изучить с помощью ATT&CK. В конечном счете, ATT&CK от MITRE служит

незаменимым инструментом для понимания современного ландшафта киберугроз. Изучая источники угроз с помощью структурированной системы ATT&CK, специалисты по кибербезопасности и лица, принимающие решения, получают более четкое представление о действиях злоумышленников, что позволяет разрабатывать более надежные стратегии защиты [76].

Методика определения угроз информационной безопасности, адаптированная по ФСТЭК для информационной системы персональных данных в среде VK Cloud (модель угроз фокусируется на рисках, связанных с нарушением конфиденциальности и целостности персональных данных).

VK Cloud - платформа с широким набором облачных сервисов для эффективной разработки и работы с данными для компаний любого масштаба.

Ключевые угрозы.

Несанкционированный доступ к данным, который реализуется через уязвимости в компонентах веб-интерфейса или API, компрометацию учетных записей сотрудников с привилегированным доступом к СУБД, либо ошибки конфигурации политик доступа к сетевым ресурсам и блочным хранилищам.

Утечка данных: возможна вследствие инъекций в прикладном слое (например, SQL-инъекции в отчетные формы), некорректной обработки ошибок, приводящей к раскрытию чувствительной информации в логах, или действий инсайдера, осуществляющего несанкционированное копирование данных на внешние носители.

Отказ в обслуживании: целевые DDoS-атаки на внешние интерфейсы системы, приводящие к нарушению доступности сервиса для пользователей и подпадающие под нарушение требований регламентов по обработке ПДн.

Верификация эффективности по методике ENISA Threat-Led Penetration Testing (TLPT): для валидации предложенных контрмер рекомендуется проведение сценарного тестирования на проникновение. Тестирование будет имитировать действия целевой угрозы (APT-группа или мотивированный киберпреступник), ставящей целью хищение баз персональных данных. Сценарий будет включать этапы:

*1. Разведка***:** сбор информации о внешнем периметре системы (доменные имена, IP-адреса) и поиск публично доступных метаданных в IaC-репозиториях.

2. Первоначальное проникновение: попытка эксплуатации уязвимости в веб-приложении или фишинговой атаки на администратора для получения учетных данных доступа к панели управления VK Cloud.

3. Расширение привилегий: в рамках облачного тенанта – попытка горизонтального перемещения между виртуальными машинами и получения доступа к экземпляру СУБД, содержащему ПДн.

4. Достижение цели: попытка эксфильтрации данных из изолированной подсети через уязвимости в настройках NAT-шлюза (посредник между внутренней и внешней сетью) или путем компрометации систем резервного копирования.

Ситуативная задача. Объектом защиты выступает информационная система персональных данных (ИСПДн) интернет-магазина, обрабатывающая: ФИО, контакты, адреса доставки (не более 100 000 субъектов); инфраструктура: размещена в VK Cloud Solutions с использованием виртуальных машин (AlmaLinux), баз даны PostgreSQL и S3-хранилища для резервных копий.

Ключевые угрозы для уровня защищенности[56] (УЗ-3) представлены в табл. 1.7

Таблица 1.7

Ключевые угрозы для УЗ-3

Категория	Примеры	Меры противодействия
Фишинг	Email-атаки на сотрудников	Обучение + многофакторная аутентификация
Уязвимости ПО	Эксплойты в веб-интерфейсе магазина	Еженедельный патчинг + WAF[57]
Инсайдеры	Утечка баз клиентов менеджером	RBAC + DLP-мониторинг[58]
DDoS	Атаки на API платежной системы	Anti-DDoS VK Cloud + лимит запросов[59]

Специфика VK Cloud: ответственность провайдера: физическая защита ЦОД, гипервизор, резервирование; ответственность клиента: настройка MFA, шифрование данных, управление доступом.

Сценарное тестирование по ENISA Threat-Led Penetration Testing.

Цель: верификация эффективности мер против актуальных TTPs.

Этап 1. Разведка (Reconnaissance).

Сценарий: сбор информации через SSL-сертификаты и DNS-записи S3-корзин.

Инструменты: Shodan + CloudScraper (системы поиска уязвимых устройств).

---

[56] Приказ Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» // СПС «КонсультантПлюс».
Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» //СПС «КонсультантПлюс».

[57] слой политик безопасности, предназначенный для предотвращения эксплуатации уязвимости (подробнее https://habr.com/ru/companies/acribia/articles/481774/)

[58] управление доступом на основе ролей (широко используемая модель контроля доступа для обеспечения безопасности, которая ограничивает доступ к системам и авторизацию на основе ролей и обязанностей сотрудников в организации)

[59] имеется ввиду мгновенная фильтрация вредоносного трафика сайтов и веб-приложений.

Ожидаемая защита:

1. VK Cloud: Скрытие метаданных инфраструктуры :cite.

2. Клиент: Конфигурация bucket как «private» (для облачных хранилищ означает, что дотуп данных ограничен).

Этап 2. Компрометация веб-интерфейса.

Сценарий: SQL-инъекция в форму поиска товаров, получение доступа к СУБД.

Инструменты: SQLmap + Burp Suite (тестирование веб-приложений).

Ожидаемая защита:

1. WAF VK Cloud с сигнатурами OWASP Top 10[60].

2. Клиент: применение параметризованных запросов.

Этап 3. Эскалация привилегий.

Сценарий: использование уязвимости CVE-2024-XXXX в AlmaLinux, доступ к хосту.

Инструменты: Metasploit (поиск уязвимостей путем проникновения).

Ожидаемая защита:

1. VK Cloud: Автоматические обновления ядра ОС.

2. Клиент: SELinux в режиме enforcing (запрет доступа на основании политик).

Этап 4. Кража данных.

Сценарий: копирование нешифрованной БД из S3 → утечка 50 000 записей.

Инструменты: AWS[61] CLI (имитация интерфейса с настройкой на VK Cloud).

Ожидаемая защита:

1. Клиент: шифрование ГОСТ 28147-89 перед загрузкой в S3 :cite [1].

2. VK Cloud: детектирование аномалий доступа через Cloud Alerting.

4. Результаты тестирования и оптимизация.

По результатам проведенного тестирования защищенности инфраструктуры VK Cloud были идентифицированы критические отклонения от требований регуляторных стандартов, требующие незамедлительной оптимизации.

Выявленные уязвимости и оценка рисков:

1. Обнаружен открытый порт 3306 на сервисе Managed PostgreSQL. Данная конфигурационная ошибка классифицируется как риск уровня High (Высокий), поскольку формирует вектор для проведения внешних атак на подсистему управления базами данных. Это создает прямую угрозу конфиденциальности и целостности хранимой информации, потенциально

[60] https://owasp.org/www-project-top-ten/

[61] Платформы облачных сервисов AmazonWebServis (отметим, что в соответствии с законодательством персональные данные должны быть локализованы, поэтому активно осуществляется переход на российские решения. В данном случае указывается как использование популярных отраслевых стандартов и инструментов для удобства клиентов, вся инфраструктура развернута в ЦОД VK Cloud).

позволяя злоумышленнику инициировать несанкционированные подключения, эксплуатировать уязвимости СУБД или осуществлять перебор учетных данных (брутфорс атаки).

2. Установлено отсутствие многофакторной аутентификации (MFA) для привилегированных учетных записей администраторов и менеджеров. Данный недостаток присвоена категория риска Medium (Средний). Несмотря на то, что для эксплуатации данной уязвимости требуются компрометированные учетные данные, ее реализация позволяет злоумышленнику, в том числе инсайдеру, получить полный контроль над облачной средой и критически важными сервисами, что приводит к эскалации привилегий и невозможности отследить несанкционированные действия.

Рекомендации по устранению в соответствии с требованиями ФСТЭК России.

Для устранения уязвимости № 1 необходимо немедленно применить механизмы групп безопасности (Security Groups) или программные средства защиты периметра (NGFW) для блокировки публичного доступа к порту 3306. Разрешить входящие подключения к СУБД следует только с доверенных IP-адресов или из определенных сегментов внутренней сети, что соответствует базовым принципам сетевой сегментации, предписываемым ФСТЭК.

Для устранения уязвимости № 2 требуется в обязательном порядке задействовать механизм многофакторной аутентификации (MFA) для всех учетных записей, обладающих правами административного доступа к панели управления и критическим сервисам облачной платформы. Данная мера напрямую соотносится с требованием ФСТЭК по усиленной аутентификации для субъектов доступа с расширенными полномочиями.

План мероприятий по оптимизации. Для полного устранения выявленных нарушений и приведения облачной инфраструктуры в соответствие с регуляторными требованиями установлен общий срок реализации всех корректирующих мер – 14 календарных дней. В течение этого периода необходимо выполнить реконфигурацию сетевых политик, активировать и настроить MFA для привилегированных учетных записей, а также провести верификацию выполненных изменений путем повторного тестового контроля защищенности (re-test).

Рекомендации по ФСТЭК. Особенности реализации мер защиты для информационных систем «жёлтого» уровня (УЗ-3)**.** При построении системы защиты информационных систем персональных данных «жёлтого» уровня (класс УЗ-3) в среде VK Cloud применяется адаптированный подход, позволяющий достичь баланса между соответствием регуляторным требованиям и оптимизацией ресурсов.

Криптографические требования для данного класса являются минимальными. В соответствии с установленными нормами, обязательное шифрование данных требуется применять исключительно при их передаче по открытым или общедоступным каналам связи, например, через публичные сети Интернет. При этом шифрование трафика внутри защищенного

периметра облачной инфраструктуры, между доверенными сегментами виртуальной сети, не является обязательным. Это позволяет снизить вычислительную нагрузку на компоненты системы без снижения общего уровня защищенности [17].

Режим аудита и контроля также применяется в упрощенном виде. Для систем УЗ-3 установлен сокращенный срок обязательного хранения журналов событий безопасности (может быть утвержден локальным, если не указаны сроки в нормативных документах). Данная мера сокращает объемы занимаемого дискового пространства в системах мониторинга и SIEM и уменьшает операционные затраты на их сопровождение, при этом сохраняя возможность ретроспективного анализа инцидентов в течение регламентированного периода.

Ресурсная оптимизация достигается за счет активного использования управляемых сервисов (PaaS), предоставляемых платформой VK Cloud. Развертывание защищенной инфраструктуры на базе управляемых сервисов баз данных, бэкенда и балансировщиков нагрузки позволяет сократить совокупные затраты на построение и эксплуатацию системы защиты примерно на 40% по сравнению с моделью самостоятельной реализации аналогичных мер контроля на инфраструктурных сервисах (IaaS). Экономический эффект формируется за счет передачи провайдеру облачных услуг ответственности за обновление, мониторинг и отказоустойчивость базовых компонентов, что позволяет команде безопасности заказчика сконцентрироваться на прикладных мерах защиты, специфичных для бизнес-логики приложения.

Заключение и рекомендации по построению системы защиты для ИСПДн «жёлтого» уровня в VK Cloud. Разбор модели безопасности продемонстрировал значительное повышение уровня защищенности информационной системы. Эффективность модели была верифицирована в ходе сценарного тестирования: если на начальном этапе покрытие актуальных угроз оценивалось в 70% (защита от тактик противника по шкале 7 из 10), а ключевым пробелом являлась некорректная конфигурация списков контроля доступа к сетевым ресурсам (NACL), то после проведенной оптимизации достигнуто соответствие обязательным требованиям для класса УЗ-3. Это подтверждает адекватность и действенность выбранного подхода.

Использование платформы VK Cloud для развертывания ИСПДн «жёлтого» уровня предоставляет ряд стратегических преимуществ:

- готовая аттестационная готовность. Развертывание системы на основе предварительно сертифицированной инфраструктуры провайдера, имеющей действующий аттестат соответствия ФСТЭК (№ 3740.XXXXX.2024 от 16 декабря 2024 года), позволяет клиенту существенно сократить временные и финансовые затраты на прохождение процедуры обязательной аттестации всей платформы;

- встроенная автоматизация мониторинга. Нативная интеграция с управляемой SIEM VK Cloud обеспечивает централизованный сбор,

корреляцию и анализ событий безопасности, что ускоряет время обнаружения и реагирования на инциденты ИБ;

- значительная экономия TCO (Total Cost of Ownership - совокупная стоимость владения). Модель разделенной ответственности и использование управляемых сервисов исключают капитальные затраты на аттестацию базовой инфраструктуры, что, согласно расчетам, снижает совокупную стоимость владения защищенной ИТ-средой.

Для обеспечения комплексной и устойчивой защиты на постоянной основе рекомендуется внедрить цикличное проведение ежеквартальных тестов на проникновение по методологии ENISA Threat-Led Penetration Testing (TLPT). Стандартный цикл тестирования должен включать этапы: подготовки (согласование правил взаимодействия), активной разведки (OSINT, сканирование), целевой компрометации (реализация сценариев атак), глубокого анализа полученных результатов и формирования детализированного отчета. Особый фокус при планировании сценариев следует уделять моделированию наиболее вероятных для систем УЗ-3 угроз, таких как целевой фишинг для кражи учетных данных сотрудников и риски, связанные с внутренними нарушителями.

Таким образом, представленная модель наглядно демонстрирует, что даже для систем «жёлтого» уровня критически важным фактором является синхронизация мер защиты, реализуемых клиентом, с возможностями и ответственностью облачного провайдера. Регулярное проактивное тестирование, такое как ENISA TLPT, трансформирует систему безопасности из статичной в адаптивную, позволяя выявлять и устранять латентные архитектурные и конфигурационные уязвимости до момента их эксплуатации в реальных кибератаках.

Глоссарий:[62]

APT (Advanced Persistent Threat) - целевая долгосрочная кибератака, проводимая государственными или высокоорганизованными группами. Пример: SolarWinds (2020).

CIA-триада (Confidentiality, Integrity, Availability) - базовая модель ИБ: конфиденциальность, целостность, доступность. Ключевой критерий классификации угроз в ЕС.

IoT (Интеренет вещей - Internet of Thungs) – это сеть физических устройств со встроенными датчиками программным обеспечением и возможностью подключения к интернету.

Paas (Platform as a Servis) - модель облачных технологий, которая предоставляет пользователям готовую платформу для создания, тестирования,

[62] Глоссарий структурирован по принципам ГОСТ Р 7.0.100-2018 и охватывает термины из: нормативных документов (187-ФЗ, GB/T 22239); технологических контекстов (квантовая криптография, MITRE ATT&CK); отраслевой специфики (КИИ, IoT, телекоммуникации).

развертывания и управления приложениями без необходимости контролировать инфраструктуру.

MITRE ATT&CK® - база знаний тактик, техник и процедур (TTPs) киберпреступников. Используется в ЕС и РФ для классификации угроз.

Threat Intelligence - система сбора и анализа данных об угрозах. (примеры платформ: MISP, QRadar).

TTPs (Tactics, Techniques, Procedures) - тактики, техники и процедуры злоумышленников. Источник: матрица MITRE ATT&CK.

MLPS 2.0 (Multi-Level Protection Scheme) - китайская система классификации объектов защиты по уровням безопасности (GB/T 22239).

SQL – инъекция (SQLi) - распространенный способ атак на веб-приложения, при котором злоумышленник внедряет вредоносный SQL код в запросы к базе данных.

Атака на BGP (Border Gateway Protocol) - манипуляция маршрутами интернет-трафика для перехвата данных или нарушения доступности.

Атаки на цепочки поставок - вид кибератаки**,** при которой злоумышленники атакуют не саму компанию, а ее поставщиков или партнеров. Цель такой атаки – получить несанкционированный доступ к инфраструктуре или данным организации через компрометацию сервиса или ИТ услуг, предоставляемым третьим лицом.

Воздействие - заключительный этап атаки, на котором злоумышленники наносят ущерб (шифрование и удаление данных, нарушение работы серверов и проч.).

Веб-приложение - представляет собой программное обеспечение, доступное через веб-браузер, которое выполняет определенные функции для пользователей.

Инфраструктура (информационно-техническая инфраструктура) - это совокупность аппаратных, программных, сетевых и сервисных компонентов, обеспечивающих функционирование, хранение, обработку и передачу данных в организации (основа, на которой строятся все ИТ сервисы и бизнес приложения предприятий).

КИИ (Критическая информационная инфраструктура) - объекты, выход из строя которых угрожает национальной безопасности. Примеры: энергосети, транспортные системы.

Киберсуверенитет - концепция контроля национального цифрового пространства (закон о «суверенном Рунете» (РФ), Великий киберщит Китая).

Кибератака – попытка получить несанкционированный доступ к информационной системе или оборудованию, чтобы нарушить из работоспособность, похитить или уничтожить данные.

Компроментация сервиса - это ситуация, когда конфиденциальная информация попадает в руки лиц, которым она не предназначалась, и может быть использована во вред владельцу.

Постквантовая криптография (PQC) - алгоритмы, устойчивые к взлому квантовыми компьютерами. Стандарт NIST FIPS 203 (США).

СКЗИ (Средства криптографической защиты информации) - аппаратно-программные инструменты для шифрования и электронной подписи.

Угроза доступности (Availability Threat) - воздействие, нарушающее доступ к ресурсам. Пример: DDoS-атака на видеосервис**.**

Уязвимость нулевого дня (Zero-Day) - неизвестная разработчику ошибка в ПО, используемая злоумышленниками до исправления.

ФСТЭК (Федеральная служба по техническому и экспортному контролю) - регулятор ИБ в РФ. Утверждает стандарты (ГОСТ Р) и методики оценки угроз.

ЭКБ (Электронная компонентная база) - отечественные микропроцессоры и чипы для СКЗИ (Проект «Эльбрус»).

Эксфильтрация - несанкционированная передача данных их среды жертвы в инфраструктуру злоумышленника.

Эксплойт (от англ. Exploit - эксплуатировать) - компьютерная программа, фрагмент программного кода или последовательных команд, использующих уязвимости в программном обеспечении для атаки на вычислительную систему.

Вопросы и задания для самоконтроля:

1. Дайте определение угрозы информационной безопасности (ИБ) в соответствии с триадой CIA. В чем заключается полисемичность этого понятия в глобальном контексте?
2. Назовите и охарактеризуйте четыре основные характеристики любой угрозы ИБ: источник, цель, способ реализации и последствия.
3. Объясните, как политико-экономические факторы (политэкономические детерминанты) влияют на формирование национальных подходов к классификации угроз ИБ.
4. В чем заключаются ключевые концептуальные различия между европейской, китайской и российской моделями информационной безопасности? Соотнесите их с понятиями «киберустойчивость», «киберсуверенитет» и «технологическая независимость».
5. Сравните нормативно-правовые основы управления ИБ в ЕС (GDPR, NIS2), Китае (Закон о кибербезопасности) и России (закон о КИИ, «суверенном Рунете»). Какой документ в каждой юрисдикции является базовым?
6. Проранжируйте приоритеты защиты (конфиденциальность, целостность, доступность, национальная безопасность) для ЕС, Китая и России. Объясните, чем обусловлены такие различия.
7. Опишите, как в каждой из трех юрисдикций подходят к вопросу контроля данных: свободное перемещение, жесткий государственный контроль, суверенное управление.

8. Какие типы нарушителей (Threat Actors) являются приоритетными для регуляторов в ЕС, Китае и России соответственно (киберпреступность, государственные APT, инсайдеры)? Приведите примеры.

9. Перечислите ключевые инфраструктурные и регуляторные особенности российского сегмента интернета (Рунета), влияющие на ландшафт угроз.

10. Опишите пошаговый алгоритм выявления и оценки угроз ИБ в РФ в соответствии с методиками ФСТЭК.

11. Каковы основные технологические тренды и уникальные инфраструктурные риски в Рунете на примере развития IoT, 5G и импортозамещенного ПО?

12. Что такое модель разделения ответственности (Shared Responsibility Model) в облачной среде? Разграничьте зоны ответственности провайдера (на примере VK Cloud) и клиента.

13. Какие основные фреймворки и таксономии используются для анализа угроз в ЕС (ENISA, MITRE ATT&CK), Китае (GB/T) и России (ГОСТ, адаптированный MITRE ATT&CK)?

14. Что такое Threat-Led Penetration Testing (TLPT) по методологии ENISA? Опишите основные этапы проведения такого тестирования.

15. Какие технологические средства (SIEM, DLP, NGFW) и организационные меры (аудит, обучение) являются наиболее эффективными для противодействия современным угрозам?

16. Составьте модель угроз (Threat Model) для объекта КИИ в энергетическом секторе России, используя фреймворк STRIDE и учитывая требования ФСТЭК.

17. DDoS-атаки на SCADA-системы и эксплуатация BGP-уязвимостей/

18. В чем заключаются ключевые направления развития постквантовой криптографии в России?

19. Проанализируйте оптимистичный и пессимистичный сценарии развития глобальных таксономий угроз ИБ до 2030 года. Какие индикаторы свидетельствуют в пользу каждого из них?

20. Сформулируйте ключевые выводы и рекомендации для специалиста ИБ, проектирующего систему защиты транснациональной компании, работающей в юрисдикциях ЕС, Китая и России.

ГЛАВА 2. КЛЮЧЕВЫЕ ПРИНЦИПЫ КЛАССИФИКАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Полиморфизм современных киберугроз и различие национальных подходов к информационной безопасности детерминируют необходимость разработки комплексных таксономий. В сфере информационной безопасности термин «таксономия» является общепринятым и не является исключительно «западной концепцией» в противовес классификации. Оба термина описывают систематизацию, но «таксономия» - это более глубокая и структурированная система.

Классификация угроз ИБ представляет собой методологический аппарат для систематизации векторов атак, атрибуции угроз-акторов и выработки адекватных контрмер. В условиях фрагментации киберпространства, когда глобальная сеть Интернет превращается во множество локальных сетей, границы между которыми устанавливаются искусственно на уровне национальных законодательств и государственного регулирования, таксономии выполняют не только техническую, но и геополитическую функцию, отражая приоритеты национальных моделей ИБ [51].

2.1. Угрозы безопасности информации: понятие и классификация

Угроза безопасности информации - это потенциальная возможность события (действия, бездействия, процесса или явления), которое, используя уязвимости активов информации (данных, систем, персонала, процессов), может привести к нанесению ущерба владельцу/пользователю информации через нарушение её конфиденциальности, целостности или доступности (триада CIA: Confidentiality, Integrity, Availability) [1].

Угрозу безопасности можно рассматривать как модель, состоящую из нескольких элементов, рассмотрим каждый из них.

1. Потенциальная возможность (вероятность).

Это прогностический компонент управления рисками. Угроза существует объективно, даже если нет явных признаков атаки. Например, угроза DDoS-атаки существует для любого онлайн-сервиса. Задача специалиста в оценке вероятности ее реализации на основе факторов – мотивы, вектор атаки и контектс.

2. Источник угрозы (Threat actor).

Классификация источников – основа таксономии угроз. Угроза всегда исходит от какого-либо субъекта (злоумышленник, недовольный сотрудник) или объекта (стихийное бедствие, сбой оборудования).

3. Использование уязвимостей.

Связующее звено между угрозой и реализацией риска. Угроза реализуется не сама по себе, а через слабости в защите (дыры в ПО, слабые пароли, необученный персонал, отсутствие резервного копирования). Угроза + Уязвимость = Риск.

4. Объект воздействия (актив).

Угроза всегда направлена на конкретный ценный актив: данные (база клиентов), систему (веб-сервер), процесс (авторизация платежа) или персонал (системный администратор).

5. Нежелательное последствие (нарушение CIA).

Цель любой угрозы - причинить ущерб через базовые цели конфиденциальность (несанкционированный доступ, раскрытие, утечка), целостность (несанкционированное изменение, уничтожение, подделка), доступность (блокирование доступа, вывод из строя, уничтожение).

6. Ущерб (вред).

Итоговая оценка последствий. Ущерб может быть как прямой, так и косвенный (нанесение материального, финансового, репутационного ущерба или ущерба деловой репутации).

Таким образом, **угроза** – это источник опасности, который, эксплуатируя уязвимость, воздействует на актив, приводя к нарушению конфиденциальности, целостности или доступности и причинению ущерба [6].

Примеры корректной формулировки угроз:

- угроза раскрытия коммерческой тайны (нарушение конфиденциальности) в результате копирования сотрудником файлов на личный USB-накопитель (использование уязвимости - отсутствие контроля съёмных носителей);
- угроза потери доступности CRM-системы (нарушение доступности) в результате успешной DDoS-атаки со стороны киберпреступной группировки (источник), использующей недостаточную пропускную способность канала (уязвимость);
- угроза подделки финансовой отчётности (нарушение целостности) вследствие компрометации учётной записи главного бухгалтера через фишинг-письмо (способ).

Важно понимать, что угроза не является синонимом инцидента. Угроза – это потенциальная опасность, а инцидент – это реализовавшаяся угроза (произошедшее событие). Задача информационной безопасности – управлять рисками, то есть предотвращать реализацию угроз или минимизировать ущерб от неё [33].

Наиболее полный и структурированный подход предлагается в стандартах и лучших практиках, таких как ГОСТ Р ИСО/МЭК 27001[63], ISO/IEC 27001.

Возможна систематизация угроз по трем основным критериям, что позволяет анализировать их с разных сторон и строить комплексные меры защиты.

Критерий I: По источнику происхождения («Кто/Что?»).

[63] Национальный стандарт РФ «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

Это классификация по природе источника угрозы:

1. Природные (стихийные бедствия и явления):

- пожары, наводнения, землетрясения, ураганы;
- электромагнитные бури (воздействие на оборудование) [23].

2. Техногенные (связанные с деятельностью человека и техникой).

- технические сбои: отказ оборудования (серверов, дисков, сетевых устройств), сбои ПО, перебои электропитания, износ носителей;
- ошибки персонала (самый частый источник): непреднамеренные действия: ввод неверных данных, случайное удаление файлов, ошибки в настройке систем безопасности, потеря устройств.

3. Умышленные (преднамеренные злонамеренные действия).

Внешние злоумышленники:

- хакеры (финансовый интерес, шпионаж, активизм);
- киберпреступные группировки (ransomware, DDoS-атаки, кража данных);
- конкуренты (промышленный шпионаж).

Внутренние нарушители:

- недовольные или коррумпированные сотрудники (инсайдеры);
- бывшие сотрудники с действующими учётными записями.

Организованные группы: государственные структуры (кибервойска), террористические организации.

Критерий II: По способу воздействия («Как?»).

Классификация по методу реализации угрозы (механизму атаки).

1. Угрозы раскрытия (нарушения конфиденциальности):

- перехват данных (сниффинг, атака «человек посередине»);
- социальная инженерия (фишинг, вишинг);
- кража устройств (ноутбуков, смартфонов);
- несанкционированный доступ к информации (подбор паролей, использование чужих учётных записей).

2. Угрозы целостности:

- несанкционированная модификация данных (изменение, подмена);
- саботаж (умышленное искажение информации);
- внедрение вредоносного ПО (вирусы, черви, трояны, ransomware);
- компрометация систем (взлом с получением прав администратора).

3. Угрозы доступности (нарушения работоспособности):

- атаки на отказ в обслуживании (DDoS);
- блокирование ресурсов (шифрование ransomware);
- физическое уничтожение или повреждение оборудования;
- технические сбои, делающие систему неработоспособной.

Критерий III: По объекту воздействия («На что?»).

Классификация по цели или компоненту информационной системы, на который направлена атака.

1. Информационные (данные):

- кража, уничтожение, шифрование, модификация баз данных, файлов, переписки.

2. Программные (ПО):

- внедрение вредоносного кода, эксплуатация уязвимостей, кража исходного кода, изменение алгоритмов работы.

3. Технические (аппаратура, «железо»):

– физический вывод из строя (серверов, маршрутизаторов, кабельных линий);

– перехват побочных излучений электронных устройств;

– подключение несанкционированного оборудования (аппаратные закладки).

4. Коммуникационные (каналы связи) [55]:

- перехват или блокирование сетевого трафика, вмешательство в протоколы связи, спуфинг (подмена сетевых адресов).

5. Персонал (люди):

- социальная инженерия, вербовка, шантаж, дезинформация, вынуждение к действиям.

Для практического применения удобно использовать инструмент для качественного анализа рисков. Например, для критичного актива «База данных клиентов» (Табл. 2.1).

Таблица 2.1.

Интегрированная модель для анализа

Источник угрозы	**Угроза раскрытия (Как?)**	**Угроза целостности (Как?)**	**Угроза доступности (Как?)**
Внешний злоумышленник	Взлом веб-интерфейса и кража данных	SQL-инъекция и изменение данных	DDoS-атака на сервер БД
Внутренний сотрудник	Копирование данных на USB-носитель	Умышленное искажение записей	Удаление таблиц по неосторожности
Техногенный сбой	-	-	Отказ дискового массива (RAID)

Краткая систематизация по другим популярным критериям:

По уровню квалификации злоумышленника: случайные, любители, профессионалы, организованные группы.

По используемым средствам: программные (вирусы), аппаратные, физические, психологические (соц. инженерия).

По этапу воздействия (Cyber Kill Chain[64]):

– разведка (Reconnaissance);

– оружие (Weaponization);

[64] The 6 Stages of the Cyber Attack Lifecycle https://www.cbtnuggets.com/blog/certifications/security/the-6-stages-of-the-cyber-attack-lifecycle

- доставка (Delivery);
- эксплуатация (Exploitation);
- установка (Installation);
- команда и управление (Command & Control);
- действия для достижения цели (Actions on Objectives).

Для построения системы защиты необходимо не просто перечислить угрозы, а провести оценку рисков, комбинируя все критерии: определить ценные активы (Критерий III), выявить уязвимости, которым они подвержены, и спрогнозировать, какие источники (Критерий I) могут использовать эти уязвимости теми или иными способами (Критерий II) для нанесения ущерба [2]. Это позволит расставить приоритеты и выделить ресурсы на защиту самого важного.

2.2. Угроза ИБ по источнику возникновения

Данный критерий отвечает на вопрос «Кто или что является инициатором угрозы?» и является первичным для организации периметра защиты и контроля доступа. Источник угрозы - это активный субъект или пассивное явление, которые служат первопричиной инцидента ИБ. Классификация по истопнику позволяет предсказывать мотивы и цели атаки, что критически важно для построения адекватной защиты [37].

Внешние угрозы (источник находится за пределами контролируемой периметром организации) характеризуются высоким уровнем профессионализма и мотивации.

Примеры: государственные APT-группы, хактивисты, киберпреступники, недобросовестные конкуренты.

Меры противодействия: межсетевые экраны (NGFW), системы обнаружения и предотвращения вторжений (IDS/IPS), Anti-DDoS решения, сервисы Threat Intelligence.

Внутренние угрозы (инсайдеры) – угрозы, вызванные деятельностью лиц, имеющих легальный доступ к информационным активам организации. Включают инсайдеров-злоумышленников и неквалифицированных пользователей. Наиболее опасны ввиду наличия привилегий и знания внутренних процессов.

Примеры: недовольные сотрудники, персонал, подвергшийся социальной инженерии, небрежные пользователи.

Меры противодействия: системы управления доступом (RBAC), мониторинг активности пользователей и привилегированных учетных записей (UEBA), DLP-системы, строгая процедура увольнения.

Природные (стихийные) угрозы: форс-мажорные воздействия на критическую информационную инфраструктуру (КИИ), обусловлены воздействием факторов непреодолимой силы.

Примеры: пожары, наводнения, землетрясения, удары молнии, перепады напряжения.

Меры противодействия: резервное копирование в географически распределенные ЦОД, системы бесперебойного питания (UPS), план аварийного восстановления (DRP).

Ключевые выводы:

- для разных источников используется разная защита (внешние угрозы - защитные сетевые экраны, для внутренних – сегментация сети и DLP[65], для техногенных – резервирование);
- главный риск весьма часто внутри защищаемого объекта;
- контекст определяет источник (для энергосистемы главная угроза –APT группы, для интернет-магазина – DDoS и т.п.).

Отметим нормативное регулирование источников угроз в представлении Европейский союза, Китая (КНР) и Российской Федерации. Сравнительный анализ регуляторных подходов представлен в табл. 2.2.

Таблица 2.2

Нормативная оценка источников угроз

Критерий	**Европейский союз**	**Китай (КНР)**	**Российская Федерация**
Приоритетность внешних угроз	Киберпреступность (NIS2 Directive[66])	Государственные APT (GB/T 22239)	Гибридные угрозы (ФСТЭК)
Классификация инсайдеров	По уровню доступа к PD (GDPR Art. 4)	По лояльности	По допуску к ГТС (ФСТЭК №239)
Учет природных угроз	В рамках CER Directive[67]	Через стандарт GB/T 37044	По ГОСТ Р
Методология атрибуции	ENISA Threat Landscape	CNCERT Technical Reports[68]	Система ФСТЭК-мониторинга

Таким образом, в ЕС фокус на негосударственных субъектах осуществляется в соответствии с директивой NIS2, при этом акцент на защите персональных данных от киберпреступности [3]. Доминирование парадигмы государственно-спонсируемых APT-групп и жесткий контроль внешнего трафика через «Великий китайский файрвол» характерная особенность КНР. В РФ используется синтез подходов с акцентом на гибридные угрозы. Требования к сегментации сетей для КИИ (ФСТЭК № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»).

[65] DLP-система (от. англ Data Leak Prevention) - система, которая предотвращает утечку конфиденциальной информации из внутренней сети компании

[66] Директива по кибербезопасности ЕС NIS2 https://nis2directive.eu/

[67] Что представляет собой директива о повышении устойчивости критически важных объектов https://www.upguard.com/blog/cer-directive

[68] Национальный центр экстренного реагирования на компьютерные инциденты (КНР).

2.3. Угроза ИБ по характеру воздействия

Деление на «активные/пассивные» и «преднамеренные/ непреднамеренные» угрозы определяет архитектуру систем детектирования (IDS) и предотвращения (IPS). В информационной безопасности данные системы критически важные элементы защиты сети.

Критерий угроз ИБ по характеру воздействия описывает намерения и активность субъекта угрозы, что критично для настройки систем детектирования и реагирования.

Преднамеренные угрозы: целенаправленные атаки с использованием эксплойтов и социальной инженерии.

Примеры: хакерская атака, установка вредоносного ПО, умышленная кража данных инсайдером.

Случайные угрозы: непреднамеренные действия, вызванные человеческим фактором или сбоями в работе средств обнаружения и коррекции.

Примеры: ошибочное удаление данных, отправка конфиденциальной информации не тому адресату, неправильная настройка сервера.

Активные угрозы: направлены на непосредственное изменение системы, данных или потока информации. Злоумышленник активно воздействует на цель.

Примеры: взлом, внедрение кода, модификация пакетов данных, блокирование ресурсов (DDoS).

Пассивные угрозы: направлены на несанкционированный сбор информации (сниффинг, сетевой футпритинг) без воздействия на систему.

Примеры: прослушивание сетевого трафика (сниффинг), сканирование портов, копирование данных, карты компьютерных сетей, содержащей список хостов, их доменные имена, адреса, открытые порты, используемые ОС.

Рассмотрим более подробно технику сбора информации футпринтинг (footprinting) и почему он важен для правоохранительных органов. Футпринтинг одна из фаз, предшествующих атаке и это не просто технический скан сети. Это систематический процесс сбора и анализа информации о цели для построения ее цифрового портрета. Для сотрудников МВД этот этап аналогичен сбору оперативных данных: установлению связей, мест работы, привычек и инфраструктуры преступной группы [7].

В сфере безопасности отслеживание представляет информационную базу, необходимую для классификации источников угроз. Оценки их возможностей и определения намерений. В таких системах как MITRE ATT&CK отслеживание наиболее тесно связано с тактикой разведки и частично с тактикой развития ресурсов – этапами, на которых злоумышленники собирают информацию для подготовки атак. Понимание этого процесса позволяет специалистам по кибербезопасности, в том числе полицейским подразделениям предвидеть атаки на ранних этапах угрозы [48].

Цели футпринтинга различаются для злоумышленника и для правоохранительных органов. Более подробно в таблице 2.3.

Таблица 2.3

Футпринтинг в контексте информационной безопасности (злоумышленник - правоохранительные органы)

Аспект	Атакующая сторона (злоумышленник)	Обороняющаяся сторона (правоохранительные органы)
Цель	Построение детального профиля цели для последующей атаки (уязвимости, векторы атак, точка входа)	Получение цифрового профиля[69] злоумышленника (его инструменты, методу, инфраструктуру) для его идентификации, расследования и привлечения к ответственности
Объект сбора данных	Целевая организация, система или сеть	Сам злоумышленник или киберпреступная группа
Методы и инструменты	Поиск в социальных сетях, анализ DNS, OSINT (разведка по открытым источникам) WHOIS, Nmap	Изучение логов атак, вредоносного кода, метаданных файлов Взаимодействие с CERT[70], SpiderFoot
Конечный результат	«Карта» уязвимостей и план атак	Доказательная база для установления виновника (юридическое дело)

Этапы футпринтинга с точки зрения злоумышленника:

1. Изучение организации-цели (организационное исследование).

На этом этапе определяется контекст, в котором работает *Цель*:

- сфера деятельности (например, финансы, энергетика, транспорт);
- география;
- руководство и организационная структура;
- публичная отчетность (годовые отчеты, нормативные документы);

[69] Четкого определения «цифрового профиля» в существующих нормативных документах не содержится (источник Мочалов А.Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex Russica. 2021. №9 (178). URL: https://cyberleninka.ru/article/n/tsifrovoy-profil-osnovnye-riski-dlya-konstitutsionnyh-prav-cheloveka-v-usloviyah-pravovoy-neopredelennosti), тут и далее будет использовано определение Постановления Правительства от 03.06.2019 № 710 «О проведении эксперимента по повышению качества и связанности данных, содержащихся в государственных информационных ресурсах» как определенным образом упорядоченный массив официальных данных о гражданине или юридическом лице, достоверность которых подтверждена компетентными органами государства.

[70] Национальные центры реагирования на инциденты - в РФ Национальный координационный центр по компьютерным инцидентам (НКЦКИ) как часть Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА).

- пратнерские отношения и связи в цепочке поставок;

- исторические инциденты.

Отмеченная информация важна для классификации угроз, поскольку различные отрасли привлекают и разных злоумышленников. Финансовые учреждения становятся мишенью для спонсируемых киберпреступных группировок, государственные учреждения – мишень для спонсируемых государственными APT групп. Операторы критически важной инфраструктуры подвергаются атакам групп, нацеленных на саботаж и нарушение работы.

2. Анализ DNS-инфраструктуры (доменные имена и субдомены, провайдеры, схемы хостинга, метаданные сертификатов SSL и проч.).

3. Работа с открытыми источниками (далее будет пункт разобран подробнее).

4. Определение сетевых диапазонов.

5. Использование дополнительных методов (например, анализ SSL-сертификатов)[71].

В целях эффективной реализации оперативной работы особое внимание уделить при работе с DNS:

– Zone Transfer (копирование записей DNS с основного сервера), что может дать полную карту сети;

– перебор имен хостов часто выявляет скрытые сервисы;

– обратные DNS-запросы помогают идентифицировать хосты (процесс, при котором по IP адресу можно получить его доменное имя).

Открытые источники информации источников сегодня играют значительную роль в оперативно-розыскной деятельности. Открытые источники (OSINT, Open Sourse Intelligent) представляют собой общедоступную информацию. Среди источников можно выделить официальные веб-сайты и пресс-релизы, социальные сети, объявления о вакансиях (технологии, используемые в кампании), научные публикации, утечки баз данных, корпоративные реестры, форумы технических сообществ.

Социальные сети и специализированные ресурсы являются настоящим кладезем информации, способным существенно увеличить оперативный потенциал специализированных служб.

Рассмотреть список российских ресурсов интересный для оперативно-розыскной деятельности.

1. Профессиональные сети и корпоративные ресурсы:

- Хабр Карьера (анализ вакансий с указанием стека технологий; профили IT-специалистов с историями трудоустройства; обсуждения корпоративных практик в комментариях; группы компаний и аффилированные лица);

[71] Цифровой сертификат, удостоверяющий подлинность сайта. Подробнее в статье «Что такое SSL-сертификат – определение и описание» по адресу https://www.kaspersky.ru/resource-center/definitions/what-is-a-ssl-certificate

- Российские GitHub-аналоги (GitFlic и Forge; открытые репозитории государственных организаций; учетные записи сотрудников с корпоративными email);

- HeadHunter (HH.ru) - резюме сотрудников с детализацией профессиональных навыков; история трудовой деятельности и проектов; указание используемых технологий и методологий.

2. Ресурсы с утечками данных и кибербразведки (XAKEP.RU и аналогичные ресурсы с публикациями о уязвимостях в российском ПО; обсуждения методов пентеста локальных систем; анализ инцидентов безопасности в РФ).

3. Специализированные поисковые системы и базы:

- ИПС Яндекс (глубокий поиск по российским доменам, поиск по конкретным типам файлов (.doc, .xls, .pdf); анализ географической привязки ресурсов, файлообменники с раздачей корпоративного ПО и баз данных, учебных материалов внутреннего обучения, архивы с конфигурациями сетевого оборудования.

- 2GIS и аналоги (планировка офисных помещений; информация о арендаторах бизнес-центров; контакты ответственных лиц).

4. Социальные сети и личные профили:

- VK («Вконтакте») закрытые группы сотрудников компаний; фотографии с корпоративных мероприятий; геометки офисов и рабочих мест; списки друзей и профессиональных связей.

- Ok («Одноклассники») профили сотрудников старшего возраста (информация о карьерном росте; связи между сотрудниками разных отделов.

- Telegram-каналы (корпоративные каналы российских компаний; каналы уволенных сотрудников; чат-боты с API доступа к внутренним системам; специализированные каналы по информационной безопасности).

5. Государственные и реестровые ресурсы:

- ФНС ЕГРЮЛ/ЕГРИП (получение официальных данных о компании; учредители и аффилированные лица; адреса регистрации и фактического расположения);

- Роскомнадзор - реестр (информация о блокировках ресурсов; данные о нарушениях в области персональных данных);

- ГосЗакупки (технические задания на поставку ПО и оборудования; контакты ответственных исполнителей; бюджеты на информационную безопасность).

6. Отраслевые и специализированные платформы с публикациями о внедрениях ИТ-систем, рейтингах поставщиков ИБ-услуг, кейсах интеграции защищенных решений (финансовая отчетность компаний RBC.ru и Kommersant.ru, форум MSK-IX с обсуждением сетевой инфраструктур и техническими проблемами операторов связи).

7. Дополнительные источники:

- Российские SSL-сертификаты (данные о доменах; выявление поддоменов государственных организаций); метаданные документов

(шаблоны именования в государственных учреждениях; авторство документов в Microsoft Office; версии ПО в организациях) и архивы Рунета (Wayback Machine).

Особое внимание следует уделять анализу профессиональных связей в VKontakte и мониторингу специализированных Telegram-каналов, где часто происходит обсуждение внутренних рабочих вопросов и технических проблем организаций. Все описанные методы работают исключительно с публично доступной информацией. При проведении оперативных мероприятий необходимо строгое соблюдение законодательства, получение соответствующих санкций и работа в правовом поле.

Выводы: футпринтинг - основа для планирования дальнейших оперативных мероприятий. Системный подход обеспечивает полноту разведданных, а непрерывность процесса позволяет отслеживать изменения в инфраструктуре. Соблюдение законности – обязательное условие при работе с этими методами.

Сравнение методологий детектирования киберугроз в ЕС, КНР и России с учетом современных подходов представлена в табл. 2.4

Таблица 2.4

Сравнительная таблица детектирования киберугроз

Страна	Методология детектирования	Особенности	Акценты и стандарты
ЕС	Применение AI/ML для выявления аномалий в трафике	Использование искусственного интеллекта и машинного обучения для пассивного мониторинга сетевого трафика и выявления аномалий поведения.	Соответствие eIDAS, акцент на пассивном мониторинге
КНР	Проактивные системы глубокой инспекции пакетов (DPI)	Инспекция глубоких сетевых пакетов в реальном времени с использованием системы Golden Shield Project для активного выявления угроз.	Проактивный контроль, контроль доступа и фильтрация
РФ	Внедрение средств обнаружения и коррекции (сертифицирован ФСТЭК)	Использование сертифицированных систем для обнаружения сложных угроз, включая продвинутые угрозы (APT).	Обязательная сертификация ФСТЭК, фокус на APT

Эта сравнительная таблица отражает разные подходы: ЕС ориентируется на интеллектуальные методы обнаружения с низким вмешательством, КНР - на глубокий проактивный анализ данных, Россия - на строго нормативные и сертифицированные методы с целью защиты от сложных целевых атак.

Процесс анализа угроз в контексте воздействия на защищаемую информацию позволяет более точно оценить риски и выбрать адекватные меры защиты. Рассмотрим его с учетом характера воздействия на данные (см. рис 2.1).

На этапе сбора данных выбираются подходящие источники (отмечены ранее), выявляются вредоносные действия и возможные утечки. Далее следует консолидация данных, которая выражается в обработке и интеграции данных, что позволяет выделить паттерны[72] и общие признаки атак. После консолидации формулируются предположения о злоумышленниках и способах атаки на систему. Сопоставление с MITRE ATT&CK дает понимание характера атаки (анализ тактик и техник). Следующий шаг - различение рисков по уровням (низкий -высокий), что определяет принятие соответствующих решений по минимизацию ущерба и восстановлению целостности системы.



Рис. 2.1. Схема сбора данных в процессе классификации угроз

Данная схема иллюстрирует важность структурированного подхода к сбору и анализу данных о киберугрозах. Каждый этап играет критическую роль в понимании угроз и необходимости реагирования на них.

[72] Под «паттерном» понимается такая комбинация определённых, с точностью до погрешности, значений некоторого подмножества признаков, что объекты с этими значениями достаточно сильно отличаются от других объектов (источник: Алескеров Ф.Т. Анализ паттернов в статике и динамике, часть 1: обзор литературы и уточнение понятия // Бизнес-информатика. 2013. № 3 (25). URL: https://cyberleninka.ru)

2.4. Угроза ИБ по аспекту защищаемой информации

Для эффективного управления рисками необходимо понимать, какие аспекты защищаемой информации подвержены рискам, и какие меры могут быть реализованы. В основе - классическая и наиболее фундаментальная модель триады информационной безопасности, модифицируемая под национальные регуляторные требования и фокусирующаяся на свойствах информации, которые необходимо защищать.

Угрозы конфиденциальности направлены на несанкционированное получение информации. Эти угрозы часто связаны с действиями злоумышленников, стремящихся вскрыть защищенные данные.

Примеры: перехват данных (несанкционированный доступ во время передачи), фишинг (методы обмана пользователей с целью получения их личных данных), кража учетных данных (различные методы для получения доступа), утечки через инсайдеров, когда сотрудники компании целенаправленно или случайно раскрывают конфиденциальную информацию.

Меры защиты: шифрование, системы DLP, строгая аутентификация.

Многие операционные системы и программы, такие как VeraCrypt или BitLocker, позволяют пользователям шифровать файлы и целые тома дисков. Пользователь может создать зашифрованный контейнер, куда помещается конфиденциальные данные и даже когда злоумышленник получит доступ к этому контейнеру, он не сможет воспользоваться информацией без ключа.

Угрозы целостности касаются несанкционированного изменения или разрушение информации, что может негативно сказаться на точности и полноте данных.

Примеры: изменение данных в БД, внедрение вредоносного кода, подмена сайта[73].

Меры защиты: контрольные суммы (методы проверок), электронная подпись (ЭП), системы контроля версий, строгое разграничение прав т.е. доступ обеспечивается только тем пользователям, которым он действительно необходим.

Угрозы доступности: направлены на создание условий, при которых доступ к информации или ресурсам становится невозможным или затрудненным.

Примеры: DDoS-атаки, криптолокеры (Ransomware), уничтожение оборудования.

Меры защиты: резервирование, балансировка нагрузки (распределение трафика между несколькими серверами), планы восстановления (разработка стратегий на случай возникновения инцидента), Anti-DDoS.

[73] Фарминг (от англ. pharming) - разновидность кибератаки, при которой трафик пользователей, направляющихся на легитимный веб-сайт, перенаправляется на поддельный ресурс очень похожий на исходный.

2.5. Угроза ИБ по объекту воздействия

Этот принцип позволяет точно определить цель атаки и спроектировать точечные меры защиты для каждого компонента информационной системы. Таксономия критически важна для реализации принципа *security by design/SbD* (SbD – подход к разработке программного обеспечения, при котором безопасность закладывается в продукт на этапе замысла, а не добавляется постфактум) и сегментации защищаемой инфраструктуры. По объекту воздействия выделяют пять объектов: данные, программное обеспечение, аппаратные средства, каналы связи и персонал.

Данные (защита на физическом уровне Data Loss Prevention).

Угрозы: кража, модификация, уничтожение (повреждение).

Меры: шифрование, резервное копирование, классификация данных.

Программное обеспечение (контроль целостности и верификация кода).

Угрозы: внедрение бэкдоров, логических бомб, эксплуатация уязвимостей.

Меры: регулярное обновление (патчинг), антивирусное ПО, сканирование на уязвимости, Application Control (метод обеспечения безопасности, который регулирует выполнение программных приложений на компьютере или в сети. Он предполагает определение и соблюдение политик, которые определяют, можно ли запускать приложения и как они должны работать) [52].

Аппаратные средства (физическая защита и защита от атак по сторонним или побочным каналам).

Угрозы: кража, физическое повреждение, перехват электромагнитного излучения (TEMPEST).

Меры: физическая охрана, видеонаблюдение, биометрический контроль доступа.

Каналы связи (противодействие DDoS и перехвату трафика).

Угрозы: перехват трафика, подмена сетевых маршрутов (BGP hijacking[74]), создание помех.

Меры: использование VPN, защищенных протоколов (HTTPS, TLS), мониторинг сетевой активности.

Персонал (управление человеческим фактором через программы обучения и информирования сотрудников организации о различных аспектах информационной безопасности, угрозах и методах их предотвращения) [56].

Угрозы: социальная инженерия, вербовка, шантаж, профессиональное выгорание.

Меры: регулярное обучение ИБ, проверка сотрудников, создание позитивного психологического климата.

---

[74] BGP hijacking с помощью добавления AS жертвы в AS-SET атакующего https://habr.com/ru/articles/442784/

Вывод. Классификация по CIA-триаде остается смысловым ядром для формулирования требований к защите. Ни одна классификация не является универсальной. Эффективная защита строится на синтезе нескольких принципов. Например, угроза может быть классифицирована как «Внешняя, преднамеренная, активная, направленная на доступность каналов связи» (DDoS-атака). Классификация по объекту воздействия наиболее тесно связана с практической реализацией технических мер контроля.

Тенденции:

Стирание границ между внешними и внутренними угрозами из-за компрометации легальных учетных записей через фишинг.

*Рост комплексных угроз***,** которые одновременно атакуют несколько аспектов CIA и несколько объектов (например, Ransomware, который нарушает конфиденциальность и доступность данных, а также целостность ПО).

*Смещение фокуса на угрозы цепочки поставок***,** где объектом воздействия становится не только конечное ПО, но и процесс его разработки и обновления.

Практические рекомендации.

Методологические меры:

– Использование многоуровневой классификации при проведении оценки рисков и моделировании угроз.

– Формализование процесса классификации инцидентов ИБ в рамках SOC (Security Operations Center).

Технологические меры:

– настройка SIEM-систем на корреляцию событий с учетом различных классификационных признаков (например, «внутренняя активность + попытка доступа к конфиденциальным данным»).

– Внедрение решений, обеспечивающих защиту across the board - для данных, приложений и инфраструктуры одновременно (например, Zero-Trust Architecture).

Организационные меры:

– внедрение системы категорирования инцидентов ИБ в соответствии с ГОСТ;

– внедрение регулярных тренировок по реагированию на инциденты, используя реалистичные сценарии, сочетающие разные типы угроз;

– разработка политик безопасности, структурированные по объектам защиты (политика обработки ПДн, политика использования программного обеспечения и т.д.).

Такой сравнительный анализ отражает централизованные и масштабные меры Китая, строгие нормативные требования Европейского союза с акцентом на защиту персональных данных, а также комплексную систему России с опорой на криптографию и собственные компоненты информационной безопасности [13].

Сравнительная таблица подходов к защите объектов информации в ЕС, Китае и России приведена в табл. 2.5.

Таблица 2.5

Сравнение подходов к защите объектов информации

Регион	Основной подход к защите	Особенности	Стандарты и нормативы
ЕС	Акцент на защиту данных и программных интерфейсов	Жёсткое регулирование по защите персональных данных (GDPR). Внимание к безопасности API, в частности финансовых (PSD2[75]).	GDPR (General Data Protection Regulation), PSD2
КНР	Тотальный контроль каналов связи и аппаратных компонентов	Централизованный контроль всех каналов связи, глубокий контроль аппаратного обеспечения.	Стандарты GB/T 20234, мониторинг и контроль информации
РФ	Комплексный подход с фокусом на криптографической защите и отечественной компонентной базе	Использование сертифицированных средств криптографической защиты информации (СКЗИ), а также развитие и поддержка отечественных электронных компонент.	Сертификация ФСТЭК, ГОСТы по криптографии, ЭКБ

Регуляторные тренды:

ЕС: Унификация таксономий через EU Cybersecurity Act и стандартизацию ENISA.

КНР: Разработка автономных классификаций в рамках стандартов GB/T.

РФ: Адаптация MITRE ATT&CK к требованиям ФСТЭК и создание отраслевых таксономий.

Примеры инцидентов (2024-2025).

Основными целями атак в 2024-2025 гг. были телекоммуникации, ИТ и финансовый сектор, а количество кибератак в III квартале 2025[76] года выросло на 73% по сравнению с аналогичным периодом 2024 года. Распространёнными векторами стали фишинг и загрузка вредоносных программ. Это показывает, как угрозы каналам связи (DDoS), ПО (вредоносные программы) и персоналу (фишинг) приводят к атакам на данные и системы.

Киберугрозы, связанные с Китаем, часто относятся к категории APT (Advanced Persistent Threat). Это долгосрочные, целенаправленные атаки, сочетающие взлом ПО, кражу данных и социальную инженерию. Объектами таких атак становятся государственные и промышленные секторы по всему миру.

[75] Директива о платёжных услугах (PSD2).

[76] Угрозы и тактики атак, нацеленных на российские компании в 2024–2025 годахhttps://www.itsec.ru/news/ugrozi-i-taktiki-atak-nazaelennih-na-rossiyskiye-kompanii-v-2024-2025-godah

В 2025 года в Европе[77] обсуждался новый тренд атаки с помощью беспилотников (БПЛА) на физическую инфраструктуру. Это яркий пример угрозы аппаратным средствам и объектам критической информационной инфраструктуры (КИИ), когда дрон может повредить серверную или центр связи.

Перспективные исследования:

– разработка квантово-устойчивых таксономий для постквантовой криптографии;

– создание онтологий угроз для интернета вещей (IoT) с учетом национальных особенностей [12].

Таким образом, современные подходы к классификации угроз ИБ отражают технологическую суверенизацию и формирование автономных киберпространств, что требует от специалистов мультиюрисдикционной компетенции и владения сравнительным анализом регуляторных требований.

Глоссарий:

APT (Advanced Persistent Threat) - целенаправленная, долгосрочная и сложная кибератака, часто проводимая высококвалифицированной группой с серьезными ресурсами (например, государственными).

CIA-триада - фундаментальная модель информационной безопасности, основанная на трех принципах: Конфиденциальность (Confidentiality), Целостность (Integrity) и Доступность (Availability).

DLP (Data Loss Prevention) - технологии и процессы, предназначенные для предотвращения утечки конфиденциальных данных за пределы корпоративной сети.

DDoS-атака (Distributed Denial of Service) - атака на отказ в обслуживании, когда на целевой ресурс направляется огромный объем мусорного трафика с множества устройств, чтобы сделать его недоступным.

ENISA (European Union Agency for Cybersecurity) - Агентство Европейского союза по кибербезопасности, занимающееся разработкой политик, рекомендаций и таксономий для стран ЕС.

GB/T (Guobiao) - национальные стандарты Китайской Народной Республики. В сфере ИБ регулируют требования к безопасности продуктов и систем.

General Data Protection Regulation (GDPR) - регламент по защите персональных данных (принят Евросоюзом с 25 мая 2018 г.). Действие документа распространяется на все компании, которые работают с персональными данными граждан ЕС.

[77] Защита объектов от воздействий атак БПЛАhttps://www.secuteck.ru/blog/zashchita-obektov-ot-vozdejstvij-atak-bpla

IDS/IPS (Intrusion Detection/Prevention System) - Системы обнаружения и предотвращения вторжений. IDS мониторит сеть и оповещает о подозрительной активности, IPS может активно блокировать атаки.

NIS2 (Network and Information Security Directive) - директива устанавливает единую правовую базу для обеспечения кибербезопасности в 18 важнейших отраслях по всему ЕС.

MITRE ATT&CK® - глобально доступная база знаний о тактиках и методах, используемых злоумышленниками на разных этапах кибератаки.

Security by Design (SbD) - подход, при котором требования безопасности закладываются в систему, продукт или процесс на этапе проектирования, а не добавляются постфактум.

SIEM (Security Information and Event Management) - система для централизованного сбора, анализа и корреляции событий безопасности из различных источников в режиме реального времени.

Zero Trust Architecture (ZTA) - концепция безопасности, основанная на принципе «никому не доверяй, проверяй всегда», предполагающая постоянную проверку легитимности любого доступа к ресурсам.

Актив (объект воздействия) - любой ценный ресурс организации, требующий защиты (данные, ПО, оборудование, люди).

Бэкдор (Backdoor) - скрытый способ обхода стандартных процедур аутентификации или шифрования для получения несанкционированного доступа к системе или данным.

ГОСТ Р / ISO/IEC 27001 - международный и принятый в РФ стандарт, описывающий требования к системе менеджмента информационной безопасности (СМИБ).

Данные - информация в любой форме (электронная, физическая), которая является конечной целью атаки.

Инцидент информационной безопасности - уже произошедшее событие, в результате которого была реализована угроза и нарушена безопасность информации.

Криптография - наука о методах обеспечения конфиденциальности, целостности и аутентичности информации путем ее преобразования с использованием секретных ключей.

Оценка рисков - систематический процесс выявления активов, угроз и уязвимостей, а также анализа вероятности и последствий инцидентов для определения приоритетов защиты.

Полиморфизм (в киберугрозах) - техника, при которой вредоносное ПО меняет свой код при каждом новом заражении, чтобы избежать обнаружения. Используется вирусами, червями, троянами (например, Emotet).

Социальная инженерия - метод манипуляции людьми для получения конфиденциальной информации или совершения определенных действий (например, фишинг).

Таксономия (в ИБ) - структурированная иерархическая система для классификации терминов и понятий (например, угроз), обеспечивающая единообразие и системность их использования.

Уязвимость - слабость в активе, системе, процедуре или контроле, которую может использовать угроза

Угроза безопасности информации - потенциальная возможность события, которое, используя уязвимость актива, может нарушить его конфиденциальность, целостность или доступность и причинить ущерб.

Футпринтинг (Footprinting) - начальный этап разведки, проводимой злоумышленником, заключающийся в сборе максимального объема открытой информации о цели (организации, сети, человеке).

ФСТЭК России (Федеральная служба по техническому и экспортному контролю) - ключевой регулятор в области информационной безопасности РФ, разрабатывающий требования и осуществляющий сертификацию средств защиты информации (например, для КИИ).

Вопросы и задания для самоконтроля:

1. Дайте определение таксономии угроз информационной безопасности. Какие основные задачи решает процесс классификации угроз?
2. Назовите и охарактеризуйте четыре ключевых принципа классификации угроз, рассмотренных в главе.
3. Объясните, почему ни одна классификация не является универсальной, и эффективная защита требует синтеза нескольких принципов. Приведите пример комплексной угрозы, описываемой через несколько классификационных признаков.
4. В чем заключаются ключевые различия между внешними, внутренними и природными угрозами с точки зрения уровня контроля, мотивов и фокуса защиты?
5. Чем инсайдер-злоумышленник принципиально отличается от внешнего нарушителя и почему он считается более опасным?
6. Сравните нормативные подходы к атрибуции источников угроз в ЕС, КНР и РФ. Какой тип угроз является приоритетным для каждого региона и почему?
7. Раскройте содержание разделения «преднамеренные/случайные» и «активные/пассивные» угрозы. Приведите по два практических примера для каждой категории.
8. Сравните методологии детектирования угроз в ЕС, КНР и России. Как различия в подходах (AI/ML в ЕС, DPI в КНР) отражают их регуляторные приоритеты?
10. Дайте определение каждому компоненту CIA-триады. Какие меры защиты соответствуют угрозам конфиденциальности, целостности и доступности?

11. Используя карту приоритетности, объясните, почему для базы персональных данных конфиденциальность является максимальным приоритетом, а для SCADA-системы АЭС – целостность и доступность.

12. Чем обусловлен акцент ЕС на конфиденциальности, КНР – на целостности, а РФ – на балансе доступности и целостности?

13. Перечислите основные объекты воздействия угроз в информационной системе. Для каждого объекта назовите по одной типичной угрозе и соответствующей мере защиты.

14. Как принцип классификации по объекту воздействия связан с практической реализацией мер безопасности и подходом Security by Design (SbD)?

15. Сравните фокус защиты в ЕС, КНР и РФ, исходя из объекта воздействия. Почему в ЕС акцент на данных и ПО, в КНР – на каналах связи и аппаратуре, а в РФ – на криптографии и отечественной компонентной базе?

16. Дайте определение футпринтинга. Почему для правоохранительных органов этот процесс аналогичен сбору оперативных данных?

17. Каковы практические аспекты работы с DNS для оперативного сотрудника? Что такое Zone Transfer и почему его редко удается выполнить?

18. Составьте краткий перечень наиболее релевантных российских интернет-ресурсов для проведения футпринтинга, разделив их на категории (профессиональные сети, ресурсы с утечками, госреестры и т.д.).

19. В чем заключается юридический аспект проведения футпринтинга сотрудниками МВД? Какие нормативные документы и принципы необходимо соблюдать?

21. Назовите три ключевых тенденции в развитии киберугроз, отмеченные в главе (например, стирание границ между угрозами, рост комплексных атак).

22. Какие практические рекомендации по внедрению рассмотренных классификаций даны в параграфе? (методологические, технологические, организационные меры).

23. Какие перспективные направления исследований в области таксономий угроз указаны в заключении (например, разработка квантово-устойчивых таксономий)?

24. Сформулируйте основной вывод главы. Как современные геополитические реалии (фрагментация киберпространства, технологическая суверенизация) влияют на подходы к классификации угроз ИБ?

ГЛАВА 3. УНИВЕРСАЛЬНЫЕ И ОТРАСЛЕВЫЕ ТАКСОНОМИИ УГРОЗ: ОБЗОР И СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ КЛАССИФИКАЦИИ

3.1. Введение в таксономии угроз

Современная парадигма информационной безопасности характеризуется фундаментальным сдвигом в количественных показателях киберугроз – от единичных инцидентов к массовым кампаниям. Воспользовавшись интерактивной картой киберугроз в режиме реального времени от «Лаборатории Касперского», можно увидеть, что происходит в сфере кибербезопасности по всему миру. Так, например, по метрике «Топ - сканирование при доступе за последнюю неделю» показатели в виде графика на рисунке 3:

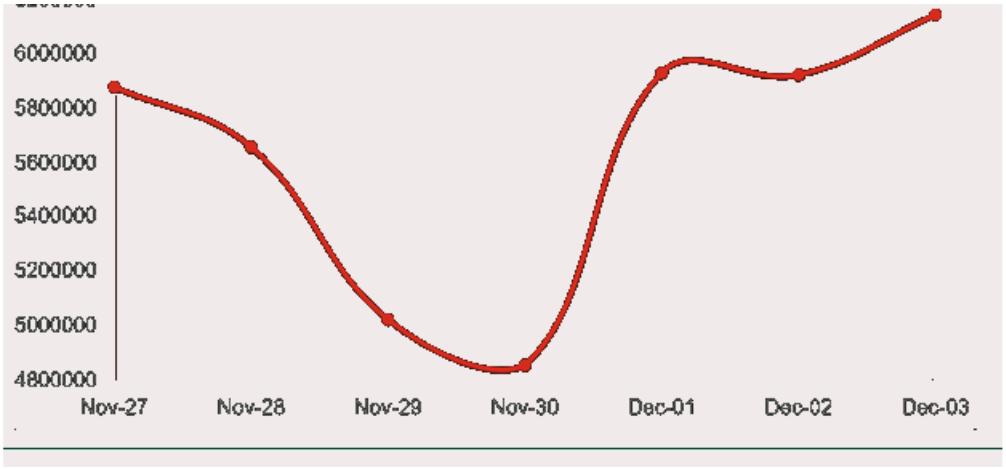


Рис.3 Аналитический виджет сайт https://cybermap.kaspersky.com

Указанная метрика «сканирование при доступе за последнюю неделю» показывает статистику по работе встроенного антивирусного сканирования при доступе (in-access). Динамика данных позволяет оценить эффективность работы антивируса и помогает выявлять тенденции. Можно заметить, что количество зафиксированных подключений за неделю варьируется в диапазоне от 4 800 000 до 6 000 000, что свидетельствует о высокой активности антивирусной системы.

Ключевым драйвером нарастающей трансформации стала тотальная автоматизация атак. Злоумышленники активно используют ботов, скрипты и целые платформы по модели MaaS (Malware-as-a-Service), что позволяет осуществлять координацию миллионов атак одновременно по всему миру. Параллельно процессы цифровой трансформации лавинообразно расширяют поверхность атаки: каждый новый IoT-девайс, облачный сервис или учетная запись создает дополнительный вектор для потенциального компрометирования информационных активов [53].

Одновременно с количественным ростом наблюдается экспоненциальное усложнение киберугроз, прошедших эволюцию от кибервандализма до инструмента геополитического влияния. Мотивация акторов информационной безопасности претерпела радикальную трансформацию: от одиночек-хакеров через организованную киберпреступность с финансовыми целями к высокопрофессиональным APT-группам, осуществляющим кибершпионаж, и далее – к государственным операциям в киберпространстве, нацеленным на критическую информационную инфраструктуру. Техническое совершенство атак достигло беспрецедентного уровня: многоступенчатые цепочки компрометации, сочетающие методы социальной инженерии, включая таргетированный фишинг, с механизмами обеспечения «живучести» в системе по принципу «постоянной серьезной угрозы», когда скрытая группа злоумышленников получает несанкционированный доступ к компьютерной сети и может оставаться незамеченной длительное время, и продвинутыми техниками обфускации под легитимную активность.

Прямым следствием этой двойной экспоненты – роста количества и сложности – стала ситуация информационной перегрузки для специалистов по информационной безопасности. Центры мониторинга информационной безопасности (SOC) и аналитики киберугроз ежедневно сталкиваются с тысячами оповещений от систем защиты, где проблема соотношения «сигнал/шум» приобретает критический характер: среди миллионов регистрируемых событий безопасности необходимо идентифицировать лишь десятки реальных инцидентов информационной безопасности. В этих условиях традиционный подход реагирования на угрозы по отдельности, аналогичный «тушению пожаров», демонстрирует свою полную несостоятельность. Современные вызовы информационной безопасности требуют системного подхода, фундаментом которого является научно обоснованная классификация и таксономия киберугроз [54].

В противовес хаосу современного киберпространства, таксономия угроз информационной безопасности представляет собой не произвольный перечень, а строгую, иерархическую и структурированную систему классификации, где каждый элемент имеет логичное место и установленные взаимосвязи с другими. Эта система строится на фундаменте ключевых осей классификации, которые позволяют всесторонне описать и категоризировать любую киберугрозу.

Ключевыми «китами» любой эффективной таксономии являются, во-первых, тактики, техники и процедуры (TTPs), отвечающие на вопрос «КАК проводится атака?». Эта ось описывает модель поведения злоумышленника, например, использование фишинга, подбора учетных данных или эксплуатацию уязвимости нулевого дня. Золотым стандартом для классификации TTPs является фреймворк MITRE ATT&CK, который стал универсальным языком для специалистов по кибербезопасности. Во-вторых, это цель воздействия (Impact), которая определяет, на какую часть триады CIA

– конфиденциальность, целостность или доступность данных и систем – направлена атака. Третья критически важная ось – «актор», отвечающий на вопрос «КТО стоит за атакой?»; это позволяет разграничивать угрозы от внутренних нарушителей, хактивистов, киберпреступных группировок или государственных структур. Четвертый элемент – «вектор атаки», который идентифицирует точку входа, например, электронную почту, уязвимость в приложении или съемный носитель. И наконец, ось «ресурс» определяет, на какой именно информационный актив направлена угроза: сервер, рабочая станция, база данных или сетевое оборудование.

Для наглядного закрепления таксономию угроз информационной безопасности можно сравнить с биологическим определителем. К примеру, злоумышленник использовал вредоносное программное обеспечение (*Царство*), которое реализует криптографическое шифрование файлов (*Тип*), распространяется через целевую рассылку фишинговых писем (*Класс*) и сопровождается требованием выкупа за дешифрацию (*Отряд*). В результате, применяя систематизированный подход, мы точно идентифицируем угрозу как *ransomware* (*Вид*). Таким образом, таксономия преобразует разрозненные данные о киберинциденте в структурированное знание, пригодное для анализа и принятия решений в области информационной безопасности.

Практическая ценность таксономии угроз информационной безопасности раскрывается в ее способности трансформировать разрозненные данные в стратегические знания, обеспечивая единый понятийный аппарат и строгую методологию идентификации и каталогизации киберинцидентов. Ключевым преимуществом является преодоление терминологической разрозненности между различными подразделениями: когда аналитик SOC оперирует понятием «APT-атака», а менеджер по рискам интерпретирует это как обычный «вирус», возникает критический разрыв в восприятии угрозы. Таксономия создает унифицированный словарь, позволяющий техническим специалистам, руководителям, юристам и аналитикам говорить на одном языке, используя стандартизированные наименования групп угроз (например, Lazarus Group или FIN7) вместо субъективных и размытых описаний [72].

Методологическая составляющая таксономии реализуется через систематизацию знаний о киберугрозах, когда вместо хаотичных заметок формируется структурированный каталог инцидентов информационной безопасности, актуальных для конкретной организации. Это позволяет перейти от реактивной к проактивной защите: зная, что определенная группа угроз использует технику T1134 по таксономии MITRE ATT&CK (смена токена доступа), специалисты по безопасности могут заблаговременно настроить правила корреляции и детектирования аномалий, связанных именно с этой тактикой. В процессе расследования киберинцидентов таксономия значительно ускоряет анализ, позволяя специалисту быстро идентифицировать атаку по ключевым признакам, восстановить ее полный жизненный цикл и эффективно локализовать последствия.

Важнейшим аспектом является возможность обоснованной приоритизации рисков информационной безопасности и оптимального распределения ресурсов. Таксономия дает четкий ответ на вопрос «Что важнее?», позволяя сравнивать атаки по комплексным критериям. Например, целенаправленная кампания по хищению финансовых данных с высоким потенциалом воздействия, исходящая от государственной APT-группы, закономерно получает приоритет над фоновым сканированием портов автоматизированным скриптом. Более того, таксономия предоставляет веские аргументы для инвестиционных решений в область безопасности, позволяя обосновать необходимость финансирования конкретных контрмер статистическими данными: «Мы направляем ресурсы на совершенствование защиты от фишинга, поскольку таксономический анализ показывает, что 60% успешных компрометаций в нашей среде инициируются через этот вектор». Таким образом, таксономия угроз становится не просто инструментом классификации, а краеугольным камнем стратегического управления рисками информационной безопасности.

Ключевые функции таксономий:

- унификация терминологии для специалистов ИБ, разработчиков и регуляторов;
- стандартизация процессов оценки рисков и управления инцидентами;
- сравнительный анализ эффективности контрмер в различных организациях;
- прогнозирование развития угроз и планирование мер защиты.

Национальные особенности таксономий приведены в табл. 3.1.

Таблица 3.1.

Национальные особенности таксономий Россия, ЕС, Китай

Страна	Характер таксономий	Основной акцент
Россия	Таксономии носят обязательный нормативный характер для государственных информационных систем и объектов КИИ	Защита государственных интересов и выполнение регуляторных требований
Европейский союз	Преобладает рамочный подход с ориентацией на операционную безопасность бизнеса	Инструмент гармонизации требований в рамках единого цифрового рынка
Китай	Таксономии интегрированы в систему государственного управления и контроля киберпространства	Обеспечение социальной стабильности и национальной безопасности

Эта таблица отражает различия в нормативных и операционных подходах к таксономиям угроз и требований в разных юрисдикциях.

3.2. Универсальные таксономии угроз информационной безопасности

А) MITRE ATT&CK Framework.

Разработан компанией MITRE на основе анализа реальных кибератак. Представляет собой базу знаний о тактиках, техниках и процедурах (TTPs), используемых злоумышленниками.

Структура матрицы:

- тактики – цели злоумышленника на различных этапах атаки;
- техники – способы достижения тактических целей;
- процедуры – конкретные реализации техник.

Преимущества:

- постоянное обновление на основе реальных инцидентов;
- детализированное описание техник с примерами;
- широкая адаптация в инструментах безопасности.

Ограничения:

- сложность первоначального освоения;
- требует значительных ресурсов для полноценного внедрения.

Б) Таксономия ENISA разрабатывается Агентством Европейского союза по кибербезопасности (ENISA) как часть общеевропейской стратегии кибербезопасности.

Ключевые особенности:

- классификация по источникам угроз и уязвимостям;
- фокус на операционных рисках;
- интеграция с требованиями NIS2 Directive.

Структурные элементы:

- угрозы-акторы (Threat Agents);
- векторы атак (Attack Vectors);
- воздействия (Impacts).

В) Национальная таксономия угроз Российской Федерации.

Разрабатывается в рамках регуляторной модели экосистемы ФСТЭК России и ФСБ России. Это не единый открытый фреймворк, а совокупность взаимосвязанных методик и требований, закрепленных в нормативных документах [35].

Ключевые особенности:

- обязательность (таксономия не является рекомендательной, а служит основой для выполнения требований законов, например, 152-ФЗ, 187-ФЗ);
- процессуальный подход (акцент сделан на каталогизацию всех возможных тактик, а на методологию моделирования угроз);
- модель ориентирована на государственные системы и ресурсы (ГИС, персональные данные граждан) и оценка угроз определяется с точки зрения ущерба.

Структурные элементы:

- источники угрозы (внутренние/внешние);
- способы реализации (уязвимости и методы, которые нарушитель может использовать против выявленных активов);
- актуальность угроз (оценка вероятности реализации угрозы для конкретной системы с учетом введенных мер защиты).

Пример из практики. Атака на информационную систему муниципальной поликлиники будет анализироваться по следующему алгоритму: объект воздействия (база данных персональных данных пациентов и медицинских работников) → источник угрозы (внешний нарушитель) → способы реализации (использование уязвимости в веб-интерфейсе) → оценка актуальности (определяется существует ли данная уязвимость в системе) → классификация по ущербу (нарушение конфиденциальности персональных данных[78]).

Г) Национальная таксономия угроз Китайской народной республики

Разрабатывается в рамках политики киберсуверенитета и регулируется администрацией киберпространства Китая (CAC). Таксономия тесно интегрирована с системой национальных стандартов GB/T и концепцитей «сетевой безопасности».

Ключевые особенности:

- обязательность государственный приоритет (таксономия рассматривает киберугрозы через призму национальной безопасности и социальной стабильности);
- контроль над информацией (наряду с техническими киберугрозами, значительная часть таксономии посвящена угрозам распространения информации, что отражено в работе системы «Золотой Щит»[79]);
- ориентация на цепочки поставок (жесткие требования к безопасности и проверке ИТ-продуктов, особенно иностранных, продвижение собственных программных продуктов) [40].

Структурные элементы:

- угрозы национальной безопасности (шпионаж, подрыв государственной сласти);
- угрозы социальной стабильности (распространение ложных слухов, нарушение общественного порядка);
- технические киберугрозы (традиционные атаки, классифицируемые по отраслевым стандартам GB/T);
- угрозы с сфере данных (несанкционированный трансграничный поток «важных данных», хищение персональных данных граждан).

[78] Методика оценки угроз безопасности информации: обзор методического документа ФСТЭК России https://safe-surf.ru/specialists/article/5289/666972/

[79] Цифровой суверенитет по-китайски: как работает самая масштабная система контроля интернета в мире: https://www.securitylab.ru/blog/personal/paragraph/355350.php

3.3. Отраслевые таксономии и стандарты информационной безопасности

В глобальной практике построения систем менеджмента информационной безопасности (СМИБ) сформировались национальные и отраслевые таксономии, отражающие различные регуляторные подходы. Данные фреймворки служат структурированной основой для классификации угроз, управления рисками, выбора и имплементации контрмер, варьируясь от гибких риск-ориентированных моделей до жестких предписывающих стандартов.

А) BSI Grundschutz (Германия).

Методологическую основу составляет набор стандартов Федерального ведомства по информационной безопасности Германии (BSI). Это комплексный (holistic) подход, предоставляющий организациям любого масштаба детализированные инструкции для построения СМИБ. Его ядро включает:

- каталог угроз (Threat Catalog), представляющий систематизированное описание актуальных векторов атак;
- каталог мер защиты (Security Measures Catalog) с конкретными практическими рекомендациями;
- стандартизированную методику оценки рисков.

Ключевые особенности: универсальность, глубокая детализация рекомендаций, обеспечивающая воспроизводимость результатов, и регулярный цикл обновления для адаптации к новым технологическим и угрозным ландшафтам. Подход BSI Grundschutz служит основой для сертификации систем защиты, что особенно востребовано государственным сектором и операторами критической инфраструктуры.

Б) NIST Cybersecurity Framework (США).

Данный фреймворк (CSF) предлагает высокоуровневую, гибкую и добровольную структуру для управления киберрисками. Его ядро организовано вокруг пяти основных функций, образующих непрерывный цикл:

- Identify (Идентификация) – каталогизация активов и оценка рисков;
- Protect (Защита) – внедрение превентивных контрмер;
- Detect (Обнаружение) – реализация возможностей мониторинга и выявления инцидентов;
- Respond (Реагирование) – действия по устранению последствий компрометации;
- Recover (Восстановление) – возврат к нормальному функционированию.

Область применения фреймворка крайне широка: от операторов критической информационной инфраструктуры (КИИ) и государственных агентств до компаний частного сектора, стремящихся повысить свою

киберустойчивость (cyber resilience). Его сила – в масштабируемости и возможности интеграции с другими стандартами, такими как NIST SP 800-53.

В) Multi-Level Protection Scheme (MLPS 2.0).

Китайская система MLPS (Dengji Baohu) представляет собой обязательный, предписывающий и иерархический стандарт, закрепленный в Законе о кибербезопасности КНР. Его фундамент – обязательная классификация всех сетевых и информационных систем по пяти уровням важности в зависимости от потенциального ущерба в случае компрометации. Для каждого уровня норматив устанавливает строгий, детализированный набор требований к организационным и техническим мерам защиты. Особенность подхода – глубокое вовлечение государственных органов в процесс аудита, инспекций и выдачи разрешений, что делает безопасность инструментом обеспечения киберсуверенитета и социальной стабильности. Система тесно связана с требованиями локализации данных и безопасности цепочек поставок, а ее соблюдение является обязательным условием для работы на рынке [14].

Г) Требования ФСТЭК/ФСБ России к объектам КИИ.

Российский подход, закрепленный в Федеральном законе № 187-ФЗ «О безопасности критической информационной инфраструктуры», сфокусирован на гарантированной защите строго определенного перечня объектов КИИ. Его методологическую основу составляют предписания регуляторов (ФСТЭК, ФСБ России), носящие детализированный и обязательный характер. Ключевые компоненты включают:

- категорирование объектов КИИ;
- обязательную оценку соответствия (аттестацию) установленным требованиям;
- использование сертифицированных средств защиты информации (СЗИ) отечественного производства;
- соблюдение профильных стандартов (например, серия ГОСТ Р). Особенность подхода в акценте на изоляции и суверенизации критически важных систем, что проявляется в требованиях к импортозамещению и использованию национальных криптографических алгоритмов. Обязательное применение российских криптографических стандартов и алгоритмов обеспечивает надежность и безопасность обработки данных. Это включает как шифрование, так и механизмы аутентификации [17].

Система требований ФСТЭК и ФСБ формирует комплексный подход к обеспечению безопасности объектов КИИ в России. Для выполнения этих требований важно, чтобы организации не только соблюдали установленный регламент, но и активно развивали внутренние процессы управления ИБ, что становится залогом защиты от современных угроз.

Сравнение отраслевых таксономий представлено в табл. 3.2.

Таблица 3.2.

Сравнительная таблица отраслевых таксономий

Критерий	MITRE ATT&CK	ENISA	BSI Grundschutz	NIST CSF
Основной фокус	Тактики атакующих	Классификация угроз	Построение СЗИ	Управление рисками
Структура	Матрица тактик и техник	Иерархическая классификация	Модульные каталоги	Framework из 5 функций
Обновляемость	Постоянно	Ежегодно	Регулярно	Периодически
Применимость	Киберзащита	Регулирование	Сертификация	Добровольное применение
Сильные стороны	Детальность TTPs	Учет европейских требований	Комплексность подхода	Гибкость внедрения

Представленные таксономии демонстрируют спектр подходов: от универсальных риск-ориентированных фреймворков (NIST) и комплексных методик (BSI) до жестких систем государственного регулирования, направленных на обеспечение суверенитета и безопасности критически важных активов (MLPS в Китае, требования к КИИ в России). Выбор или необходимость следования определенной таксономии определяется не только отраслевой принадлежностью организации, но и геополитическим контекстом и регуляторным полем, в котором она функционирует [16].

Сравнительный анализ национальных подходов к структурированию знаний в области информационной безопасности позволяет нам сосредоточиться на регуляторных и методологических таксономиях Российской Федерации, Китайской Народной Республики и Европейского Союза. В отличие от технических фреймворков, эти системы воплощают государственную политику в области киберсуверенитета, управления рисками и обеспечения безопасности критической информационной инфраструктуры (КИИ) [72].

Национальные таксономии в ИБ – это не просто классификации. Это нормативно-правовые конструкции, определяющие модель угроз, приоритеты защиты, зоны ответственности и критерии соответствия. Они формируют ландшафт управления информационными рисками на уровне государства и задают рамки для построения систем менеджмента информационной безопасности (СМИБ) для организаций.

Сравнительная характеристика национальных подходов.

Китай: таксономия как система тотального контроля и технологического суверенитета:

Происхождение и основной фокус: основу составляет Закон КНР о кибербезопасности (2017 г.), который закрепляет принципы киберсуверенитета и безопасности данных. Фокус – на контроле над данными (включая правило локализации) и обеспечении безопасности критически

важных сетей. Ключевым элементом является система Multi-Level Protection Scheme (MLPS 2.0) – детализированная таксономия для классификации информационных систем по уровням важности с предписывающими мерами защиты, обязательная для всех операторов КИИ.

Структура и обновляемость: система иерархична и носит жестко регламентированный, предписывающий характер. Обновления регуляторных актов происходят в рамках реализации государственных стратегий (например, «Пекинская инициатива по контролю над данными»). Акцент делается на самодостаточности технологического стека и контроле над цепочками поставок.

Применимость и сильные стороны: сила модели – в ее всеобъемлющем, обязательном характере и глубокой интеграции с государственным надзором. Она эффективна для централизованного управления рисками на национальном уровне и подавления угроз, связанных с иностранным технологическим влиянием. Слабые стороны могут проявляться в гибкости и адаптации к быстро меняющимся тактикам APT-групп.

Европейский Союз: таксономия как система гармонизированного регулирования и управления рисками

Происхождение и основной фокус: подход ЕС основан на гармонизации законодательства стран-членов. Краеугольные камни: Директива NIS/NIS2 (безопасность сетей и информационных систем), GDPR (защита персональных данных) и Акт о киберустойчивости (CRA). Фокус – на управлении операционными рисками, обеспечении непрерывности бизнеса и защите прав субъектов данных. Акцент делается на докладах об инцидентах и требованиях к отчетности.

Структура и обновляемость: подход рамочный и риск-ориентированный. Он задает цели безопасности (например, в NIS2), но оставляет конкретные методы реализации на усмотрение операторов важнейших услуг (OES). Постоянно развивается за счет введения новых схем сертификации (по схеме EUCC, EUCS). Обновляется через пересмотр директив и регламентов.

Применимость и сильные стороны: сила – в создании единого правового поля, стимулировании обмена информацией об угрозах (TI) и развитии европейского рынка кибербезопасных продуктов. Модель поощряет адаптацию мер защиты под конкретную модель угроз организации, что повышает эффективность. Однако сложность согласования между странами-членами может приводить к фрагментации исполнения.

Российская Федерация: таксономия как система государственного регулирования и обеспечения безопасности КИИ

Происхождение и основной фокус: основа – Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» и Федеральный закон № 152-ФЗ «О персональных данных». Фокус – на обеспечении безопасности объектов КИИ и защите информации, составляющей государственную тайну. Ядро методологии – совокупность

требований и руководящих документов ФСТЭК России, которые формируют детализированную таксономию мер защиты (как организационных, так и технических).

Структура и обновляемость: структура носит предписывающий и детализированный характер, особенно в части защиты гостайны и объектов КИИ (например, Приказ ФСТЭК №239, устанавливающий 16 групп актуальных угроз). Центральную роль играет процедура аттестации (сертификации) объектов КИИ и аттестации средств защиты информации (СЗИ). Обновляется путем выпуска новых приказов и методик регуляторов (ФСТЭК, ФСБ).

Применимость и сильные стороны: сила – в высокой степени формализации и детализации требований, что упрощает процесс проверки (аттестации/контроля) и делает систему прозрачной для поднадзорных организаций. Она эффективна для защиты узко определенного контура (КИИ, госсектор) от широкого спектра угроз. К вызовам можно отнести сложность адаптации к гибким DevOps-процессам и потенциальный разрыв с международными фреймворками управления рисками [71].

Резюмируя относительно стратегических приоритетов, закодированных в таксономиях, можно выделить *три парадигмы*.

Китай: парадигма суверенного контроля. Таксономия служит инструментом технологической автаркии и всеобъемлющего государственного надзора за цифровым пространством. Безопасность неотделима от суверенитета и контроля над данными.

Европейский Союз: парадигма гармонизированного управления рисками. Таксономия нацелена на создание устойчивого единого цифрового рынка через согласованные правила, обмен TI и защиту фундаментальных прав (конфиденциальность). Акцент на отчетности и непрерывности бизнеса.

Российская Федерация: парадигма защищенного государственного контура. Таксономия сфокусирована на гарантированной защите строго очерченных критически важных активов (КИИ, гостайна) через детальные предписания и систему аттестации. Это модель «цифровой обороны» ключевых объектов.

Таким образом, сравнительный анализ национальных таксономий в области ИБ демонстрирует, как через технические классификации и регуляторные требования реализуются фундаментальные государственные стратегии: от построения суверенного цифрового пространства до обеспечения устойчивости транснационального рынка.

3.4. Российские таксономические подходы в информационной безопасности

Российские таксономические подходы в области информационной безопасности формируют строго регламентированную систему, обладающую выраженной национальной спецификой. В отличие от многих международных

рамочных стандартов, носящих рекомендательный характер, российская модель основана на принципах обязательности и единообразия применения. Её фундамент составляют методические документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России), которые являются обязательными для исполнения в отношении государственных информационных систем. Дальнейшая детализация реализуется через профильные отраслевые стандарты, разрабатываемые для объектов критической информационной инфраструктуры (КИИ), что обеспечивает учет специфики таких ключевых секторов, как энергетика, здравоохранение, транспорт и связь. Вся эта архитектура выстроена в строгом соответствии с регуляторными требованиями, установленными законодательством о безопасности КИИ [15].

Нормативно-методическая база российских таксономических подходов закреплена в ключевых документах, среди которых центральное место занимают Приказы ФСТЭК России. В частности, Приказ № 239 (от 25 декабря 2017) утверждает «Об утверждении требовании по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», а Приказ № 21 устанавливает «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Важным элементом системы являются ГОСТы серии Р 50000, такие как ГОСТ Р 51275-2006, регламентирующий основы защиты информации, а также многочисленные отраслевые стандарты безопасности, которые конкретизируют общие требования применительно к специфическим технологическим процессам.

Сравнительный анализ позволяет выделить ключевые особенности российского подхода. Во-первых, это жесткая регламентация не только целей, но и конкретных методов защиты, что оставляет минимальное пространство для вариативности при реализации мер безопасности. Во-вторых, принцип обязательности применения для определенных законодательством категорий информационных систем и объектов КИИ, что придает таксономии императивный характер. В-третьих, глубокая интеграция с национальными системами сертификации средств защиты информации и лицензирования деятельности по технической защите конфиденциальной информации, что создает замкнутую систему контроля и надзора. Таким образом, российская таксономическая модель представляет собой централизованную, иерархически выстроенную систему, ориентированную на обеспечение защищенности стратегически важных информационных активов в рамках реализации государственной политики в области кибербезопасности [16].

Национальная специфика:

– методики ФСТЭК России – обязательные к применению в государственных информационных системах;

– отраслевые стандарты – для критической информационной инфраструктуры;

– регуляторные требования – в соответствии с законодательством о КИИ.

Ключевые документы:

– Приказы ФСТЭК России №№ 239, 21;
– ГОСТы серии Р 50000;
– Отраслевые стандарты безопасности.

Сравнительные особенности:

– жесткая регламентация методов защиты;
– обязательность применения для определенных категорий систем;
– интеграция с системами сертификации и лицензирования.

Российская таксономическая модель в области ИБ – это уникальная централизованная система, движимая логикой государственного суверенитета и контроля. Ее сильные стороны – четкость, обязательность и предсказуемость для регулируемых организаций. Однако она требует значительных ресурсов[80] и может ограничивать гибкость и инновации. В условиях цифровой трансформации и импортозамещения система продолжает эволюционировать, интегрируя современные концепции безопасности, но сохраняя свою иерархическую и императивную сущность. Будущее развитие будет скорее связано с поиском баланса между жестким регулированием и необходимостью адаптации к быстро меняющейся среде.

3.5. Практическое применение таксономий угроз информационной безопасности

Практическое применение таксономий угроз информационной безопасности находит свое отражение в конкретных сценариях использования, каждый из которых ориентирован на решение определенных задач в рамках построения комплексной системы защиты. Одним из ключевых сценариев является построение и операционная деятельность центра мониторинга и реагирования на инциденты информационной безопасности. В данном контексте фреймворк MITRE ATT&CK используется в качестве фундаментальной основы для настройки корреляционных правил и механизмов детектирования, позволяя аналитикам SOC идентифицировать не отдельные разрозненные события, а целостные тактики и техники злоумышленников, тем самым повышая эффективность противодействия сложным многоэтапным атакам [18].

Для задач независимой и внутренней оценки защищенности информационных систем идеально подходит методология BSI Grundschutz, которая применяется для проведения комплексного аудита безопасности. Ее структурированные каталоги угроз и контрмер предоставляют аудиторам детализированный чек-лист, обеспечивающий всестороннюю проверку

[80] Россия вошла в топ-10 стран мира по расходам на кибербезопасность https://www.forbes.ru/tekhnologii/532961-rossia-vosla-v-top-10-stran-mira-po-rashodam-na-kiberbezopasnost

соответствия состояния информационной безопасности организации установленным эталонным требованиям.

В условиях ужесточения регуляторного давления особую актуальность приобретает сценарий, направленный на обеспечение соответствия законодательным требованиям. Таксономия, разрабатываемая Агентством Европейского союза по кибербезопасности, служит инструментом для приведения процессов информационной безопасности в соответствие с директивами ЕС, такими как NIS2, выполняя роль связующего звена между операционной деятельностью и ожиданиями регуляторов.

Наконец, для системного подхода к киберрискам внедрение фреймворка NIST Cybersecurity Framework позволяет выстроить цикличный процесс управления рисками информационной безопасности. Фреймворк кибербезопасности NIST CSF представляет собой комплексную модель управления рисками информационной безопасности, структурированную вокруг пяти базовых функций. Функция *Identify* (Идентификация) формирует основу для управления рисками ИБ через каталогизацию информационных активов, оценку уязвимостей программного обеспечения и аппаратных комплексов, а также анализ угроз для бизнес-процессов. В рамках функции *Protect* (Защита) реализуются превентивные меры безопасности, включая внедрение средств контроля доступа, шифрования конфиденциальных данных, обеспечения целостности систем и проведения программ осведомленности в области кибербезопасности.

Функция *Detect* (Обнаружение) ориентирована на непрерывный мониторинг событий информационной безопасности с использованием систем SIEM, анализ сетевого трафика для выявления аномалий и оперативное обнаружение индикаторов компрометации. При активации функции *Respond* (Реагирование) осуществляется выполнение плана реагирования на инциденты ИБ, включая сдерживание распространения вредоносного кода, эрадикацию угроз и сбор цифровых доказательств для последующего криминалистического анализа. Завершающая функция *Recover* (Восстановление) обеспечивает восстановление работоспособности информационных систем после киберинцидента через активацию планов непрерывности бизнеса, восстановление данных из резервных копий и проведение пост-инцидентного анализа для повышения устойчивости ИБ-инфраструктуры.

Данный фреймворк создает цикличный процесс управления рисками информационной безопасности, позволяющий организациям системно выстраивать защиту критически важных активов, минимизировать операционные простои и последовательно совершенствовать свой уровень киберустойчивости.

Выбор оптимальной таксономии или их комбинации является стратегическим решением и должен основываться на ряде ключевых критериев. Первостепенное значение имеет отраслевая принадлежность организации, поскольку объекты критической информационной

инфраструктуры, финансовый сектор и государственные информационные системы часто подпадают под действие специфических стандартов. Другим критически важным фактором являются императивные требования регуляторов, которые в некоторых юрисдикциях могут предписывать использование конкретных фреймворков. Не менее важную роль играет реалистичная оценка доступных ресурсов на внедрение, включая бюджет, персонал и технологическую базу, поскольку сложные таксономии требуют значительных затрат для своей полноценной реализации.

И, наконец, отправной точкой для выбора должен служить текущий уровень зрелости процессов информационной безопасности организации, поскольку попытка внедрения продвинутого фреймворка при низком уровне зрелости не принесет ожидаемого эффекта и создаст дополнительные операционные риски.

Сценарии использования:

1. Построение SOC – использование MITRE ATT&CK для настройки детектов.

2. Аудит безопасности. Например, применение подхода BSI Grundschutz для комплексной проверки.

3. Соответствие требованиям – использование ENISA для выполнения директив ЕС.

4. Управление рисками – внедрение NIST CSF для оценки и обработки рисков.

Критерии выбора таксономии:

- отраслевая принадлежность организации;
- требования регуляторов;
- доступные ресурсы на внедрение;
- уровень зрелости процессов ИБ.

3.6. Перспективы развития таксономий

Современное развитие таксономий угроз информационной безопасности характеризуется рядом выраженных тенденций, обусловленных необходимостью противодействия усложняющимся киберугрозам. Наблюдается устойчивая конвергенция международных стандартов и фреймворков, проявляющаяся в гармонизации подходов MITRE ATT&CK, NIST Cybersecurity Framework и отраслевых моделей, что создает предпосылки для формирования унифицированного понятийного аппарата в сфере управления рисками информационной безопасности. Параллельно происходит углубленная разработка отраслевых специализаций, где базовые таксономии адаптируются под специфические требования объектов критической информационной инфраструктуры, таких как системы АСУ ТП в энергетике или медицинские информационные системы, учитывающие особенности их архитектуры и профили угроз.

Значительное ускорение получает автоматизация процессов классификации киберинцидентов, где ручной анализ данных безопасности постепенно замещается алгоритмами корреляции событий, способными сопоставлять наблюдаемые артефакты атаки с тактиками и техниками из эталонных таксономий. Наиболее перспективным направлением становится интеграция систем искусственного интеллекта и машинного обучения в процессы таксономического анализа, позволяющая реализовать проактивное выявление неизвестных угроз через анализ аномальных паттернов поведения, прогнозирование векторов атак и автоматическую верификацию индикаторов компрометации. Этот эволюционный переход от статических классификаторов к динамическим интеллектуальным системам существенно повышает эффективность процессов обнаружения и реагирования на инциденты информационной безопасности в условиях реального времени.

Тенденции:

- конвергенция международных стандартов;
- разработка отраслевых специализаций;
- автоматизация процессов классификации;
- интеграция с системами ИИ и машинного обучения.

Выводы:

Современный ландшафт информационной безопасности диктует необходимость комплексного подхода к классификации угроз, что находит свое отражение в пяти ключевых выводах.

Во-первых, универсальные таксономии, такие как MITRE ATT&CK и NIST CSF, формируют необходимый базовый фундамент, предоставляя общий язык и структурированную модель для описания тактик, техник и процедур злоумышленников. Однако их основным ограничением является обобщенный характер, в связи с чем они требуют обязательной адаптации под конкретные условия каждой организации – ее технологический стек, бизнес-процессы и профиль рисков. Без такой кастомизации их практическая ценность существенно снижается.

Во-вторых, отраслевые таксономии, напротив, изначально разрабатываются с учетом специфики различных секторов экономики, будь то энергетика, здравоохранение или финансы. Они предлагают готовые наборы контрмер для защиты критической информационной инфраструктуры и объектов АСУ ТП. Обратной стороной такой специализации является потенциальное ограничение гибкости, так как они могут не успевать за новыми угрозами, не характерными исключительно для одной отрасли, и сковывать инициативу при построении системы защиты.

В-третьих, выбор таксономии не может быть произвольным; он должен основываться на трехстороннем анализе. Первый и часто определяющий фактор – это требования регуляторов, которые в рамках законодательства о КИИ могут предписывать использование конкретных стандартов. Второй фактор – отраслевые особенности, которые определяют релевантность тех или иных угроз и уязвимостей. И наконец, третий – уровень зрелости процессов

ИБ организации, поскольку попытка внедрения сложного фреймворка без должной подготовки обречена на провал.

В-четвертых, современная практика показывает, что наиболее эффективная система защиты строится не на одной, а на комбинации нескольких таксономий. Например, организация может использовать MITRE ATT&CK для настройки детектов в SOC, NIST CSF для управления рисками на стратегическом уровне, а отраслевой стандарт – для выполнения специфических регуляторных предписаний. Такой гибридный подход позволяет перекрыть слепые зоны, присущие любой отдельно взятой модели.

Наконец, в-пятых, развитие таксономий движется по трем четким векторам. Это детализация – углубление в специфические домены, такие как облачные среды и IoT; автоматизация – интеграция таксономий в системы SIEM/SOAR для автоматической классификации инцидентов; и интеллектуализация – интеграция с системами ИИ и машинного обучения для прогнозирования векторов атак и проактивного выявления неизвестных угроз.

Таким образом, эволюция таксономий угроз ведет от статических классификаторов к динамическим, интеллектуальным системам, которые становятся ядром оперативного управления информационной безопасностью, обеспечивая не только реакцию на инциденты, но и прогнозирование и предотвращение кибератак.

Глоссарий:

Безопасность информации (Информационная безопасность) – состояние защищенности информации, при котором обеспечиваются её целостность, конфиденциальность и доступность**.**

Кибербезопасность (Cybersecurity) – процесс защиты информации путем предотвращения, обнаружения и противодействия атакам, а также способность защищать или оборонять использование киберпространства от кибератак. Включает восстановление систем для обеспечения их доступности, целостности, аутентификации, конфиденциальности и неотказуемости.

Конфиденциальность (Confidentiality) – свойство информации, при котором доступ к ней имеют только уполномоченные лица (субъекты). Обеспечение того, что информация не раскрывается неуполномоченным лицам, процессам или устройствам.

Целостность (Integrity) – свойство информации, при котором она остается неизменной или изменения вносятся только уполномоченными субъектами. Гарантия того, что данные не были изменены несанкционированным образом с момента их создания, передачи или хранения.

Доступность (Availability) – свойство информации и ресурсов информационной системы, при котором уполномоченные субъекты могут получить к ним доступ и использовать их по требованию. Своевременный и надежный доступ к данным и системам для авторизованных пользователей.

Аутентификация (Authentication) – процесс верификации идентичности пользователя, процесса или системы, часто как предварительное условие для предоставления доступа к ресурсам информационной системы.

Неотказуемость (Non-repudiation) – гарантированная возможность доказать факт совершения действия или передачи информации определенным субъектом, что не позволяет этому субъекту впоследствии отказаться от данного факта.

Угроза (безопасности информации) (Threat) – совокупность условий и факторов, создающих потенциальную опасность нарушения свойств безопасности информации (конфиденциальности, целостности, доступности) и являющихся причиной инцидента ИБ.

Уязвимость (Vulnerability) – слабое место в активе, системе, процедуре или контроле, которое может быть использовано источником угрозы для нарушения безопасности информации.

Нарушитель (Актор угрозы) – субъект (лицо, группа, организация), являющийся источником угрозы. Может быть внешним или внутренним (инсайдером) по отношению к организации.

Кибератака (Cyber Attack) – целенаправленное вредоносное воздействие на информационный актив с целью нарушения его нормального функционирования или реализации угрозы безопасности обрабатываемой информации.

Вектор атаки (Attack Vector) – путь или метод, который использует нарушитель для получения несанкционированного доступа к системе или информации (например, фишинг, эксплуатация уязвимости).

Тактики, техники и процедуры (TTPs) – модель поведения нарушителя: **Тактика** – цель атаки на определенном этапе (например, получение первоначального доступа). **Техника** – конкретный способ достижения тактической цели (например, фишинг). **Процедура** – индивидуальная реализация техники конкретным актором.

Вредоносное программное обеспечение (Malware) – программа, устанавливаемая на компьютер или устройство с целью нарушения конфиденциальности, целостности или доступности данных, приложений или операционных систем. К распространенным типам относятся вирусы, черви, трояны, программы-вымогатели и шпионское ПО.

Программа-вымогатель (Ransomware) – тип вредоносного программного обеспечения, которое блокирует доступ к данным пользователя (обычно путем шифрования) и требует выкуп для восстановления доступа.

Фишинг (Phishing) – метод социальной инженерии, заключающийся в рассылке fraudulent (мошеннических) сообщений (часто по электронной почте) для получения конфиденциальной информации или побуждения жертвы к опасным действиям.

Инсайдер (Insider) – внутренний нарушитель, которым может быть действующий или бывший сотрудник, подрядчик или партнер, имеющий или

имевший авторизованный доступ к системам организации и использующий его для нанесения ущерба.

Информационный актив (Asset) – информация или ресурс информационной системы, имеющие ценность для организации и являющиеся объектом защиты.

Риск информационной безопасности (Risk) – потенциальная возможность того, что источник угрозы воспользуется уязвимостью актива для причинения ущерба организации. Обычно является функцией от вероятности события и серьезности его последствий.

Управление рисками (Risk Management) – скоординированная деятельность по руководству и контролю организации в отношении рисков. Включает идентификацию, анализ, оценку и обработку рисков, а также мониторинг.

Инцидент (информационной) безопасности (Cyber Incident) – событие или группа связанных событий, которые фактически или потенциально нарушают конфиденциальность, целостность или доступность информационной системы, либо нарушают политики безопасности. Может привести к успешной кибератаке и нанесению ущерба.

Классификация инцидентов (Incident Classification) – процесс категоризации инцидентов безопасности по различным признакам (тип атаки, затронутые активы, источник, воздействие) для стандартизированного учета, анализа и отчетности. ENISA разрабатывает референтную таксономию для таких классификаций.

Моделирование угроз (Threat Modelling) – структурированный процесс идентификации и документирования потенциальных угроз для системы, оценки их серьезности и определения контрмер.

Киберустойчивость (Cyber Resilience) – способность организации продолжать выполнение своих функций перед лицом кибератак или других инцидентов безопасности, а также своевременно восстанавливать нормальную работу.

Средство защиты информации (СЗИ) – технический, программный или программно-аппаратный продукт, предназначенный или используемый для обеспечения безопасности информации.

Аутентификация с многофакторной проверкой (Multi-factor Authentication, MFA) – метод аутентификации, при котором для подтверждения личности пользователя требуется предоставить два или более различных типа доказательств (факторов), таких как знание (пароль), владение (токен) или биометрия.

Шифрование (Encryption) – криптографическое преобразование данных (открытого текста) в форму (шифротекст), скрывающую исходное содержание, чтобы предотвратить его раскрытие или использование. Обратимый процесс дешифрования восстанавливает исходные данные.

Брандмауэр (Firewall) – устройство или программа, предназначенная для контроля сетевого трафика на основе заданных правил безопасности с целью блокирования несанкционированного доступа.

Система обнаружения и предотвращения вторжений (IDS/IPS) – технология, которая отслеживает сеть или активность системы на предмет злонамеренных действий или нарушений политик. Система предотвращения (IPS) также может предпринимать действия для блокировки такой активности.

Вопросы и задания для самоконтроля:

1. Назовите и охарактеризуйте две основные причины, приведшие к ситуации информационной перегрузки в сфере ИБ.
2. Дайте определение таксономии угроз информационной безопасности. Чем она принципиально отличается от простого списка угроз?
3. Перечислите и раскройте пять ключевых «китов» классификации любой таксономии угроз.
4. Опишите три практические выгоды, которые получает организация от внедрения таксономии угроз (помимо создания единого языка).
7. В чем заключается основное предназначение фреймворка MITRE ATT&CK? Как расшифровывается аббревиатура TTP?
8. Опишите трехуровневую структуру матрицы MITRE ATT&CK (тактика – техника - процедура). Приведите конкретный пример связки для каждой из стадий атаки.
9. Сравните фокус таксономии ENISA и фреймворка MITRE ATT&CK. Какой из подходов больше ориентирован на операционные риски бизнеса в рамках европейского регулирования?
10. Назовите ключевые преимущества и ограничения MITRE ATT&CK с точки зрения его внедрения в организации.
11. Охарактеризуйте подход BSI Grundschutz. Что представляют собой его основные компоненты?
12. Какова основная цель NIST Cybersecurity Framework? Перечислите и кратко раскройте его пять основных функций (Identify, Protect, Detect, Respond, Recover).
13. Для каких типов организаций и систем изначально разрабатывались BSI Grundschutz и NIST CSF?
14. Заполните сравнительную таблицу по памяти, указав для каждой таксономии (MITRE ATT&CK, ENISA, BSI Grundschutz, NIST CSF) ее происхождение, основной фокус и ключевые сильные стороны.
15. Объясните, в чем заключается принципиальное различие между таксономией, ориентированной на тактики атакующих (как MITRE ATT&CK), и фреймворком, ориентированным на управление рисками (как NIST CSF). Как они могут дополнять друг друга?
16. В чем состоит национальная специфика российских подходов к таксономии угроз согласно представленным материалам?

17. Перечислите ключевые документы ФСТЭК России, которые формируют основу для обязательной таксономии и классификации угроз в РФ.

18. Какой основной акцент в построении таксономий делается в России, ЕС и США?

19. Приведите по одному практическому сценарию использования для каждой из таксономий: MITRE ATT&CK, BSI Grundschutz, ENISA, NIST CSF.

20. Сформулируйте четыре ключевых критерия, которыми должна руководствоваться организация при выборе таксономии угроз для внедрения.

21. Назовите основные тенденции в развитии таксономий угроз, представленные в материалах главы.

22. Сделайте обоснованный вывод: почему современная практика информационной безопасности требует комбинированного использования нескольких таксономий, а не опирается на какую-либо одну?

23. Сформулируйте свою позицию на предмет того какую таксономию (или их комбинацию) вы бы рекомендовали для крупного российского банка и почему? Аргументируйте, исходя из требований регуляторов, отраслевой специфики и операционных задач.

ГЛАВА 4. ФОРМАЛЬНЫЕ МОДЕЛИ ПРЕДСТАВЛЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: НАЗНАЧЕНИЕ И ПРИМЕРЫ

В условиях экспоненциального роста сложности и скоординированности кибератак, эвристические и описательные подходы к анализу угроз становятся недостаточными. Формальные модели представления угроз выполняют критическую функцию структурирования знаний о TTPs (Tactics, Techniques, and Procedures) противника, обеспечивая переход от реактивного к проактивному позиционированию систем защиты. Эти модели служат онтологическим каркасом для унификации языка специалистов ИБ, автоматизации процессов киберразведки (Threat Intelligence) и разработки детерминированных сценариев реагирования на инциденты.

4.1. Назначение и методологическая база формальных моделей информационной безопасности

Формальные модели информационной безопасности представляют собой абстрактные конструкты и математизированные представления, предназначенные для трансформации неструктурированных данных об угрозах в детерминированные схемы, пригодные для алгоритмического анализа, верификации и автоматизированной обработки. Они служат концептуальным каркасом, который формализует взаимодействия между активами, уязвимостями, акторами угроз и мерами защиты, обеспечивая переход от интуитивного понимания рисков к системному инженерному подходу.

Ключевые функции формальных моделей раскрываются в следующих аспектах:

1. *Таксономическая функция*: модели обеспечивают унификацию терминологии и создают иерархические системы для классификации векторов атак, тактик, техник и процедур (TTPs). Это формирует общий понятийный аппарат, позволяющий специалистам по кибезащите, разработчикам и регуляторам однозначно идентифицировать и категоризировать инциденты. Примером является модель MITRE ATT&CK, которая стандартизирует описание поведения противника.

2. *Аналитическая функция*: модели позволяют проводить декомпозицию жизненного цикла кибератаки на дискретные, логически связанные фазы (например, разведка, начальное проникновение, закрепление, выполнение целей). Такой подход, воплощенный в моделях типа Cyber Kill Chain, обеспечивает точечный анализ уязвимостей на каждом этапе, выявление точек отказа системы защиты и оценку эффективности контрмер.

3. *Прогностическая функция*: на основе каталогизированных TTPs и анализа трендов формальные модели позволяют проводить моделирование сценариев атак (threat modeling). Это включает в себя проактивное выявление

потенциальных векторов компрометации для конкретной архитектуры системы, оценку вероятности реализации угрозы и прогнозирование возможного ущерба (impact). Модели вроде STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) используются для систематического поиска уязвимостей на этапе проектирования.

4. *Операционная функция*: важнейшим практическим итогом моделирования является формирование матрицы контроля (Control Matrix) или таблицы сопоставления. Данный инструмент устанавливает прямые связи между идентифицированными угрозами, уязвимостями и конкретными организационно-техническими мерами защиты. Это позволяет оптимально распределять ресурсы, обосновывать выбор средств защиты информации (СЗИ) и выстраивать приоритеты для системы управления информационными рисками.

Сравнительный анализ роли моделей в национальных стратегиях информационной безопасности демонстрирует, как формальные подходы адаптируются под различные регуляторные и геополитические задачи:

Европейский Союз: в рамках ЕС формальные модели служат, прежде всего, основой для кросс-граничного обмена информацией об угрозах (Threat Intelligence). Это является ключевым требованием Директивы NIS2 и центральной задачей Агентства ЕС по кибербезопасности (ENISA). Акцент делается на моделях, ориентированных на обеспечение конфиденциальности и целостности данных, таких как модификации STRIDE для оценки рисков в контексте Общего регламента по защите данных (GDPR). Модели здесь выступают инструментом гармонизации и создания устойчивого единого цифрового рынка.

Китайская Народная Республика: в КНР формальные модели глубоко интегрированы в государственные системы контроля и мониторинга киберпространства, такие как «Великий киберщит». Национальные стандарты (например, серия GB/T) предписывают использование формализованных подходов для категорирования информационных систем и управления рисками. Приоритет отдается моделям, которые позволяют осуществлять атрибуцию кибератак и классифицировать их как угрозы национальной безопасности или социальной стабильности. Таким образом, модель становится инструментом обеспечения киберсуверенитета и государственного управления.

Российская Федерация: в РФ применение формальных моделей жёстко привязано к задачам защиты критической информационной инфраструктуры (КИИ) и выполнению требований регуляторов (ФСТЭК, ФСБ России). Развиваются гибридные подходы, которые сочетают международные, признанные фреймворки, такие как MITRE ATT&CK, с детализированными отечественными методиками, описанными в стандартах типа ГОСТ Р 59533 (Защита информации в АСУ ТП). Это позволяет адаптировать передовые практики таксономирования угроз и анализа TTPs к специфическим

требованиям российского законодательства, включая необходимость использования сертифицированных СЗИ и соблюдения принципов импортозамещения. Модель здесь служит целям построения защищённого государственного контура.

Таким образом, формальные модели трансформируются из чисто технического инструментария в стратегический актив, отражающий приоритеты национальной политики в области кибербезопасности – будь то защита прав граждан и трансграничных потоков данных (ЕС), тотальный контроль и суверенитет (КНР) или обеспечение безопасности изолированных критически важных объектов (РФ).

4.2. Модель цепочки кибератаки (Cyber Kill Chain®): таксономия и противодействие многоэтапным угрозам

Модель цепочки кибератаки (Cyber Kill Chain®), разработанная компанией Lockheed Martin, представляет собой фундаментальный формальный таксономический фреймворк, который декомпозирует жизненный цикл сложной целевой атаки на линейную последовательность из семи дискретных стадий. Эта модель служит картой для кибераналитиков, переводя хаотичные события безопасности в структурированный нарратив действий противника, что позволяет перейти от реактивного тушения пожаров к проактивному противодействию путем «обрыва цепочки» на наиболее ранних и уязвимых этапах.

Семь стадий модели образуют полный путь реализации угрозы:

1. Разведка (Reconnaissance): на этой начальной фазе злоумышленник осуществляет пассивный и активный сбор разведывательной информации о цели. Это может включать анализ публичных данных в открытых источниках (OSINT), сканирование сетевых портов для выявления уязвимостей и составление профиля ключевых сотрудников для последующих атак социальной инженерии.

2. Создание инструмента атаки (Weaponization): на основе собранных данных осуществляется подготовка вредоносного полезного груза (malware payload). Эта стадия включает связывание эксплойта, нацеленного на конкретную уязвимость нулевого дня (zero-day) или известную CVE, с бекдором в единый пакет, например, в виде специально сформированного документа PDF или исполняемого файла.

3. Доставка (Delivery): происходит транспортировка созданного инструмента атаки к целевой системе. Типичные векторы доставки включают фишинговые электронные письма с вложениями, компрометированные веб-сайты (watering hole attacks) или зараженные съемные носители.

4. Эксплуатация (Exploitation): после доставки активируется эксплойт, который использует выявленную уязвимость в программном обеспечении или конфигурации системы для выполнения произвольного кода. Целью является

преодоление периметровых средств защиты и получение первоначального доступа к системе.

5. Установка (Installation): на этой стадии на скомпрометированный ресурс устанавливается постоянное вредоносное программное обеспечение, обеспечивающее устойчивое присутствие злоумышленника. Это может быть бекдор, руткит или другое средство обеспечения постоянного доступа (persistence).

6. Управление и контроль (Command and Control – C2): установленное вредоносное ПО устанавливает скрытый канал управления (C2-channel) с сервером злоумышленника. Этот канал позволяет атакующему удаленно отправлять команды, передавать похищенные данные (exfiltration) и масштабировать свое влияние внутри инфраструктуры жертвы.

7. Действия по достижению целей (Actions on Objectives): финальная стадия, на которой реализуется изначальная цель атаки. В зависимости от мотивации актора угроз, это может быть хищение конфиденциальных данных (data breach), нарушение целостности информации, шифрование данных для выкупа (ransomware) или деструктивное воздействие для нарушения доступности сервисов (DoS-атака).

Сравнительный анализ применения модели в различных национальных стратегиях кибербезопасности демонстрирует её адаптацию под специфические регуляторные и оперативные задачи (табл. 4.1).

Таблица 4.1

Применение модели в различных национальных стратегиях кибербезопасности

Юрисдикция	Контекст применения	Ключевой акцент и адаптация
Европейский Союз	Используется национальными группами реагирования на компьютерные инциденты (CERT/CSIRT).	Анализ инцидентов и формирование скоординированных предупреждений в рамках европейской платформы обмена информацией об угрозах (Threat Intelligence). Модель служит общим языком для выполнения требований директив NIS2.
Китай (КНР)	Интегрирована в государственные системы мониторинга и нормативные стандарты (GB/T).	Акцент на превентивном обрыве цепочки на стадиях Delivery (фильтрация входящего трафика) и C2 (блокировка внешних командных серверов). Модель адаптирована для защиты киберсуверенитета и контроля за трансграничными потоками данных.
Российская Федерация	Применяется для построения систем обнаружения вторжений (СОВ/IDS) и защиты критической информационной инфраструктуры (КИИ).	Интеграция с отечественными криптографическими решениями (ГОСТ-шифрование) для противодействия перехвату и анализу трафика на стадии C2. Фокус на обеспечении отказоустойчивости и целостности объектов КИИ от сложных APT-атак.

4.3. Матрица MITRE ATT&CK®: таксономия поведения противника как основа проактивной обороны

Матрица MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) представляет собой эволюцию формальных моделей угроз, трансформировавшуюся из внутренней аналитической базы знаний в глобальный стандарт де-факто для классификации и описания поведения злоумышленников в киберпространстве. Назначение и эволюция модели заключаются в предоставлении структурированной основы для проактивного противодействия. В отличие от линейных моделей, таких как Cyber Kill Chain, ATT&CK фокусируется не на последовательности этапов, а на детализированном каталоге тактик, техник и процедур (TTPs), используемых противниками на протяжении всего жизненного цикла атаки после первоначального компрометирования. Понимая, что стоимость противодействия для защищающейся стороны экспоненциально возрастает с каждой последующей стадией Kill Chain, модель призывает к раннему детектированию и нейтрализации угроз. Эта модель служит универсальным таксономическим языком, позволяющим аналитикам киберугроз, специалистам центров мониторинга безопасности (SOC) и архитекторам систем защиты перейти от абстрактного понимания угрозы к операциональному анализу конкретных методов противника.

Несмотря на то, что современные атаки часто имеют нелинейный, итеративный характер, а фреймворк MITRE ATT&CK предлагает более детализированную таксономию TTPs, модель Cyber Kill Chain остается эффективным инструментом для обучения, стратегического планирования обороны и анализа сложных целевых атак (Advanced Persistent Threat, APT), обеспечивая таксономическую ясность в процессе расследования инцидентов.

Структура и концептуальная основа матрицы построена на иерархии трех ключевых элементов:

1. *Тактика* (Tactic) – отвечает на вопрос «ЗАЧЕМ?» атакующий выполняет определенное действие в рамках своего операционного цикла. Это цель злоумышленника на конкретном временном отрезке атаки. Примеры тактик включают Первоначальный доступ (Initial Access), Закрепление (Persistence), Привилегированное расширение прав (Privilege Escalation), Латеральное перемещение (Lateral Movement), Сбор данных (Collection) и Выполнение целей (Impact). Всего в матрице для корпоративных сред (ATT&CK for Enterprise) определено 14 тактик.

2. *Техника* (Technique) – отвечает на вопрос «Как?» достигается тактическая цель. Это конкретные методы или действия, используемые злоумышленником. Например, для тактики Первоначальный доступ техниками являются Фишинг (Phishing), Эксплуатация публичных приложений (Exploit Public-Facing Application) или Использование съемных носителей (Replication Through Removable Media).

3. *Под-техника* (Sub-technique) – представляет собой более детализированное описание техники, дающее гранулярное понимание конкретного вектора атаки. Например, техника Фишинг (Phishing) включает под-техники Специальный фишинг (Spearphishing Attachment), Фишинг через сервис (Spearphishing Link) и Фишинг через сторонние сервисы (Spearphishing via Service).

Практическая ценность и применение матрицы MITRE ATT&CK раскрывается в нескольких ключевых сценариях:

Построение и совершенствование систем обнаружения (Detection Engineering): матрица служит основой для проактивной настройки корреляционных правил в системах управления событиями и инцидентами безопасности (SIEM) и платформах безопасности (XDR/SOAR). Аналитики могут сопоставлять наблюдаемые в сети аномалии (например, нестандартное использование PowerShell) с конкретными техниками (T1059.001 – Командный интерпретатор: PowerShell), что позволяет выявлять не просто вредоносное ПО, а цепочки компрометирующих действий.

Анализ угроз и атрибуция (Threat Intelligence & Attribution): Группы реагирования на инциденты (CERT/CSIRT) и аналитики используют ATT&CK для описания TTPs конкретных групп продвинутых постоянных угроз (APT). Это позволяет создавать профили поведения акторов, отслеживать эволюцию их методов и осуществлять предварительную атрибуцию новых атак на основе совпадения известных техник.

Оценка защищенности и моделирование атак (Red Teaming & Purple Teaming): Команды красных команд (Red Team) применяют матрицу как план для моделирования реалистичных многоэтапных атак, проверяя эффективность существующих контрмер. Совместные учения «фиолетовых команд» (Purple Teaming), где синие (оборона) и красные (атака) команды работают вместе, используют ATT&CK как общий язык для анализа пробелов в защите.

Управление рисками и приоритизация контрмер: Организации могут проводить сопоставление своих возможностей обнаружения и защиты с техниками матрицы, выявляя тактические и технические «слепые зоны». Это позволяет обоснованно распределять ресурсы и инвестиции в средства защиты, фокусируясь на противодействии наиболее релевантным для их отрасли и инфраструктуры TTPs.

Эволюция и специализация. Изначально созданная для корпоративных IT-сетей (ATT&CK for Enterprise), матрица была расширена для покрытия специализированных доменов:

ATT&CK for Mobile – фокусируется на техниках атак против мобильных операционных систем (iOS, Android).

ATT&CK for ICS – таксономия для индустриальных систем управления (АСУ ТП), критически важная для защиты объектов критической информационной инфраструктуры (КИИ) в энергетике, промышленности и на транспорте.

ATT&CK for Cloud – описывает техники, специфичные для облачных сред (AWS, Azure, GCP), такие как манипулирование сервисами идентификации или несанкционированное создание вычислительных экземпляров.

Национальный контекст применения. В российской практике, особенно в государственном секторе и на объектах КИИ, матрица MITRE ATT&CK не заменяет, а дополняет требования национальных стандартов (ГОСТ Р 59533, методики ФСТЭК). Она используется для:

– детализации модели угроз, требуемой регуляторами, путем привязки общих категорий угроз к конкретным, наблюдаемым в мире техникам;

– повышения эффективности отечественных систем обнаружения вторжений (СОВ) и SIEM-решений за счет имплементации правил детектирования, основанных на актуальных TTPs;

– обмена информацией об угрозах на международном профессиональном уровне, что позволяет отечественным CERT-ам понимать и заранее готовиться к методам, используемым иностранными APT-группами.

Таким образом, матрица MITRE ATT&CK® представляет собой не статичный справочник, а живую, постоянно обновляемую таксономическую платформу. Она трансформирует управление информационной безопасностью из дисциплины, основанной на сигнатурах вредоносного ПО и изолированных событиях, в интеллектуальный процесс, ориентированный на поведение противника и проактивное построение обороны, что является краеугольным камнем современной концепции киберустойчивости (Cyber Resilience).

4.4. Модель STRIDE: таксономия угроз на этапе проектирования

Модель, ориентированная на анализ угроз на этапе проектирования архитектуры и разработки программного обеспечения (Security by Design) [42].

Выделяют шесть категорий угроз:

Spoofing (Маскировка): несанкционированный доступ с использованием легитимных учетных данных.

Tampering (Изменение данных): несанкционированная модификация данных или кода.

Repudiation (Отказ от операций): возможность субъекта отрицать совершение действия.

Information Disclosure (Раскрытие информации): несанкционированное получение данных.

Denial of Service (DoS) (Отказ в обслуживании): нарушение доступности сервиса.

Elevation of Privilege (Повышение привилегий): получение неавторизованных прав доступа.

Назначение: систематическое выявление угроз безопасности при проектировании систем и приложений, проведение Threat Modeling.

Сравнительный анализ применения.

ЕС: широко используется для compliance с требованиями GDPR (защита целостности и конфиденциальности) и директивы eIDAS (идентификация).

КНР: применяется при разработке ПО для государственных нужд в рамках стандарта GB/T 25000, с особым вниманием к категориям «Tampering» и «Information Disclosure».

РФ: рекомендована ФСТЭК для анализа защищенности информационных систем, особенно в части противодействия «Spoofing» и «Elevation of Privilege» при реализации требований к аутентификации и управлению доступом (табл. 4.2).

Таблица 4.2

Сравнительный анализ формальных моделей представления угроз

Критерий	Cyber Kill Chain	MITRE ATT&CK	STRIDE
Уровень детализации	Макроуровень (фазы)	Тактико-технический (TTPs)	Архитектурный (категории)
Основное назначение	Проактивная защита, обрыв атаки	Атрибуция, настройка детектирования, тестирование	Проектирование безопасных систем (Threat Modeling)
Гибкость	Линейная модель	Адаптивная, таксономическая матрица	Таксономическая модель
Приоритет в ЕС	Высокий (CERTs, NIS2)	Очень высокий (SOC, Threat Intel)	Высокий (GDPR, Secure SDLC)
Приоритет в КНР	Средний (адаптация под GB/T)	Средний (селективное использование)	Средний (для гос. ПО)
Приоритет в РФ	Высокий (КИИ, СОВ)	Очень высокий (адаптация под ФСТЭК)	Средний (рекомендации ФСТЭК)

Выводы и актуальные тренды

Методологические выводы:

1. Наблюдается эволюция от линейных (Kill Chain) к многомерным таксономическим моделям (ATT&CK), обеспечивающим более глубокий контекстный анализ угроз.

2. Эффективность модели напрямую коррелирует с ее интеграцией в регуляторные требования и операционные процессы SOC.

3. Ключевым трендом является конвергенция моделей: например, использование тактик ATT&CK для детализации стадий Kill Chain или применение STRIDE для оценки угроз отдельным техникам ATT&CK.

Регуляторные тренды:

ЕС: унификация использования ATT&CK через ENISA и стимулирование Threat Modeling (STRIDE) в рамках законодательства о киберустойчивости.

КНР: развитие суверенных таксономий на основе GB/T, с элементами заимствования из ATT&CK для целей внутреннего контроля.

РФ: формализация требований к использованию моделей (в первую очередь, адаптированного ATT&CK и Kill Chain) в документах ФСТЭК по защите КИИ.

Практические рекомендации для специалистов ИБ.

Для построения SOC:

– используйте MITRE ATT&CK в качестве базовой таксономии для настройки корреляционных правил в SIEM и формирования Use Cases;

– реализуйте процесс Threat Hunting, основанный на профилях TTPs из матрицы ATT&CK.

Для защиты КИИ (РФ):

– проводите обязательное моделирование угроз по методологии ФСТЭК, комбинируя подходы Kill Chain и STRIDE;

– адаптируйте техники MITRE ATT&CK для создания отраслевых «Атласов угроз» с привязкой к критическим процессам.

Для транснациональных компаний:

– разрабатывайте интегральные карты угроз, совмещающие тактики ATT&CK с регуляторными требованиями GDPR (ЕС), GB/T (КНР) и ФСТЭК (РФ).

Перспективные исследования:

– разработка моделей угроз для киберфизических систем (CPS) и интернета вещей (IoT), учитывающих пересечение кибер- и физических атак [41].

– создание онтологий для представления угроз в условиях активного внедрения технологий искусственного интеллекта и машинного обучения.

Глоссарий:

Информационная безопасность (Information Security) - состояние защищенности информации, при котором обеспечиваются её целостность, конфиденциальность и доступность. Защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения для обеспечения целостности, конфиденциальности и доступности.

Кибербезопасность (Cybersecurity) - практика защиты систем, сетей и программ от цифровых атак. Часто используется как синоним ИБ, но с акцентом на киберпространство.

Целостность (Integrity) - состояние информации, при котором она либо остается неизменной, либо изменения осуществляются только теми, кто имеет на это право. Охрана от неправомерного изменения или уничтожения информации.

Конфиденциальность (Confidentiality) - состояние информации, при котором доступ к ней имеют только те, кто обладает соответствующими

правами доступа. Сохранение установленных ограничений на доступ и раскрытие информации.

Доступность (Availability) - состояние информации (ресурсов информационной системы), при котором обладающие необходимыми правами доступа могут их беспрепятственно реализовать. Обеспечение своевременного и надежного доступа к информации и её использования.

Угроза безопасности информации (Threat) - совокупность условий и факторов, создающих потенциальную опасность нарушения свойств безопасности информации и являющихся причиной инцидента ИБ.

Уязвимость (Vulnerability) - слабое место актива или средства контроля, которое может быть использовано злоумышленником для реализации угрозы безопасности информации.

Актор угрозы (Threat Actor) - субъект (нарушитель), являющийся источником угрозы. Может быть внешним или внутренним (инсайдером).

Продвинутая постоянная угроза (Advanced Persistent Threat (APT)) - киберугроза, обычно относящаяся к интернет-шпионажу с использованием различных методов сбора разведданных для доступа к конфиденциальной информации.

Тактика, техника и процедура (Tactics, Techniques, and Procedures (TTPs)) - классификация способов реализации угроз по применяемым злоумышленниками тактикам (цели), техникам (методы) и процедурам (конкретные реализации).

Моделирование угроз (Threat Modeling) - идентификация всех угроз, которые могут нанести ущерб, и векторов атак, которые могут быть использованы источниками угроз. Проактивный процесс анализа архитектуры системы на предмет потенциальных уязвимостей.

Цепочка кибератаки (Cyber Kill Chain®) - формальная модель, описывающая этапы целевой атаки: разведка (Reconnaissance), создание инструмента атаки (Weaponization), доставка (Delivery), эксплуатация (Exploitation), установка (Installation), Управление и контроль (Command & Control), действия по достижению целей (Actions on Objectives).

MITRE ATT&CK® - таксономическая матрица и база знаний о тактиках (цели противника, *зачем*), техниках (конкретные методы, *как*) и под-техниках (деталях), используемых злоумышленниками в различных средах (Enterprise, ICS, Mobile).

Модель STRIDE - модель классификации угроз для проектирования, включающая шесть категорий: Спуфинг (Spoofing), Изменение данных (Tampering), Отказ от операций (Repudiation), Раскрытие информации (Information Disclosure), Отказ в обслуживании (Denial of Service), Повышение привилегий (Elevation of Privilege).

Компьютерная группа экстренного реагирования (Computer Emergency Response Team (CERT/CSIRT)) - группа экспертов по ИТ-безопасности, предоставляющая реактивные и проактивные услуги, одной из основных является реагирование на инциденты.

Критическая информационная инфраструктура (КИИ) (Critical Information Infrastructure) - информационная инфраструктура (сети, оборудование, ПО), критически важная для функционирования государства или страны (например, ИТ в сфере здравоохранения или энергетики).

Общий регламент по защите данных (General Data Protection Regulation (GDPR)) - Основной нормативный акт ЕС, регулирующий обработку и защиту персональных данных физических лиц.

Вопросы и задания для самоконтроля:

1. Охарактеризуйте четыре ключевые функции формальных моделей представления угроз и приведите пример их практической реализации для каждой функции.
2. Проведите сравнительный анализ моделей Cyber Kill Chain и MITRE ATT&CK по следующим критериям: уровень детализации, гибкость применения и эффективность против APT-атак.
3. Каковы основные ограничения линейной модели Cyber Kill Chain при анализе современных многовекторных кибератак?
4. Объясните, как тактики, техники и процедуры (TTPs) в матрице MITRE ATT&CK соотносятся с этапами моделирования угроз STRIDE.
5. Проанализируйте, почему модель STRIDE считается наиболее эффективной на этапе проектирования систем (Security by Design).
6. Сравните подходы ЕС, КНР и РФ к адаптации международных моделей представления угроз. Какие политические и регуляторные факторы определяют эти различия?
7. Обоснуйте, почему в Европейском союзе модель MITRE ATT&CK стала де-факто стандартом для SOC, тогда как в Китае наблюдается ее селективное использование.
8. Какие особенности защиты критической информационной инфраструктуры (КИИ) в РФ обуславливают активную адаптацию моделей Cyber Kill Chain и MITRE ATT&CK?
9. Проанализируйте, как требования GDPR повлияли на модификацию модели STRIDE в европейской практике информационной безопасности.
10. Почему в КНР формальные модели угроз интегрированы преимущественно в государственные системы мониторинга, а не в коммерческий сектор?
11. Разработайте план интеграции MITRE ATT&CK в процессы Security Operations Center (SOC) многонациональной корпорации.
12. Каким образом можно комбинировать модели Cyber Kill Chain и STRIDE при проведении оценки защищенности объекта КИИ в РФ?
13. Обоснуйте выбор конкретной модели представления угроз для каждого из следующих сценариев:
    - расследование инцидента безопасности в финансовом секторе;
    - проектирование системы защиты персональных данных;

– организация противодействия целевым атакам на промышленные системы.

14. Какие технические и организационные сложности возникают при сопряжении тактик MITRE ATT&CK с контрмерами, требуемыми ФСТЭК?

15. Разработайте концепцию использования формальных моделей угроз для построения системы Threat Intelligence в транснациональной компании.

16. Проанализируйте основные тренды конвергенции формальных моделей представления угроз. Приведите примеры успешной интеграции различных моделей.

17. Какие новые классы угроз требуют разработки специализированных моделей представления, и какие подходы к их созданию наиболее перспективны?

18. Критически оцените эффективность существующих формальных моделей для анализа угроз киберфизическим системам (CPS).

19. Какие методологические проблемы возникают при адаптации западных моделей представления угроз в условиях импортозамещения в РФ?

20. Спрогнозируйте развитие формальных моделей представления угроз в контексте активного внедрения технологий искусственного интеллекта и машинного обучения.

ЗАКЛЮЧЕНИЕ

Настоящий учебник представил систематизированное исследование современной парадигмы угроз информационной безопасности, последовательно раскрывая их сущность, эволюцию и методы противодействия в условиях цифровой трансформации. Рассмотрение проблемы осуществлялось по восходящему принципу: от фундаментальных определений к сложным таксономическим системам и формальным моделям проактивной защиты.

Синтез ключевых идей материала учебника позволяет сформулировать следующие выводы:

1. Угроза ИБ предстает не как статичный фактор, а как динамичный процесс, детерминированный источником, целью, способом реализации и потенциальными последствиями. Анализ практических кейсов в юрисдикциях ЕС, КНР и РФ продемонстрировал, что оценка угроз и выбор мер защиты неразрывно связаны с национальными правовыми экосистемами, приоритетами государственной политики (киберсуверенитет, защита персональных данных, безопасность КИИ) и технологическим суверенитетом (импортозамещение, постквантовая криптография).

2. Многообразие принципов классификации (по источнику, воздействию, аспекту CIA-триады, объекту) формирует многомерное пространство для анализа угроз. Это пространство структурируется с помощью универсальных и отраслевых таксономий. Сравнительный анализ показал, что такие фреймворки, как MITRE ATT&CK, BSI Grundschutz и NIST CSF, создают общий язык для специалистов, в то время как национальные стандарты (GB/T в Китае, требования ФСТЭК в России) обеспечивают нормативное закрепление конкретных мер защиты, отражая специфику регуляторных подходов.

3. Формальные модели представления угроз (Cyber Kill Chain®, MITRE ATT&CK®, STRIDE) являются логическим завершением эволюции от классификации к операционализации знаний. Они трансформируют описательные категории в инженерные схемы, пригодные для алгоритмического анализа, моделирования атак, проактивного Threat Hunting и построения систем обнаружения. Адаптация этих моделей под задачи защиты критической информационной инфраструктуры, с учетом требований ГОСТ Р и отечественных СЗИ, является необходимым условием построения эффективной обороны в российском сегменте.

Таким образом, современная защита от угроз информационной безопасности – это не применение разрозненных технических средств [34], а комплексный управленческий и инженерный процесс, основанный на:

– глубоком понимании мотивации и TTPs современных акторов (от киберпреступников до APT-групп);

– строгой таксономической дисциплине, позволяющей унифицировать терминологию, обмениваться данными об угрозах и измерять эффективность контрмер;

– проактивной позиции, реализуемой через моделирование угроз на этапе проектирования (Security by Design) и постоянный поиск признаков компрометации;

– неразрывном учете регуляторного контекста, который в современных условиях определяет не только обязательные требования, но и стратегические направления развития систем защиты.

Перспективы дальнейшего развития области видятся в углубленной конвергенции таксономий и моделей, их интеграции с системами искусственного интеллекта для прогнозной аналитики, а также в разработке специализированных методологий для защиты киберфизических систем, интернета вещей (IoT) и технологических цепочек создания стоимости в условиях гибридных угроз. Учебник закладывает теоретический и практический фундамент для подготовки специалистов, способных отвечать на эти вызовы, сочетая знание международных стандартов с компетенциями в области национальных требований к безопасности информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ENISA Threat Landscape Report 2023 / European Union Agency for Cybersecurity. – Luxembourg: Publications Office of the European Union, 2023. – 120 p. – ISBN 978-92-9206-123-4.
2. MITRE ATT&CK® Matrix for Enterprise / The MITRE Corporation. – 2024. – *Текст: электронный* // MITRE. – URL: https://attack.mitre.org (дата обращения: 01.07.2025).
3. NIST FIPS 203 (Draft). Module-Lattice-Based Key-Encapsulation Mechanism Standard / National Institute of Standards and Technology. – Gaithersburg: NIST, 2023. – 142 p.
4. Why information protection is important. - URL: https://data.uq.edu.au/data-and-information-essentials/why-information-protection-important (дата обращения: 30.10.2025).
5. Акапьев В.Л. Методы анализа угроз нарушения информационной безопасности ведомственного объекта информатизации: учебное пособие / В.Л. Акапьев, А.В. Борисенко, Е.Г. Ковалева, Е.А. Новикова, Ю.А. Пироженко. – СПб.: Наукоемкие технологии, 2026. – 104 с.
6. Акапьев В.Л. Объекты защиты в области информационной безопасности по российскому законодательству / С.Е. Савотченко // Алтайский юридический вестник. 2023. № 3 (43). С. 27-35.
7. Акапьев В.Л. Оценка защищенности объекта информатизации ОМВД России / Е.Г. Ковалева, А.В. Борисенко // Вестник Воронежского института ФСИН России. 2025. № 2. С. 20-30.
8. Акапьев В.Л. Оценка защищенности объекта информатизации от утечки информации по виброакустическому каналу / Е.Г. Ковалева, А.В. Борисенко // Вестник Воронежского института ФСИН России. 2025. № 3. С. 42-50.
9. Акапьев В.Л. Проблемы информационного обеспечения деятельности правоохранительных органов // Сборник статей XII Всероссийской научно-практической конференции. - Белгород, 2025.
10. Акапьев В.Л. Проблемы реализации регуляторной политики государства в области информационной безопасности хозяйствующих субъектов / С.Е. Савотченко // Вестник владимирского юридического института. 2024. № 1 (70). С. 95-102.
11. Акапьев В.Л. Публично-правовое регулирование обеспечения безопасности объектов критической информационной инфраструктуры / С.Е. Савотченко // Вестник Удмуртского университета. Серия Экономика и право. 2024. Т. 34. № 3. С. 494-503.
12. Аналитика рынка интернета вещей в России / Росатом инфраструктурные решения. – М., 2024. URL: https://rosatom.cnews.ru/news/line/2024-12-13_issledovanie_rosatoma (дата обращения: 30.06.2025).

13. Ануфриев А.С. Криптография на решётках: алгоритмы и реализация / А.С. Ануфриев, В.Г. Болотов, И.В. Чугунков. – М.: Криптософт, 2023. – 320 с. – ISBN 978-5-9905-1234-5.

14. Аудит информационной безопасности: учебное пособие / С.И. Козьминых, С.А. Борисов. – М.: КНОРУС, 2026. – 336 с.

15. Баланов А.Н. Комплексная информационная безопасность. Полный справочник специалиста. Практическое пособие. - М.: Инфра-Инженерия. 2024. - 156 с.

16. Баранова Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 2-е изд., стер. – Москва: КНОРУС, 2025. – 132 с.

17. Баранова Е.К. Информационная безопасность. История специальных методов криптографической деятельности: учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. – Москва: РИОР: ИНФРА-М, 2024. – 236 с.

18. Баранова Е.К. Информационная безопасность: лабораторный практикум / Е.К. Баранова, А.В. Бабаш, Ю.Н. Мельников. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2024. – 336 с.

19. Белоус А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А.И. Белоус. – Москва; Вологда: Инфра-Инженерия, 2020. – 644 с.

20. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. - М.: МГТУ им. Н. Э. Баумана. 2024. - 252 с.

21. Борисенко А.В. Оценка защищенности объекта информатизации от утечки информации по акустическому каналу / Е.Г. Ковалева, В.Л. Акапьев // Вестник Воронежского института ФСИН России. 2025. № 2. С. 31-45.

22. Бурлаков М.Е. Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум: учебное пособие / М.Е. Бурлаков, М.Н. Осипов. – Самара: Издательство Самарского университета, 2021 – 96 с. ил.

23. Васильев Р.А., Ротков Л.Ю. Обнаружение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса «Легенда»: учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2018 – 45 с.

24. Васильева Т.Ю., Куприянов А.И., Мельников В.П. Информационная безопасность. Учебник. - М.: КноРус. 2023. - 372 с.

25. Вехен Джульен Безопасный DevOps. Эффективная эксплуатация систем. – СПб.: Питер, 2020. - 432 с.: ил.

26. Владстон Феррейра Фило, Мото Пиктет Теоретический минимум по Computer Science. Сети, криптография и data science. - СПб.: Питер, 2022. – 288 с.: ил.

27. Внуков А.А. Основы информационной безопасности: защита информации. – М.: ЮРАЙТ, 2024. – 162.

28. Вострецова Е.В. Основы информационной безопасности: учебное пособие. – Екатеринбург, 2019. – 204.

29. Галатенко В.А. Информационная безопасность // Открытые системы. 2015. № 1. С. 38-43.

30. Грибунин В.Г. Комплексная система защиты информации на предприятии / В.Г. Грибунин, В.В. Чудовский: учебное пособие рек. УМО вузов РФ. – Москва: Академия, 2013. – 416 с.

31. Гродзенский Я.С. Информационная безопасность: учебное пособие. - М.: РГ-Пресс. 2024. - 144 с.

32. Девянин П.Н. Постквантовые криптографические протоколы для систем защиты информации: монография / П.Н. Девянин [и др.]. – СПб.: Политехника, 2022. – 215 с. – ISBN 978-5-7325-1234-8.

33. Еремин А.Л. Информационная и цифровая гигиена. - М.: Лань. 2023. - 92 с.

34. Зайцев А.П. Технические средства и методы защиты информации: учебное пособие: рек. УМО вузов по образованию / А.П. Зайцев [и др.] – Москва: 2012. – 614 с.

35. Запечников С.В. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Том 1 – Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников [и др.] – Москва, 2011. – 536 с.

36. Защита информации в компьютерных системах: учеб. пособие / А.А. Симаков, А.В. Кургузов. - Омск: Омская академия МВД России, 2022. -108 с.

37. Зенков А.В. Информационная безопасность и защита информации. - М.: Юрайт, 2023. - 108 с.

38. Зенков А.В. Основы информационной безопасности: учебное пособие / А.В. Зенков. – Москва; Вологда: Инфра-Инженерия, 2022. – 104 с.: ил., табл.

39. Иванова С.В. Защита информации // СПС КонсультантПлюс. 2024.

40. Использование особенностей системного программного обеспечения для противодействия преступности в сфере информационно-телекоммуникационных технологий: учебное пособие / А.А. Дрога, С.Е. Савотченко, В.Л. Акапьев. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2023. – 76 с.

41. Исследование устойчивости российского сегмента интернета – 2023. Qrator Labs. – М.: ИКС Медиа, 2023. – 45 с.

42. Казарин О.В., Шубинский И.Б. Основы информационной безопасности: надежность и безопасность программного обеспечения. - М.: Юрайт, 2023. - 343 с.

43. Ковалева Е.Г. Системный подход к обеспечению информационной и экономической безопасности хозяйствующего субъекта / С.Е. Савотченко, В.Л. Акапьев // В сборнике: Проблемы информационного обеспечения деятельности правоохранительных органов. сборник статей IX Всероссийской научно-практической конференции. 2022. С. 142-146.

44. Комплекс виброакустической защиты «БАРОН». - URL: https://bezar.ru/zaschita-informacii-poiskovaya-tehnika/generatory-radioshuma-i-pomeh?product_id=898 (дата обращения 16.11.2025).

45. Комплексы для проведения акустических и виброакустических измерений СПРУТ-7М. – М.: ЗАО НПЦ фирма «НЕЛК», 2025.

46. Комплектация устройства Соната-Р2. Основные и дополнительные элементы: сертификат. – URL: // https://sertifikatru1.ru/sonata-r2-sertfstek-generator-radioshuma-i-pemin-td-videoglaz-moskva/ (дата обращения 16.11.2025).

47. Корабельников С.М. Преступления в сфере информационной безопасности. – М.: Юрайт, 2024. – 112 с.

48. Куприянов А.И., Мельников В.П. Информационная безопасность. Учебник. - М.: КноРус, 2022. - 268 с.

49. Левушкин А.Н. Обеспечение баланса интересов граждан, предпринимателей и публично-правовых образований как участников имущественных правоотношений в цифровом пространстве и защите информации // Вестник Тверского государственного университета. Серия: Право. 2022. № 4 (72). С. 81 – 90.

50. Лукацкий А. Законодательные требования РФ по информационной безопасности // URL: https://www.youtube.com/watch?v=qfxj-vHr5lU&t=1368s (дата обращения: 04.03.2025).

51. Максуров А.А. Обеспечение информационной безопасности в сети Интернет: монография. - М.: Инфра-М, 2023. - 226 с.

52. Малькольм М. Грокаем безопасность веб-приложений. – СПб.: Питер, 2025. – 336 с.: ил.

53. Нестеров С.А. Основы информационной безопасности. - М.: Лань. 2023. - 324 с.

54. Николаева М.О. Информационная безопасность: современная картина, проблемы информационной безопасности и защиты информации // Мониторинг. Образование. Безопасность. 2023. Т. 1. № 1. С. 51-57.

55. Новиков А.А. Уязвимость и информационная безопасность телекоммуникационных технологий / А.А. Новиков, Г.Н. Устинов: учебное пособие для вузов. – Москва: Радио и связь, 2012. – 296 с.

56. Организационная защита информации. Часть 1. Методологические основы организационной защиты информации: учебное пособие. - СПб.: Изд-во СПб ун-та МВД России, 2019. - 156 с.

57. Пестунова Т.М. Информационная безопасность и защита информации: краткое введение и практикум: учебное пособие / Т.М. Пестунова, А.А. Перов. – М.: РУСАЙНС, 2025. – 134 с.

58. Проблемы безопасности умного дома: учебное пособие / Е.А. Верещагина, А.Л. Золкин, А.С. Ярмонов. – М.: РУСАЙНС, 2025. – 104 с.

59. Прохорова О.В. Информационная безопасность и защита информации. – М.: Лань, 2025. – 124 с.

60. Развитие отечественных сетей связи пятого поколения: технологические вызовы и решения. – М.: ComNews, 2024. – 56 с.

61. Российский рынок интернета вещей: вопросы выбора стандарта и безопасности // ЦИПР-2023. URL: https://cipr.ru/izdanie-2023/rossijskij-rynok-

interneta-veshhej-voprosy-vybora-standarta-poiska-detalej-i-obespecheniya-bezopasnosti/ (дата обращения: 30.06.2025).

62. Рыженко С., Василенко В., Сидак А. Методы и средства защиты акустической речевой информации от утечки по техническим каналам: лабораторный практикум. – М.: Директ-Медиа, 2023. – 92 с.

63. Рынок интернета вещей в России: стратегии развития и безопасности / Росатом инфраструктурные решения. – М.: РИО, 2024. – 88 с. – Текст: электронный // Росатом. – URL: https://rosatom.cnews.ru/news/line/2024-12-13_issledovanie_rosatoma (дата обращения: 01.07.2025).

64. Савотченко С.Е. Информатизация правоохранительной деятельности в условиях цифровой трансформации общества / В.Л. Акапьев // В сборнике: Развитие информационных технологий органов внутренних дел Российской Федерации. Сборник научных трудов Всероссийская научно-практическая конференция. Москва, 2025. С. 82-91.

65. Савотченко С.Е. Нормативно-правовое регулирование защиты конфиденциальной геологической информации // В.А. Захаров, В.Л. Акапьев // В сборнике: Проблемы информационного обеспечения деятельности правоохранительных органов. Сборник статей 11-й Всероссийской научно-практической конференции. Белгород, 2024. С. 235-239.

66. Савотченко С.Е. Проблемы правового регулирования защиты конфиденциальной геологической информации / В.А. Захаров, В.Л. Акапьев // В сборнике: «Современные информационные технологии в профессиональной деятельности сотрудников органов внутренних дел». Сборник научных трудов по итогам Всероссийской научно-практической конференции. - Ростов-на-Дону, 2025. С. 5-12.

67. Савотченко С.Е. Терминологическо-образовательные аспекты реализации мер информационной безопасности детей в современном обществе / В.Л. Акапьев // Право и образование. 2023. № 12. С. 67-79.

68. Система виброакустической защиты SEL SP-157 Шагрень. – URL: https://detsys.ru/catalog/vibroakusticheskaya_zashchita/sel_sp_157/ (дата обращения 17.11.2025).

69. Скабцов Н. Kali Linux в действии. Аудит безопасности информационных систем. 2-е изд. – СПб.: Питер, 2024. – 384 с.: ил.

70. Сычев Ю.Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. – Москва: ИНФРА-М, 2023. – 201 с.

71. Тенденции искусственного интеллекта в кибербезопасности – 2025 / TAdviser Analytics. – М.: TAdviser, 2024. – 34 с. – *Текст: электронный* // TAdviser. – URL: https://www.tadviser.ru/index.php/Статья:Главные_тенденции_в_защите_информации (дата обращения: 01.07.2025).

72. Тенденции применения ИИ в кибербезопасности – 2025 / TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Главные_тенденции_в_защите_информации (дата обращения: 30.06.2025).

73. Физические основы защиты информации: учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. – М.: РИОР: ИНФРА-М, 2026. – 204 с.

74. Ховард Рик Кибербезопасность: главные принципы. – СПб.: Питер, 2024. – 320 с.: ил.

75. Хорев А.А. Техническая защита информации: учебное пособие для студентов вузов: в 3 т. – Т. 1. Технические каналы утечки информации / А.А. Хорев; под ред. Ю.Н. Лаврухина. – М.: НПЦ «Аналитика», 2008. – 436 с.

76. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие рекомендовано УМО по образованию. – Москва: Академия, 2013. – 256 с.

77. Чернова Е.В. Информационная безопасность человека: учебное пособие для вузов / Е.В. Чернова. – 3-е изд., перераб. и доп. – Москва: Юрайт, 2024. – 327 с.

78. Швечкова О.Г., Бабаев С.И. Информационная безопасность. Часть 1. Теоретические основы. Учебник. – М.: КУРС, 2022. – 144 с.

79. Швечкова О.Г., Бабаев С.И. Информационная безопасность. Часть 2. Теоретические основы. Учебник. – М.: КУРС, 2022. – 144 с.

80. Шевцов В.Ю. Программно-аппаратная защита локальных АРМ с использованием ПО Secret Net: учебно-методическое пособие / В.Ю. Шевцов, Е.В. Булгакова. – Москва; Вологда: Инфра-Инженерия, 2024. – 80 с.

81. Шостак А. Защита систем. Чему «Звездные войны» учат инженера ПО. – М.: Эксмо, 2025. – 444 с.

82. Ярочкин В.И. Информационная безопасность: учебник для вузов. – Москва: Академический Проект, 2014. – 544 с.

ПРИЛОЖЕНИЕ 1

Практикум: Разработка модели угроз (Threat Model) для мобильного приложения банка с учётом требований ФСТЭК

Задание: создайте модель угроз для мобильного приложения Сбера с учетом:

- требований 152-ФЗ (персональные данные);
- рисков импортозамещенного ПО;
- угроз квантового взлома.

Итоговый документ должен содержать полное описание архитектуры и матрицу угроз с привязкой в ФСТЭК.

Решение:

1) Классификация активов:
- аутентификационные данные (пин-код, пароль)
- биометрия клиентов (высокий риск);
- транзакционные данные;
- конфиденциальные документы;
- криптографические ключи.

2) Применение фреймворка MITRE ATT&CK.

3) Карта угроз
- угроза канала связи (T1557);
- угрозы, связанные с биометрией;
- угрозы квантового криптоанализа;
- угрозы импортозамещенного ПО.

4) Матрица приоритизации рисков

Угроза	Вероятность	Влияние	Уровень риска
Утечка биометрии	Средняя	Критическое	Высокий
Наличие бэкдора	Средняя	Критическое	Высокий
Спуфинг биометрии	Высокая	Высокое	высокий
DDoS на банковский API	Высокая	Среднее	Средний

Практическое задание для слушателей:

На основе примера с банком разработать модель угроз для:

1. облачного сервиса организации;
2. системы здравоохранения (РФ).

Решение (пример 1):

На основе анализа технологий, архитектуры и регуляторных особенностей VK Cloud Solutions разработана комплексная модель угроз с использованием фреймворка STRIDE и требований ФСТЭК/152-ФЗ. Модель структурирована по компонентам сервиса, источникам угроз и мерам противодействия.

1. Контекст облачного сервиса VK Cloud Solutions.

Модель услуг: IaaS/PaaS/SaaS.

Ключевые компоненты:

- виртуальные машины (KVM, OpenStack);
- управляемые Kubernetes и базы данных (MySQL, Vertica);
- S3-хранилища, Data Lakehouse (Cloud Trino).

Регуляторный статус: аттестован по 152-ФЗ (УЗ-1), ГОСТ Р 59533, ISO 27001/27017.

2. Модель угроз по фреймворку STRIDE.

Spoofing (маскировка).

Угрозы:

- компрометация учетных записей администраторов через фишинг;
- подделка API-ключей Cloud Trino/MeiliSearch.

Меры:

- многофакторная аутентификация (MFA) и ротация ключей;
- сертифицированные криптошлюзы (ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ 34.11-2012, ГОСТ 34.11-94, ГОСТ 28147-89, ГОСТ 34.12-2018 (ГОСТ Р 34.12-2015), ГОСТ 34.13-2018 (ГОСТ Р 34.13-2015));

Tampering (изменение данных).

Угрозы:

- манипуляции с данными в S3-хранилищах или Data Lakehouse 4;
- изменение конфигураций ВМ через уязвимости Hypervisor 2.

Меры: цифровые подписи ГОСТ Р 34.10-2012 + контроль целостности журналов.

Repudiation (отказ от действий).

Угрозы: отсутствие аудита операций с персональными данными в ИСПДн.

Меры: SIEM-системы с сохранением логов ≥1 года (требование ФСТЭК №21).

Information Disclosure (Раскрытие информации)

Угрозы:

- утечки из-за ошибок конфигурации S3-корзин (публичный доступ);
- компрометация данных в Kubernetes (AlmaLinux ноды).

Меры: шифрование данных по ГОСТ 28147-89 + DLP-системы.

Denial of Service (отказ в обслуживании).

Угрозы:

- DDoS-атаки на API-шлюзы или BGP-маршрутизацию;
- перегрузка Cloud Trino при ETL-процессах.

Меры:

- Anti-DDoS с фильтрацией трафика + резервирование каналов.

Elevation of Privilege (повышение привилегий).

Угрозы: эксплуатация уязвимостей в OpenStack/Kubernetes; злоупотребление правами в сервисах Managed Kubernetes.

Меры: патчинг + принцип минимальных привилегий (RBAC).