O‘QUV ADABIYOTINING NASHR RUXSATNOMASI

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining 2023-yil 29-avgustdagi 895-22-sonli buyrug‘iga asosan

N.S.Yuldasheva, O.N.Mavlonov, D.J.Sodiqova,

(muallif familiyasi, ismi-sharifi)

R.SH.Meliqoziyev, M.A.Shakarov

5330300-“Axborot xavfsizligi (sohalar bo‘yicha)”

(ta’lim yo‘nalishi(mutaxassisligi))

ning talabalari (o‘quvchilari) uchun tavsiya etilgan

Политика кибербезопасности

(O‘quv adabiyotlar nomi va turi: darslik, o‘quv qo‘llanma)

O‘quv qo‘llanma ga

O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan litsenziya berilgan nashriyotlarda nashr qilishga ruxsat beriladi

Rektor _____ **B.Sh. Maxkamov**

(imzo)

M.O‘

Ro‘yxatga olish raqami
№ 2023-087

РЕСПУБЛИКА УЗБЕКИСТАН
МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ, НАУКИ И ИННОВАЦИ

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛЬ-ХОРАЗМИ

Н.С.ЮЛДАШЕВА, О.Н.МАВЛОНОВ, Р.Ш.МЕЛИКУЗИЕВ
Д.Ж.СОДИ КОВА, М.А.ШАКАРОВ

ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ

(Руководство)

Рекомендовано Министерством высшего образования, науки и инноваций Республики Узбекистан в качестве учебного пособия для студентов высшего учебного заведения «5330300 - Информационная безопасность (по отраслям)»

ТАШКЕНТ-2024

УДК: 004.056 (075.8)
ББК 74.90

Юлдашева Н.С., Мавлонов О.Н., Содиқова Д.Ж., Меликозиев Р.Ш. М. А. Шакаров Политика кибербезопасности. Методическое пособие. 2024. –292 стр.

Учебное пособие посвящено рассмотрению таких важных вопросов, как актуальность и важность концепции политики в области кибербезопасности, охватывающей административные, аппаратные и программные политики, используемые в информационных системах и технологиях. В частности, в учебном пособии освещены понятие, эволюция, цели кибербезопасности, необходимые документы и каталоги для лиц, принимающих решения, международные подходы к разработке политики кибербезопасности, национальное законодательство, значение геополитики в обеспечении кибербезопасности, вопросы внедрение и разработка политики кибербезопасности, корпоративной, роли отдельных лиц и правоохранительных органов в обеспечении кибербезопасности, политик в информационных системах и процессах их управления,

Учебное пособие 5330300 – Информационная безопасность (по направлениям) предназначено для бакалавров, обучающихся по специальностям, и может быть использовано широким кругом специалистов, деятельность которых связана с обеспечением информационной безопасности.

УДК: 004.056 (075.8)
ББК 74.90

Рецензенты:

Х.К.Самаров - доцент кафедры «Информационная безопасность» Ташкентского университета информационных технологий имени Мухаммада Аль-Хоразми.

Н.Б. Насруллаев –Исполняющий обязанности директора Нурафшанского филиала Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми, кандидат технических наук, доцент.

ISBN 978-9910-9339-1-2

© Н.С.ЮЛДАШЕВА, 2024
© «Ilm ziyo zakovat», 2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ…….. 5

1. ОБЩИЕ СВЕДЕНИЯ О ПОЛИТИКЕ КИБЕРБЕЗОПАСНОСТИ…… 7

1.1. Концепция политики кибербезопасности и введение в науку…… 7

1.2. Эволюция кибербезопасности……... 16

1.3. Цели кибербезопасности…..... 24

Вопросы самоконтроля……..... 34

2.КАТАЛОГ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ..... 36

2.1 Руководство для лиц, принимающих решения..... 36

2.2 Подход каталога..... 55

2.3 Каталог политики кибербезопасности..... 62

Вопросы самоконтроля..... 116

3. ПОДХОДЫ К ПОЛИТИКЕ КИБЕРБЕЗОПАСНОСТИ. ГЕОПОЛИТИКА И КИБЕРБЕЗОПАСНОСТЬ..... 118

3.1 Политика кибербезопасности: подход США..... 118

3.2 Политика кибербезопасности: подход России..... 130

3.3 Политика кибербезопасности: узбекский подход..... 155

3.4 Геополитика и кибербезопасность..... 171

Вопросы самоконтроля..... 186

4.ПРИМЕНЕНИЕ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ…… 188

4.1 Реализация и разработка политики кибербезопасности.. 188

4.2 Отношение корпораций к киберпреступности..... 203

4.3 Роль отдельных лиц в предотвращении 214

кибербезопасности……..
Вопросы самоконтроля..... 223
5. ПОЛИТИКИ В УПРАВЛЕНИИ И ИСПОЛЬЗОВАНИИ..... 224
5.1 Роль правоохранительных органов в предотвращении кибербезопасности..... 224
5.2 Политики в управлении данными..... 232
5.3 Политики в использовании систем..... 242
Вопросы самоконтроля..... 248
6. ИНФОРМАЦИЯ О БЕЗОПАСНОСТИ..... 250
6.1 Ресурсы по технологиям безопасности..... 250
6.2 Инструменты кибербезопасности..... 263
6.3 Обучение сотрудников технике безопасности..... 274
Вопросы самоконтроля..... 281
ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА..... 287

Введение

В современную цифровую эпоху, когда технологии пронизывают все стороны нашей жизни, на первый план вышла безопасность информации и информационных систем. Хотя быстрое развитие технологий принесло много преимуществ, оно также подвергло нас новым и постоянно меняющимся угрозам. В результате потребность в эффективной политике кибербезопасности никогда не была выше, чем сегодня.

Этот учебник служит руководством, которое пытается ответить на ряд вопросов в понимании и применении на практике сложной области политики кибербезопасности. Он разработан, чтобы дать вам прочную основу для принципов, практики и проблем разработки и реализации политик кибербезопасности. Область политики кибербезопасности динамична и постоянно развивается. То есть появляются новые угрозы, развиваются технологии и, конечно же, актуализируются и регламенты. Этот учебник поможет вам получить знания и навыки, необходимые для адаптации к этим изменениям, и подготовит вас к разработке надежной и эффективной политики кибербезопасности.

Хотя это учебное пособие считается технологической дисциплиной, вы можете видеть, что оно было разработано в отношении национальных и международных правовых областей, геополитики, управления и других типов дисциплин. Обеспечивает всестороннее понимание многогранного характера политики кибербезопасности, от основ кибербезопасности и принципов формирования политики до управления рисками, правовых и этических соображений и международного сотрудничества. Его также можно использовать в качестве ресурса для практиков, политиков и всех, кто интересуется пониманием важной роли политики кибербезопасности в обеспечении безопасности нашего цифрового мира.

Темы включают в себя примеры из реальной жизни, международный опыт и подходы, а также наводящие на размышления вопросы, которые помогут улучшить ваш учебный опыт. Эти элементы помогут вам применить изученные концепции и развить практическое понимание того, как политики кибербезопасности работают в различных контекстах.

Поскольку в нашей республике продолжается развитие информационных технологий как в государственном, так и в

хозяйственном управлении, особое внимание уделяется обеспечению информационной безопасности. Это внимание ярко проявляется в различных инициативах, в том числе в постановлении Президента Республики Узбекистан от 8 февраля 2017 года «О мерах по коренному совершенствованию системы распространения нормативно-правовых документов». Кроме того, в Стратегии действий по дальнейшему развитию Республики Узбекистан на 2017-2021 годы особое внимание уделяется вопросу обеспечения информационной безопасности, особое внимание уделяется совершенствованию системы защиты информации, оперативному и адекватное реагирование на угрозы в информационном поле. Несомненно, успешная реализация этих задач является решающим фактором нашей политики.

Настоящее учебное пособие рекомендуется для бакалавров, обучающихся по специальности 60610300 - «Информационная безопасность», и может быть использовано широким кругом специалистов, деятельность которых связана с информационной безопасностью.

ГЛАВА I. ОБЩАЯ ИНФОРМАЦИЯ О ПОЛИТИКЕ КИБЕРБЕЗОПАСНОСТИ

§ 1.1. Введение в концепцию и науку политики кибербезопасности

Развитие современных методов обработки, передачи и сбора информации приводит к увеличению угроз, связанных с потерей, нарушением и разглашением информации о пользователях. Поэтому обеспечение информационной безопасности в компьютерных системах и сетях является одним из ведущих направлений развития информационных технологий.

Даже люди, работающие в индустрии безопасности, по-разному относятся к кибербезопасности в зависимости от аспектов киберпространства, с которыми они лично взаимодействуют. Независимо от того, является ли система физическим объектом или набором компонентов киберпространства, роль специалиста по безопасности, назначенного для этой системы, заключается в планировании и подготовке к потенциальной атаке. Хотя слово «кибер» в основном используется на просторечии, трудно точно понять, что оно означает. Научно-фантастический термин, основанный на зарождавшейся в то время области компьютерного управления и связи, когда-то известной как кибернетика, теперь относящейся к электронной автоматизации (Safire 1994).

Чтобы системы выполняли свои задачи, 3 оператора должны следовать установленным процедурам. Применительно к безопасности это трио подчеркивает, что безопасность не может быть обеспечена только профессионалами в области безопасности и что кибербезопасность не может быть достигнута только с помощью технологий. Решения и действия защищаемой системы или организации должны включать в себя другие человеческие элементы, которые играют решающую роль в успехе программ обеспечения безопасности. Даже если у всех этих людей есть мотивация и заинтересованность в том, чтобы оставаться в безопасности, они не знают, как работать вместе для предотвращения, выявления и восстановления после вреда без заранее спланированного процесса. И так,

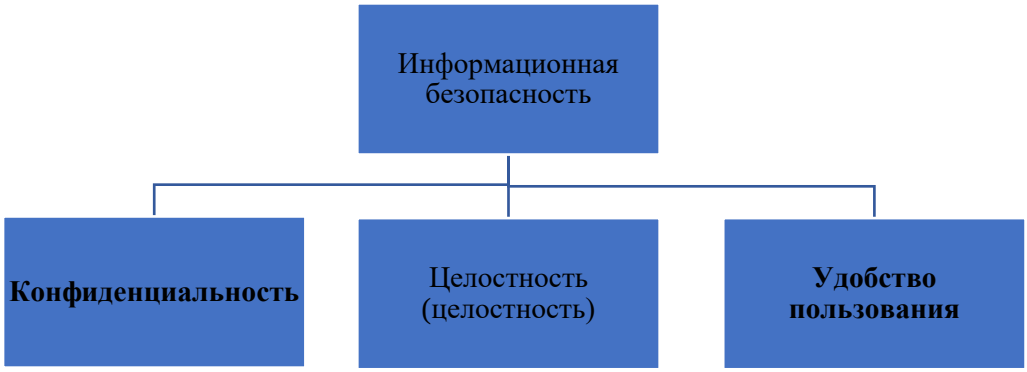


Рисунок 1.1.Цели информационной безопасности

Цели информационной безопасности включают:

1. Конфиденциальность;
2. Целостность (целостность);
3. Удобство использования.

Конфиденциальность– Эти правила гарантируют, что информация «читается» только законными пользователями, и понимается возможность ограничения распространения системной информации разрешенными видами использования.

Целостность (целостность)– относится к способности поддерживать подлинность, точность и источник записанных и представленных данных, т. е. защищать информацию от несанкционированного изменения или «записи».

Удобство использования- обеспечение точности и достоверности информации, означающей своевременную доставку функционала, доступность данных, информации и систем, то есть защиту от несанкционированного «исполнения».

Эти цели информационной безопасности применялись к информации еще до появления компьютеров, но появление киберпространства изменило способы достижения целей, а также относительную сложность их достижения. Технологии, поддерживающие конфиденциальность, целостность (целостность), удобство использования, часто конфликтуют друг с другом. Например, усилия по обеспечению высокой доступности данных в киберпространстве часто затрудняют обеспечение конфиденциальности данных.

Разобраться в том, что означают конфиденциальность, целостность (целостность) и удобство использования для каждого типа данных в конкретной системе, является специальностью специалиста по кибербезопасности. Кибербезопасность в целом относится к использованию людей, процессов и технологий для

предотвращения, обнаружения и восстановления конфиденциальности, целостности и удобства использования информации в киберпространстве.

Киберпространство повысило производительность всего общества, эффективно и своевременно распространяя информацию. Независимо от отрасли или приложения, в котором реализовано киберпространство, ключевым направлением является повышение эффективности. Быстрая доставка информации в киберпространство часто снижает безопасность всей системы. Для специалистов по производительности меры безопасности часто расходятся с прогрессом из-за превентивных мер, которые сокращают, останавливают или задерживают доступ пользователей, мер обнаружения, которые потребляют критически важные системные ресурсы, и требований реагирования, которые отвлекают внимание руководства от системных функций.

Слово «политика» применяется к множеству ситуаций, связанных с кибербезопасностью. Он использовался для обозначения законов и правил, касающихся распространения информации, целей частного предпринимательства для защиты информации, методов компьютерных операций для управления технологиями и переменных конфигурации в электронных устройствах. Но в литература есть много других способов использования фразы «политика кибербезопасности». Как и в случае с термином «киберпространство», единого определения не существует, но когда термин «кибербезопасность» используется в качестве политики, он используется как общая тема.

Цель этого руководства — предоставить читателю достаточную информацию для понимания и размышлений о предмете и его производных. Те, кто читает ее, должны уверенно раскрыть многие типы политик кибербезопасности. В общем, термин «политика кибербезопасности» относится к руководящим принципам, разработанным для обеспечения кибербезопасности.

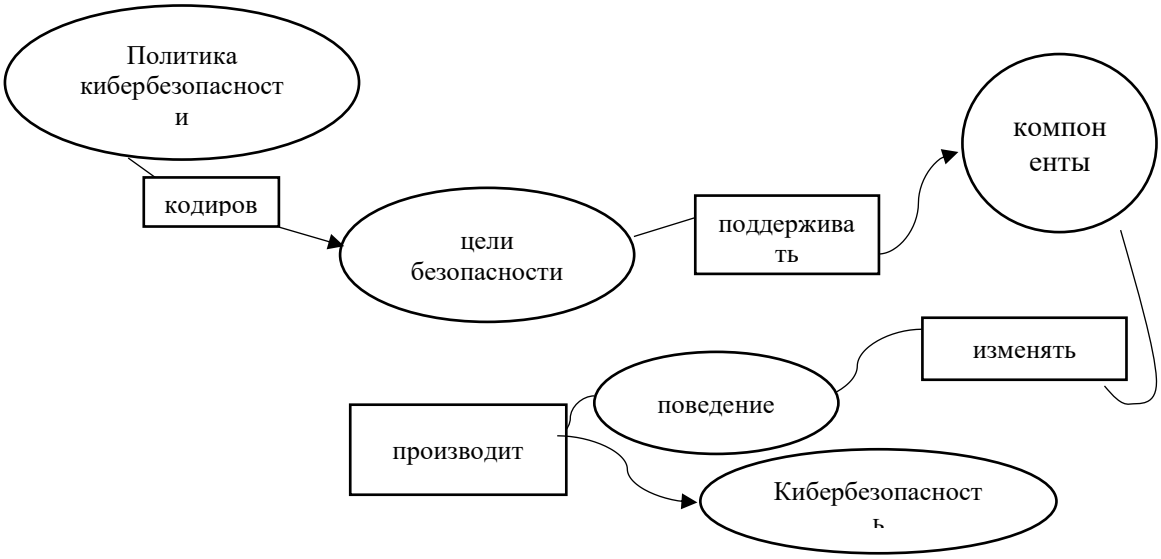


Рисунок 1.2. Определение политики кибербезопасности.

Ожидается, что опора примет взгляд непрофессионала на концепцию. Другие перспективы определяемого понятия могут быть выражены как дополнительные перспективы сложного понятия. На рис. 1.2 политика кибербезопасности представлена как важный аспект, кодифицирующий цели безопасности для поддержки компонентов, которые, как ожидается, изменят свое поведение в соответствии с политикой кибербезопасности. Рисунок 1.3 иллюстрирует концепцию, объединяющую различные подходы к политике кибербезопасности. Хотя не все дополнительные узлы и ссылки входят в определение политики кибербезопасности, они дают представление о структуре, показанной в основной части блок-схемы на рис. 1.2. 1. На рис. 3 ссылки на узел «руководящие органы» указывают на то, что политики кибербезопасности принимаются руководящими органами как способ достижения целей безопасности. Это число преднамеренно является общим, поскольку руководящие органы часто существуют вне организаций, которыми они управляют. Например, рисунок 1.3.

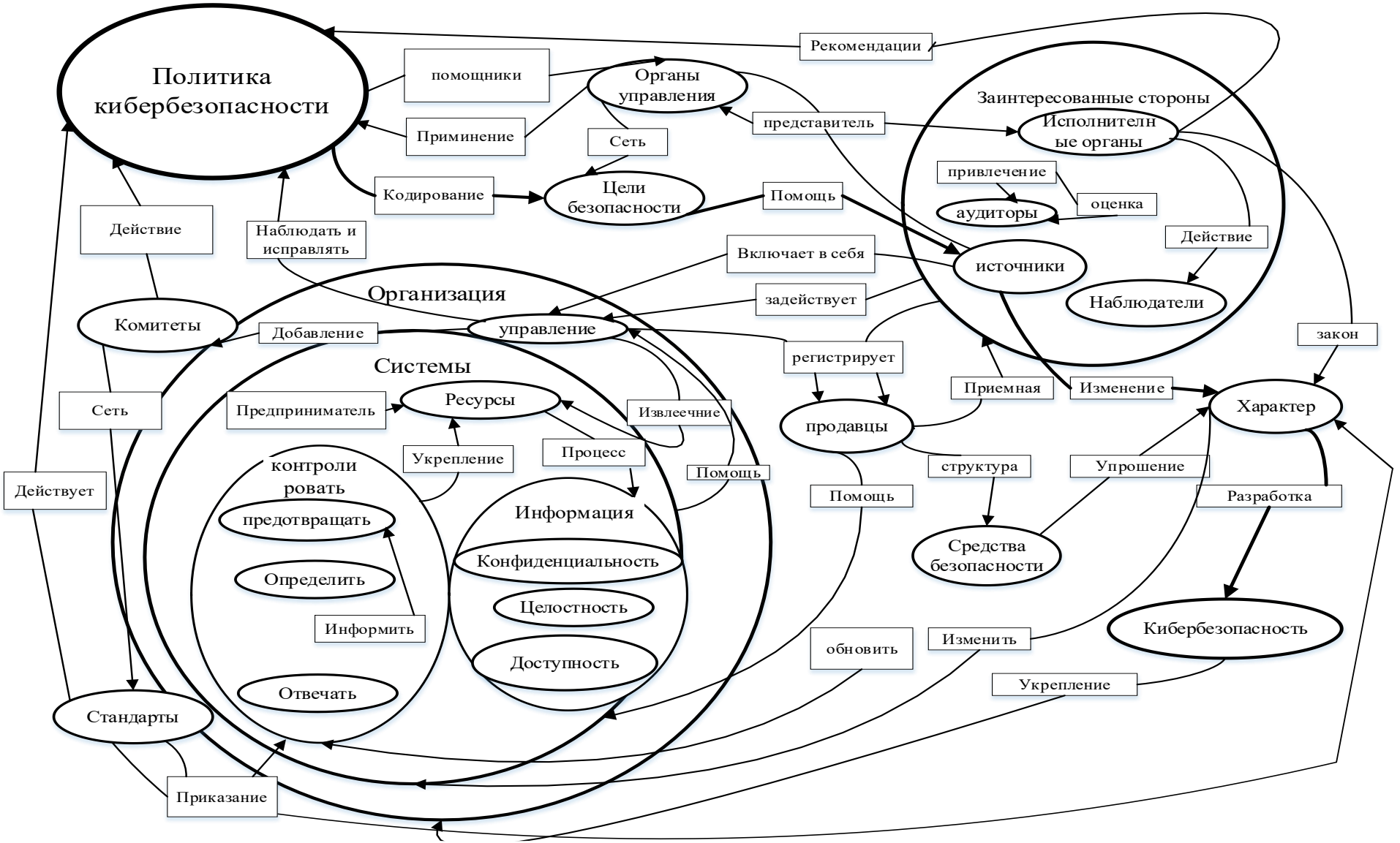


Рисунок 1.3. Перспективы политики кибербезопасности

Обратите внимание, что, как показано на рис. 1.3, роль политики состоит в том, чтобы обеспечить структуру для определения правил поведения, необходимых для достижения кибербезопасности. Существует множество кибердоменов с различными заявлениями о политике и соответствующими правилами. Эти домены подробно показаны на рис. 1.3.

Цели кибербезопасности не зависят напрямую от поведения, но ожидается, что стратегия кибербезопасности, основанная на целях кибербезопасности, приведет к улучшению политики кибербезопасности. Организации создают стандарты для внедрения средств управления технологиями и связанных с ними операционных процессов, а компоненты используют эти стандарты для соблюдения политик. Сами по себе стандарты не являются политикой. Скорее, они относятся к набору технологий и операционных процессов для целей политики. Если стандарт фокусируется на соблюдении политики, он определяет комбинацию конфигурации процесса и технологии, которая обеспечивает соответствие политике. Однако могут быть выпущены стандарты, которые не касаются какой-либо конкретной цели политики, а политики могут не содержать соответствующих стандартов.

Перспективы политики кибербезопасности.Ссылки из узла «Принудительные органы» показывают роль силовых структур, которые устанавливают правила, влияют не только на поведение учредителей, но и на других, тем самым воздействуя на стейкхолдеров политики — это процесс, который превращается в стороны. Ссылки на крайней левой стороне признают роль стандартов, установленных руководством организаций, которые связаны политикой руководящих органов. Ссылки из узла с пометкой «Поставщики» описывают отношения поставщиков компонентов и управления, которые влияют и влияют на поставщиков, которые предоставляют инструменты соответствия политике безопасности и поддерживают безопасность системы с помощью продуктов и услуг.

Кластеры узлов и ссылки внутри узла «Организации» и связанные с ним относятся к организации, на которую распространяется политика. Это указывает на то, что такие организации придерживаются политик кибербезопасности, опубликованных органами управления, а также устанавливают свои собственные внутренние политики кибербезопасности. Это также

показывает, что управление организацией поддерживается системами, на которые распространяется политика безопасности.

Узел «Системы» относится к системам, используемым для управления киберпространством, подчеркивая взаимосвязь между управлением безопасностью и системными ресурсами. Это указывает на то, что существует компромисс между системными ресурсами, выделенными для мер безопасности, и ресурсами, необходимыми для обработки информации; то есть, чем больше процессов управления безопасностью интегрировано в работу системы, тем меньше вероятность потери ресурсов. Типичной целью внутренней стратегии кибербезопасности организации является оптимизация этой договоренности с использованием документированной политики в качестве инструмента связи для информирования о том, что такие решения были приняты.

Законы и правила.Политика кибербезопасности каждой страны теперь является частью ее политики национальной безопасности. Хотя национальная политика кибербезопасности считается такой же, как внешняя политика или экономическая политика, эти политики не имеют такой же силы закона. Скорее, политика устанавливается и выражается через отчеты и речи, беседы и переговоры. Политика используется для принятия решения о том, какие законы и правила следует учитывать. Это не относится к самим законам и правилам. Конечно, мировые договоры, законы и постановления отражают самую лучшую и продуманную политику. Однако можно иметь исполнительные директивы, законы и постановления по кибербезопасности, вообще не формулируя политику кибербезопасности. Например, Китай ясно дал понять, что деятельность в киберпространстве, имеющая решающее значение для деятельности национального государства, должна контролироваться . В этой политике четко определено, что Интернет служит интересам экономики и государства. Эта политика привела к принятию законов и правил, которые позволяют китайскому правительству изолировать, отслеживать и контролировать телекоммуникации, а также блокировать доступ к веб-сайтам, которые, по его мнению, противоречат его интересам.

Независимо от того, разработало правительство политику кибербезопасности или нет, его правила кибербезопасности ограничены сферой деятельности правительства. То есть ветвь или агентство правительства находятся в рамках любой нормативно-

правовой базы штата, и поэтому ее политика и правила должны соответствовать этой более широкой структуре. Филиал или агентство может создавать новые законы только для своего избирательного округа и в рамках своего собственного устава. Например, политика кибербезопасности, выпущенная отраслевым регулирующим органом, будет применяться только к его области регулирования. Регулятор энергетики может потребовать от энергетического объекта резервирования, но не может требовать от поставщиков телекоммуникационных услуг прокладки резервных кабелей к каждому энергетическому объекту.

Политика компании.Организации частного сектора, как правило, не так ограничены, как правительства, в преобразовании политики высшего руководства в действенные правила. В корпоративной среде соблюдение политики обычно ожидается под угрозой санкций, вплоть до увольнения. Например, кадровая, юридическая или бухгалтерская политика защищены до такой степени, что любые случаи несоблюдения могут быть основанием для увольнения. Когда менеджеры среднего звена поддерживают такие процессы, как прием на работу или оплата расходов, они могут согласовать деятельность отдела с этими политиками и часто должны устанавливать меры отдела для соблюдения требований. Как и в случае с правительством, любая такая подорганизация подлежит ограничениям с точки зрения полномочий. Хотя есть исключения, когда к классификации информации относятся очень серьезно, корпоративная политика безопасности, изданная генеральным директором, обычно применяется ко всей корпорации, а политика, издаваемая директором по информационным технологиям, обычно применяется только к техническим сотрудникам. Недавним изменением в организационной среде является назначение главного сотрудника по информационной безопасности или главного сотрудника по безопасности, который отвечает за отдельные аспекты состояния безопасности организации.

Разница между большинством корпоративных политик кибербезопасности и политиками, издаваемыми юридическим отделом или отделом кадров, заключается в том, что политики кибербезопасности часто ставят оценку рисков кибербезопасности посередине. Основной причиной этого являются менеджеры, которые не знакомы с концепциями кибербезопасности или

управления рисками.

Например, в политике кибербезопасности может быть указано, что «при наличии высокого риска нарушения конфиденциальности информации информация не должна передаваться поставщику без тщательной проверки способности поставщика защитить информацию». Этот тип политики оставляет оценку информационного риска менеджеру, который может быть заинтересован в снижении затрат за счет аутсорсинга части информационного потока отдела. Чтобы еще больше сократить эти расходы, может быть принято решение о том, что тот же самый менеджер не требует проведения комплексной проверки.

Технологическая конфигурация.Поскольку многие стандарты работы технологий реализуются с использованием специального программного обеспечения и устройств безопасности, операторы технологий обычно ссылаются на техническую конфигурацию этих устройств, как это определено стандартом, как на «политику безопасности». Эти спецификации были реализованы на протяжении многих лет поставщиками и поставщиками услуг, которые разработали технические конфигурации вычислительных устройств, которые позволяют системным администраторам заявлять о соответствии различным стандартам. Это побудило поставщиков обозначить альтернативные технические конфигурации для своих продуктов как «политики безопасности». Маркетинговая литература поставщика "политика" этих технических конфигураций.

Стратегия против политики.Политика в области кибербезопасности формулирует стратегию достижения целей в области кибербезопасности и предоставляет ее участникам рекомендации по надлежащему использованию мер кибербезопасности. Направление может быть установлено общественным соглашением или руководящим органом. Мы также признаем, что независимые компании должны установить руководящие принципы управления для поддержки своей стратегии кибербезопасности, и мы используем модифицированный термин «политика предприятия» для обозначения только тех политик, которые применяются в конкретном корпоративном сообществе. Как правило, такие корпоративные политики часто основаны на стандартах кибербезопасности, установленных Международной организацией по стандартизации (ISO) (ISO/IEC 2005 a,b) и NIST

(Ross, Katzke et al. 2007), которые сами по себе не являются политиками. Такие стандарты обычно включают сочетание технологических указаний с рекомендациями по технологическому контролю. Руководство по процессу рекомендует задать политику, но ее нельзя назвать прямой политикой.

В том смысле, что все политики отличаются от стандартов реализации, к которым они применяются, политики могут быть спекулятивными, поскольку простое принятие политик не гарантирует наличия правильных правил для достижения целей безопасности. Без четкого концептуального представления о влиянии кибербезопасности будет сложно разработать стратегию кибербезопасности и соответствующие политики. Даже когда существует широкое соглашение о механизмах применения политики и его можно напрямую проследить до директив политики, коллективное суждение может быть ошибочным, и эти механизмы могут не соответствовать целям политики безопасности.

Ключом к формулированию политики кибербезопасности является признание того, что решения по управлению безопасностью принимаются независимо от наличия формальной политики, понимание того, что политика является подходящим инструментом для управления несколькими независимо принимаемыми решениями в области безопасности, и понимание того, как решения в области безопасности влияют на безопасность. Процесс разработки стратегии заключается в том, чтобы узнать как можно больше о том, что он делает.

§ 1.2. Эволюция кибербезопасности

Чтобы понять политику кибербезопасности, нам нужно понять, как развивалась кибербезопасность. Когда компьютеры запустили первые автоматизированные процессы, основной целью всех таких проектов было повышение производительности за счет замены людей-калькуляторов автоматизированными программами, которые давали более точные результаты. Чем больше программного обеспечения доступно, тем больше увеличивается производительность компьютеров. Внедрение Интернета еще больше повысило производительность за счет более быстрой и точной передачи данных. Это напрямую привело к возможности обрабатывать бизнес-транзакции в режиме онлайн. Эта способность была названа электронной коммерцией. К 2000 году экономика стала настолько зависеть от электронной коммерции, что он стал частой

мишенью для киберпреступников, и технологии безопасности развились для защиты данных, которые могут быть использованы для выполнения мошеннических операций. Такие технологии обычно называют мерами противодействия, поскольку они представляют собой меры безопасности, предназначенные для противодействия конкретной угрозе. Сегодня достижения в области технологий кибербезопасности привели к глобальной гонке кибервооружений, в которой меры противодействия отстают.

Производительность.История кибербезопасности начинается с мэйнфреймов в 1960-х годах. Это был первый компьютер, который был достаточно дешевым, чтобы предприятия могли окупить вложения в свои системы электронной обработки данных. До этого слово «компьютер» относилось к человеку, производящему вычисления, а слово «кибер» было областью научной фантастики. В те времена компьютеры охранялись охраной и специальными методами. Процедуры физической безопасности предназначены для обеспечения того, чтобы только уполномоченные лица имели физический доступ к компьютерам. Компьютеры были настолько большими, что сотни квадратных футов пространства пришлось приспособить для использования специальным персоналом службы безопасности. Функция охранника иногда совмещалась с ролью оператора ЭВМ и называлась специалистом по ведению дел. Люди, которым нужно было использовать компьютер, хранили свои данные и программы на стопках перфокарт и стояли в очереди перед охранником. Охранник проверяет доступ пользователя к компьютеру, берет стопку карт и помещает ее в устройство чтения карт, которое автоматически переводит слоты на картах в биты и байты (Шахт, 1975). К концу 1960-х можно было получать перфокарты из нескольких офисов, подключенных к главному компьютеру через удаленное соединение. Затем на персонал компьютерной безопасности была возложена дополнительная ответственность за прокладку этих кабелей под фальшполами, через пустоты в стенах и каналы передачи, чтобы гарантировать, что на другом конце сидит уполномоченное лицо.

Руководители этих первых автоматизированных компьютерных систем прекрасно осознавали риски безопасности, но триада конфиденциальности, целостности и удобства использования еще не стала отраслевым стандартом. За исключением нескольких устройств в вооруженных силах и разведке, конфиденциальность не

была основным требованием безопасности. Хотя компании хотели сохранить конфиденциальность своих списков клиентов, непроверенное программное обеспечение всегда терпело неудачу, поэтому их главной заботой была целостность, а не конфиденциальность. Возможность человеческой ошибки, которая может привести к катастрофическим ошибкам в целостности данных, всегда была присуща разработке и эксплуатации компьютерного программного обеспечения.

Организации, занимающиеся разработкой программного обеспечения, первыми подняли тревогу безопасности, когда компьютеры стали управлять системами, сбои в работе которых могли быть опасными для жизни (Ceruzzi, 2003). Кроме того, к началу 1970-х компьютерные преступления в форме финансового мошенничества стали обычным явлением, что сделало их популярными в художественной литературе и на телевидении (McNeil, 1978). Даже если мы предположим, что человеческий фактор исключен из числа угроз безопасности, известно, что системные сбои происходят невинно с тех пор, как была обнаружена первая реальная ошибка между электронными лампами компьютерной системы (Слейтер, 1987, стр. 223). В 1970-х перфокарты были заменены электронным вводом и выводом через клавиатуру и терминалы. Кабели и терминалы еще больше расширили диапазон, в котором авторизованные пользователи могли сидеть во время обработки данных. Системная безопасность была расширена и теперь включает отслеживание кабелей через стенные перегородки и транки, чтобы гарантировать, что кабели заканчиваются в офисах, занятых авторизованными пользователями компьютеров. Это позволило людям в офисах, расположенных далеко от реального компьютера, подключаться к порту ввода-вывода и использовать его со своего рабочего стола. Охранник остался у двери компьютерного зала, но в основном для проверки посетителей или поставщиков услуг по обслуживанию, которые бродили по компьютерному залу. Информационная безопасность перешла в область настраиваемой бизнес-логики.

Пользователям назначаются имена для входа в систему, связанные с меню, которые предоставляют экраны, необходимые для выполнения их рабочих функций. В результате большинство пользователей увидят один и тот же главный экран, но разным пользователям будут доступны разные поля данных и пункты меню.

Экраны ограничены бизнес-логикой, закодированной в программном обеспечении. Например, если у клерков есть экран обслуживания клиентов, они могут просматривать записи клиентов, но не могут изменять свой баланс. Однако экраны бизнес-логики часто содержат переопределения. Например, супервайзер, наблюдающий за сотрудником службы поддержки клиентов, может ввести специальный код, чтобы разрешить единовременное изменение баланса через ограниченную функциональность экрана. Широкое использование компьютеров, работающих с использованием технологии клавиатуры, привлекло внимание к проблеме контроля конфиденциальности. Возросло использование военных и разведывательных компьютеров. Финансируемые государством исследования в области криптографии разработали несколько алгоритмов, которые преобразуют данные в нечитаемые форматы с использованием длинных последовательностей битов, называемых «ключами», которые блокируют и разблокируют данные. Возросло использование военных и разведывательных компьютеров. Финансируемые государством исследования в области криптографии разработали несколько алгоритмов, которые преобразуют данные в нечитаемые форматы с использованием длинных последовательностей битов, называемых «ключами», которые блокируют и разблокируют данные. Возросло использование военных и разведывательных компьютеров. Финансируемые государством исследования в области криптографии разработали несколько алгоритмов, которые преобразуют данные в нечитаемые форматы с использованием длинных последовательностей битов, называемых «ключами», которые блокируют и разблокируют данные.

Такие криптографические алгоритмы основаны на диффузии, распространении сообщения в статистически более длинные и неоднозначные форматы и запутывании, при котором отношения между зашифрованным сообщением и соответствующим ключом должны быть очень отдаленными и предсказуемыми (Шеннон, 1949). Однако достижения в области вычислительной мощности значительно повысили способность решительного противника определять взаимосвязь между сообщениями и ключами. Было легко представить себе день, когда существующие автоматизированные криптографические методы не будут настолько изощренными, чтобы сломать автоматизированный статистический анализ (Грэмпп

и Макилрой, 1989). Налоговая служба,

Признавая растущие требования к конфиденциальности, но не имея возможности их удовлетворить, Национальное бюро стандартов США (теперь Национальный институт стандартов и технологий [NIST]) начало работать над достижением этой цели.

В 1974 году Закон США о компьютерной безопасности (Закон о конфиденциальности) стал первым законом, призванным установить контроль над распространением информации. Документ охватывал только использование компьютеров правительством и только то, что сегодня известно как информация, позволяющая установить личность (PII). Но он выделил конфиденциальность и связанные с ней усилия по улучшению технологии шифрования в качестве ключевых целей кибербезопасности. По мере развития технологий в 1970-х годах мини-компьютеры, такие как DEC PDP-11, часто заполняли мэйнфреймы крупных компаний и вскоре нашли свое применение в малых предприятиях, которые теперь могли автоматизировать офисные задачи, такие как обработка текстов. Для тех, кто все еще не может позволить себе компьютер любого размера, технически подкованные предприниматели запустили услуги, которые позволяют людям арендовать компьютер на определенный период времени. Их называли «услугами с разделением времени», потому что компании, занимающиеся этим бизнесом, взимали плату со своих клиентов в зависимости от времени, которое они провели за своими компьютерами.

После того, как технологии терминалов и клавиатур позволили протянуть устройства ввода-вывода по кабелям, они использовали технологию аналоговой модуляции и демодуляции (модемы и мультиплексоры), чтобы расширить зону действия компьютерного терминала за пределы стен здания с помощью обычных телефонных линий. Эти компании начали специализироваться по отраслям, разрабатывая сложное программное обеспечение, такое как расчет налога на заработную плату и расчет коммерческой аренды.

Разработка такого программного обеспечения является программным обеспечениемвряд ли удастся добиться успеха в анализе затрат и выгод для компании, не занимающейся бизнесом, но это был трудоемкий ручной процесс, управляемый многими предприятиями. Службы разделения времени позволяли отделам, которые не были основной частью бизнеса, использовать автоматизацию, даже если для этого им требовался доступ к чужому

компьютеру. Сегодня эти услуги доступны через Интернет, но модели их оплаты изменились, и они больше не называются «разделением времени», а «облачными вычислениями».

Эти службы с разделением времени взимают плату за вычислительные ресурсы в зависимости от активности пользователя, поэтому у них должен был быть способ идентифицировать пользователей для выставления счетов. В большинстве случаев этот идентификатор пользователя был просто названием компании, но пароль иногда раскрывался, когда у служб таймшера были конкурирующие клиенты. Однако, с точки зрения пользователя, имя пользователя связывает его с данными на компьютере, а подключение к модему не представляет угрозы безопасности. В то время любая компания, достаточно крупная, чтобы владеть компьютером, представляла собой фирму с определенными активами и контентом. поэтому предполагалось, что компаниям, предоставляющим услуги разделения времени, нужна физическая безопасность вокруг их компьютеров, а пароли были еще одним доказательством их проверки безопасности. Для поставщиков услуг разделения времени считалось рискованным предоставлять логический доступ к клиентам, и, учитывая их богатство и характер, можно было ожидать, что они будут соответствующим образом защищать свои активы. С 1970-х по 1980-е годы миникомпьютеры стали более доступными, что в конечном итоге позволило людям владеть целым компьютером для собственного использования. Apple представила персональные компьютеры в конце 1970-х годов. Вскоре они вошли в среду обработки данных и в 1981 году появился персональный компьютер IBM.

Позже сетевые технологии позволили настольным компьютерам в одном здании обмениваться информацией друг с другом, и имена компьютеров стали важными для людей, чтобы обмениваться информацией с другими компьютерами в сети. Кабели локальной вычислительной сети (LAN) были защищены так же, как компьютерные терминалы были подключены к мейнфреймам, за исключением того, что новый тип сетевого оборудования, называемый «концентратором», позволял осуществлять связь, а концентраторы должны были находиться в безопасной зоне. Концентраторы, которые позволяют кому-то подключить свой компьютер к локальной сети, защищены закрытыми шкафами. До появления локальных сетей контроль доступа к вычислительной

среде был скорее исключением, чем нормой. Если учетные данные для входа распространялись, они редко удалялись.

Вместо того, чтобы ограничивать доступ к данным, они использовались как удобный способ пометить больше данных, чтобы увидеть, кому они принадлежат. Однако из-за большого количества вычислительных сред, подключенных к локальной сети, и связанных с ними ПК людям очень сложно отслеживать активность компьютеров в сети, поскольку они обычно имеют доступ только к настольному компьютеру. По мере того, как локальные сети становились все больше, для корпоративных мэйнфреймов разрабатывались схемы централизованного управления государственными исследовательскими лабораториями (Schweitzer, 1982, 1983). Принудительный контроль доступа позволяет определять системные компьютерные объекты (программы и файлы) и контролировать субъектов (пользователей), которые могут получить к ним доступ. Они дополнялись дополнительными схемами,

Поскольку многие пользователи компьютеров в локальной сети имели на своих столах терминал главного компьютера, эти компьютеры вскоре переняли функцию терминала, и локальная сеть была подключена к главному компьютеру. Именно это развитие сделало кибербезопасность горячей темой в управлении технологиями. Хотя в локальных сетях использовалась некоторая технология паролей со сдвигом во времени, имена пользователей в локальных сетях в основном поддерживались для облегчения работы служб каталогов, а не для предотвращения атак обнаружения. То есть было полезно знать имя человека, написавшего тот или иной файл или разместившего заметку в записи клиента.

До этого момента эволюции киберпространства транзакции на мэйнфреймах можно было отследить до отдельного терминала в определенном физическом месте, и дальнейшее расследование с использованием физической и цифровой криминалистической экспертизы имело все шансы идентифицировать подозреваемого. Однако локальные сети и модемы мешали общению между пользователями, и преступнику было легко отрицать активность через рабочий стол локальной сети или использовать быстро распространяющуюся версию компьютерной безопасности. Даже там, где требовались пароли, они были достаточно слабыми, чтобы их можно было угадать.

Не существовало понятия сетевого шифрования, поэтому любой, у кого был доступ к концентраторам, мог видеть пароли, путешествующие по сети. Кроме того, многие сетевые программы допускали анонимный доступ, поэтому имена пользователей не были доступны для каждого подключения. Руководству потребовалось несколько случаев мошенничества с использованием инсайдерской информации, чтобы понять, что текущая ситуация слишком рискованна, чтобы ее поддерживать. Таким образом, технология безопасности, которая до этого была предметом военных исследований, была спешно использована крупными поставщиками компьютеров и применена к наборам данных мэйнфреймов и файловым ресурсам локальной сети. К ним относятся идентификатор пользователя, включая аутентификацию в виде все более сложных паролей и административного доступа к компьютеру. Вскоре Министерство обороны СШАрешение сделало полный набор системных функций, необходимых для работы в среде, легкодоступной, так называемой "оранжевой книгой" (DoD 1985). Полный набор функций включен стандарты и сложная терминология для технической реализации, процессы для обеспечения идентификации и аутентификации пользователей проверено. Шифрование также было заявлено как точное решение для нашел решение различных проблем компьютерной безопасности (NRC 1996), но это было роскошью мало у кого за пределами армии было достаточно запасных компьютеров, следовательно, чем меньше компьютер, тем слабее алгоритмы шифрования поставщика. могло быть, и шифрование использовалось с точностью. Хотя ответственность за обработку транзакций стала быстрой горячая тема на конференциях по мошенничеству, деятельность по обеспечению соблюдения законов о доменах производительность компьютера была ограничена. Тем не менее, начало 1980-х было также началом эры цифровых доказательств.

В сотрудничестве с правоохранительными органами поставщики технологий для производства программного обеспечения, которое восстанавливает файлы преступников пытался удалить с компьютеров (Schmidt 2006).

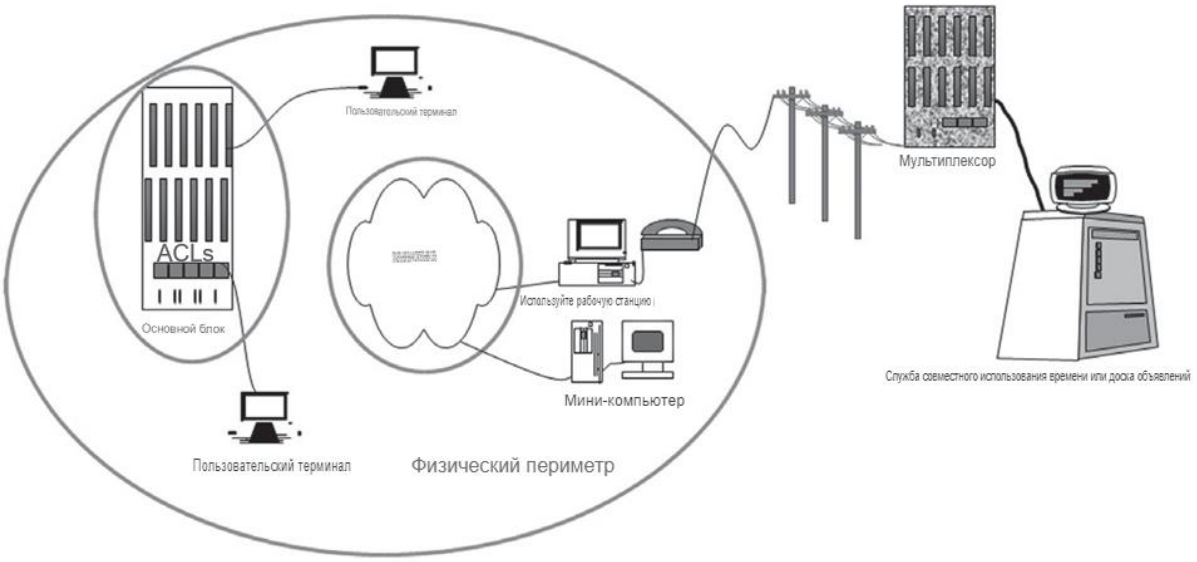


Рисунок 1.4. Архитектура киберпространства 1980-х годов

Рисунок 1.4 изображает архитектуру киберпространства в ее типичной конфигурации. В начале 1980-х гг. Мэйнфреймы, микро- и мини-компьютерысуществовали бок о бок и не нуждались в объединении в сеть. Однако миникомпьютеры часто использовались для подключения к удаленным компьютерам по телефонным линиям того же типа, что и для голосовых вызовов. Однако из-за быстрого развития технологических инноваций эта ситуация постоянно развивалась, и изменения были неизбежны.

§ 1.3. Цели кибербезопасности

Учитывая сложную природу технологий кибербезопасности и постоянно растущий характер угроз кибербезопасности, можно ожидать, что директивные органы будут постоянно сталкиваться с решениями о том, как реагировать на новейшие угрозы. Однако, поскольку решения о мерах кибербезопасности часто остаются за технологами, директивные органы могут не видеть, как принимаются эти решения, и, следовательно, не иметь возможности измерить организационное влияние различных альтернативных подходов.

На самом деле гонка вооружений в области кибербезопасности часто предлагает очень мало альтернатив. Практически сразу после внедрения технологии кибербезопасности ее использование объявляется отраслевым стандартом каким-либо регулирующим органом, что не позволяет организациям принять определенный подход к контрмерам. Например, если регулируемая организация решит использовать подход к кибербезопасности, не использующий

брандмауэры, она подвергнется тщательной проверке со стороны регулирующих аудиторов. Специалистам по кибербезопасности кажется, что проще идти в ногу с новейшими инструментами и технологиями безопасности, чем переосмысливать свой организационный подход.

Обратите внимание, что эти цели политики кибербезопасности не согласовывались и не должны совпадать с целями кибербезопасности организации в то время. Однако в этой главе мы также рассмотрим методы, используемые для определения того, были ли достигнуты цели политики кибербезопасности. Мы наблюдаем, что те, кто ставит цели безопасности, часто совершают ошибки для достижения своих целей безопасности. Мы пришли к выводу, что текущие показатели кибербезопасности вообще не измеряют безопасность. Глава завершается тремя примерами из практики, которые иллюстрируют, как определяются цели кибербезопасности и как можно измерить достижение целей кибербезопасности.

Показатели кибербезопасности.Измерение — это процесс отображения из эмпирического мира в мир формальных отношений, результаты которого описывают атрибут рассматриваемого объекта.

Комбинация измерений, соответствующих нематериальному атрибуту, считается производными измерениями и должна интерпретироваться в контексте абстрактной модели измеряемой вещи (ISO/IEC 2007). Показатели — это общий термин, который относится к набору измерений, описывающих конкретную область. Кибербезопасность не является прямым объектом измерения или достаточно понятным атрибутом системы, чтобы легко определить полученные измерения или метрики.

Таким образом, метрики кибербезопасности измеряют другие вещи и делают на их основе выводы о достижении целей безопасности. Эта проблема породила область исследований, называемую индикаторами безопасности (Jaquith and Geer 2005). Метрики физической безопасности традиционно фокусировались на способности системы выполнять свою задачу по противодействию проектным угрозам (DBT) (Garcia 2008). DBT описывает характеристики наиболее мощного и инновационного противника, от которого можно ожидать защиты.

В Нью-Йорке это может быть террорист, оснащенный сложной аппаратурой связи и взрывными устройствами. В Айдахо это могут

быть головорезы лет двадцати на мотоциклах с автоматическим оружием. Принятие DBT-подхода к безопасности означает, что степень защиты, требуемая системой, должна рассчитываться на основе технического описания того, как она может быть атакована. В физической безопасности этот процесс прост. Если ДБТ состоит из 20 человек с определенными типами взрывчатых веществ, то прочность физических преград от несанкционированного доступа должна выдерживать тонны силы, которые могут применить эти 20 человек.

Специфицируются материалы барьерной защиты, разрабатываются системы задержки и реагирования на угрозы, и соответственно проводятся проверочные испытания. Кибербезопасность включает следующие термины:

— Преступник;
— Угроза;
— Эксплуатация;
— Слабость.

Этоттермины являются условиями торговли, и их значения являются отдельными и взаимозависимыми. Как показано на системной диаграмме на рис. 1.4, преступником является физическое или юридическое лицо.

Угроза – это потенциальное действие, которое может быть совершено или не совершено преступником. Эксплуатация относится к техническим деталям, связанным с атакой.

Уязвимость — это характеристика системы, позволяющая успешно использовать эксплойт.

Таким образом, основная предпосылка системной диаграммы на рис. 1.4 гласит: «Безопасность удерживает преступников, которые используют уязвимости системы для осуществления угроз, которые наносят ущерб, неблагоприятный для стоимости» (Bayuk, Barnabe et al. 2010).

С момента зарождения компьютерных систем DBT для компьютерной безопасности предназначались для потенциальных преступников, таких как хакеры в форме наездников, злонамеренных агентов киберразрушения и агентов шпионажа.

Однако, в отличие от анализа физической безопасности DBT, меры противодействия, разработанные в ответ на угрозу, сосредоточены не на самих субъектах угрозы и возможной их последней тактике, а на уязвимостях технологии, используемой для

реализации последней угрозы. По мере того, как каждый тип системной уязвимости достиг определенного уровня осведомленности в сообществе безопасности, на рынок выходит соответствующий набор технологий контрмер, которые становятся частью растущего числа рекомендаций по передовому опыту.

Были приняты меры против уязвимых частей системы, и предполагалось, что угрозы системам будут компенсированы общим эффектом их реализации.

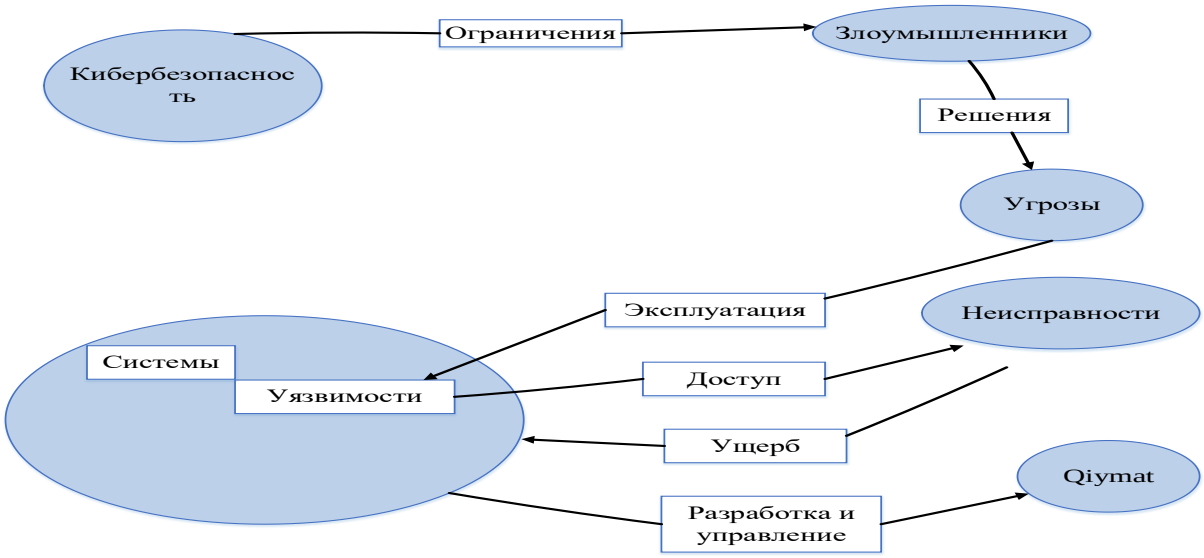


Рисунок 1.5. Схема системы кибербезопасности

Рисунок 1.6 иллюстрирует этот подход добавлением этих понятий и взаимосвязей между ними к системной диаграмме на рисунке 1.5.

На рис. 1.6 показано, как показатели кибербезопасности, подходы к управлению, аудиты и методы расследования основаны на инструментах и методах обеспечения безопасности.

Консенсус в отношении того, что цели безопасности достигаются с помощью технологии контрмер, достигается за счет обращения к DBT как части конструкции системы.На рис. 1.7 показана разница между этим традиционным подходом к архитектуре безопасности и целостным подходом на уровне системы. Он описывает слабые атрибуты системы как подмножество атрибутов системы и цели преступников как подмножество слабых атрибутов системы.

Традиционно техника безопасности решала эту проблему с помощью специальных компонентов безопасности, уничижительно называемых «болтами».

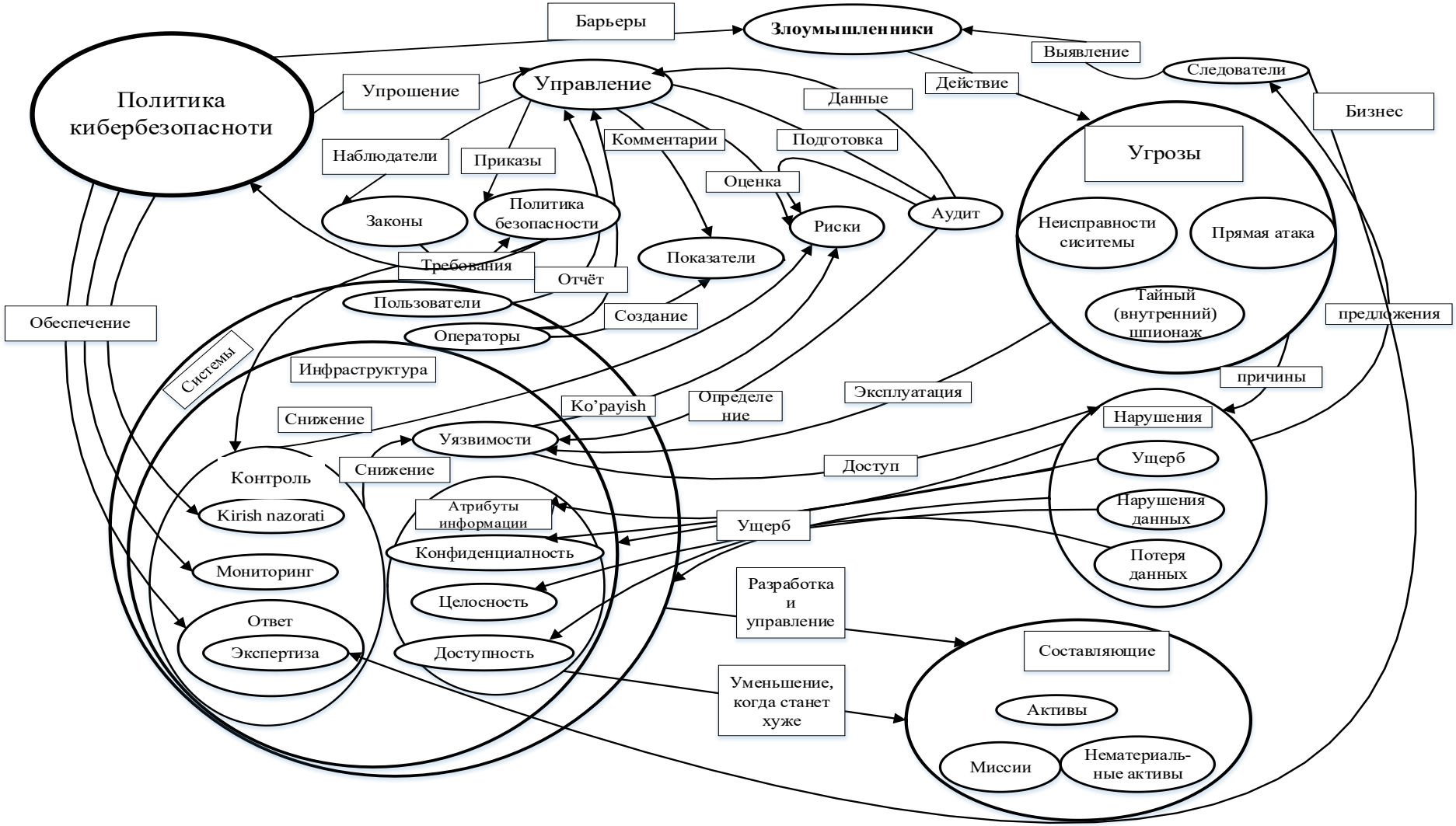


Рисунок 1.6. Полная системная диаграмма

Болтоны по определению не принадлежат самой системе, т.е. в главе 1 описаны процессоры с брандмауэрами. Нижняя часть рисунка 1.7 иллюстрирует конфликт между изящным подходом к решению проблем безопасности и дизайном безопасности. подход, который, как ожидается, изменит атрибуты системного уровня, чтобы устранить или уменьшить уязвимость. Если сначала попробовать этот подход, количество средств управления компенсацией безопасности должно быть минимальным. Тем не менее, как описано в главе 1, список технологий безопасности, по-видимому, используется почти бессознательно. В результате типичное представление целей безопасности показывает процесс реализации технологий безопасности, перечисленных в бизнес-домене и операционной системе компьютера. Рисунок 1.8 является типичным примером.

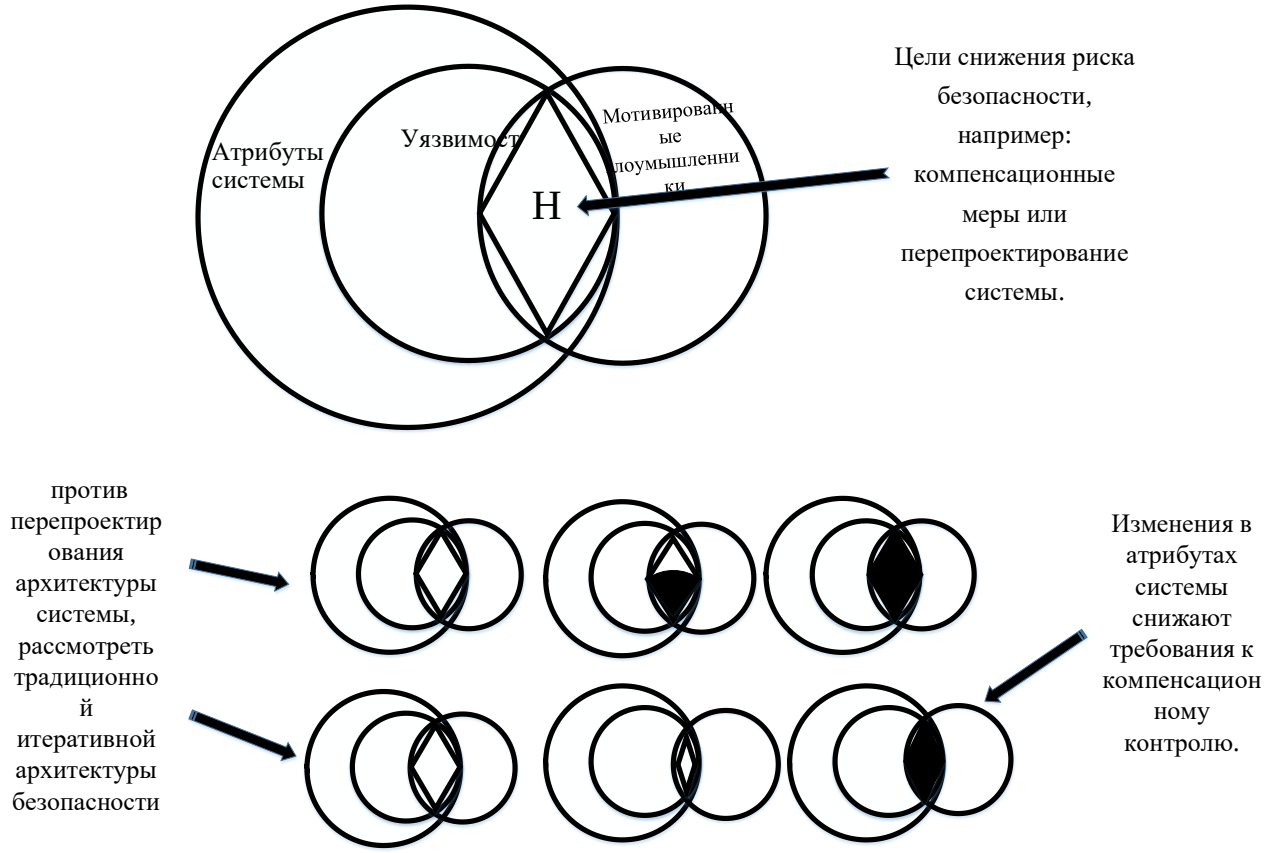


Рисунок 1.7. Конструкция с болтовым креплением

Цели управления безопасностью.У многих лидеров нет четкой цели в отношении безопасности, кроме «Я хочу быть в безопасности». В этих случаях есть элемент цели, который можно полностью выразить так: «Я хочу быть в безопасности, практически не влияя на мою организацию». Они делегируют это руководство

специалистам по безопасности точно так же, как они делегируют управление балансом бухгалтерскому персоналу и говорят: «Я хочу, чтобы цифры были точными». Если оставить в стороне сходство между двумя профессиями, связанное с необходимостью соблюдения правовых и нормативных документов, делегация считает, что исполнительные делегаты понимают проблемы и могут тесно сотрудничать со всеми в бизнесе.

Однако бухгалтерская профессия имеет несколько тысячелетий истории, подтверждающих ее способность определять доверие в терминах отношений, включая комбинацию ситуаций и санкций..

Напротив, профессия кибербезопасности существует всего около полувека с тех пор, как появились первые отраслевые или национальные стандарты безопасности, и тем более с момента появления международных стандартов безопасности (см. DoD 1985; ISO/IEC 2005 a,b для небольшого образец); ФИЭК 2006; Росс, Кацке и др. 2007 г.; PCI 2008). Кроме того, вместо какого-либо согласованного отраслевого стандарта, такого как общепринятые принципы бухгалтерского учета (GAAP), существует так много конкурирующих стандартов в области кибербезопасности, которые предприятия создали для их каталогизации и сравнения (продолжение UCF). Продукт поставляется в виде электронной таблицы или другого формата структурированных данных. Он предназначен для импорта в систему управления информацией о безопасности (SIM) и позволяет менеджеру по безопасности продемонстрировать соответствие нескольким стандартам, не читая их все. Программы безопасности, разработанные для соблюдения нормативных требований, не предназначены специально для достижения организационных целей безопасности, а предназначены для демонстрации соответствия стандартам управления безопасностью. Таким образом, сами стандарты стали де-факто таксономиями показателей безопасности, которые выходят за организационные границы. Программы безопасности, разработанные для соблюдения нормативных требований, не предназначены специально для достижения организационных целей безопасности, а предназначены для демонстрации соответствия стандартам управления безопасностью. Таким образом, сами стандарты стали де-факто таксономиями показателей безопасности, которые выходят за организационные границы. Программы безопасности, разработанные для соблюдения нормативных

требований, не предназначены специально для достижения организационных целей безопасности, а предназначены для демонстрации соответствия стандартам управления безопасностью. Таким образом, сами стандарты стали де-факто таксономиями показателей безопасности, которые выходят за организационные границы.

Практикующим специалистам часто советуют организовать свою работу на основе требований стандартов управления безопасностью, которые можно проверить. Существует также международный стандарт по использованию стандартов управления безопасностью для создания показателей безопасности (ISO/IEC 2009b).

Недостатком такого подхода к управлению безопасностью является то, что сведения о соответствии рассматриваются как изолированные технологические конфигурации, которые сравниваются с предустановленной системой показателей, в отличие от системы показателей, предназначенной для отражения целей корпоративной безопасности.

Ни один из этих стандартов не включает общепринятый способ прямого измерения безопасности с точки зрения достижения в устранении угроз (King 2010). Как правило, они используются для обеспечения того, чтобы руководство проявило должную осмотрительность при установлении действий, которые должны обеспечивать безопасность, а не для измерения того, были ли действия эффективными. Сравните это с тем, как обычные люди относятся к безопасности. Например, специалисты по перемещению рабочих мест иногда измеряют уровень безопасности в старых и новых фирмах, основываясь на степени сложности доступа к критически важным данным и информации локально и удаленно. Например, они могут определить количество паролей, которые им нужно использовать со своих компьютеров дома для доступа к клиентским данным в офисе, и решить, что фирма, которая заставляет их использовать больше факторов аутентификации, более безопасна. На рис. 1.8 показана схема этого типа многоуровневой защиты системной безопасности. Такой слой часто называют глубокоэшелонированной защитой. Этот термин относится к архитектуре, в которой меры безопасности являются многоуровневыми и избыточными, а уязвимость в одной части системы покрывается другой.

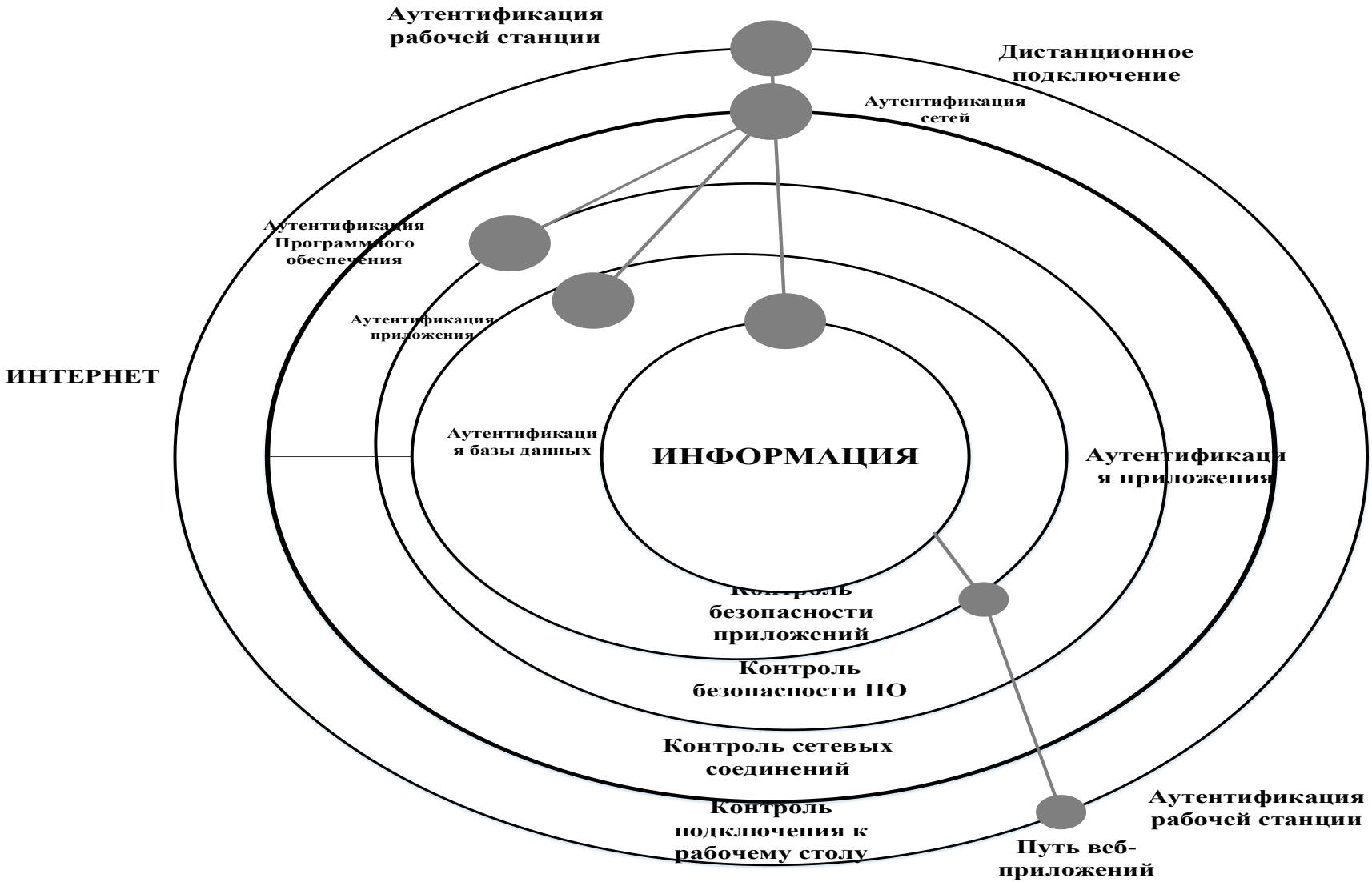
То есть ни один элемент управления не должен представлять собой единую точку отказа, так как по крайней мере два элемента управления должны быть нарушены, чтобы злоумышленник мог получить доступ. Он имеет несколько «уровней» безопасности, как показано в центре нижней части диаграммы. В верхней части диаграммы показано, как пользователь удаленного доступа должен пройти аутентификацию на рабочей станции, которая может управляться или не управляться предприятием.

Затем пользователь проходит аутентификацию в корпоративной сети через Интернет. Из точки доступа к сети удаленный пользователь может пройти аутентификацию непосредственно на любом из других уровней внутренней сети. Поэтому удаленный доступ обычно требует высокого уровня безопасности, так как существуют различные варианты доступа к платформе после выхода во внутреннюю сеть.

Этот путь удаленного доступа противоположен пути доступа к веб-приложению на рис. 1.8. В случае веб-приложения наличие уровней на самом деле не является глубокоэшелонированной защитой. Это связано с тем, что такие веб-приложения обычно доступны через единый вход.

Путь к веб-приложению указывает, что пользователи Интернета обычно проходят проверку подлинности на своих рабочих станциях, которые не управляются предприятием. Затем пользователь может получить доступ к приложению без аутентификации в сети, поскольку брандмауэр позволяет любому пользователю Интернета напрямую обращаться к экрану входа в приложение на веб-сервере.

Кроме того, нет необходимости проходить аутентификацию в операционной системе сервера. Оказавшись внутри приложения, уровень аутентификации данных не виден пользователю; приложение автоматически подключится к нему от имени пользователя. Эти средства изображены на рисунке как мосты через уровни, для прохождения которых удаленный пользователь должен аутентифицироваться, а пользователь приложения — нет. Следовательно, в данном случае было бы неправильно использовать термин «глубокоэшелонированная защита». Понятно, что несколько устройств должны быть настроены скоординировано, чтобы гарантировать, что необходимая технология действительно закрыта, потому что не каждый замок на каждом уровне имеет ключ. И так,



1.8. картина Доступ к веб-приложению

большая часть литературы по эффективности безопасности предполагает, что цель состоит в том, чтобы правильно настроить все эти уровни (Hayden 2010). Однако, несмотря на это предположение, стандартной таксономии показателей безопасности не существует. Принципы, использованные в такой классификации, исследовались разными исследователями, и эти исследования дали разные результаты.

Контрольные вопросы.

1. Какие технологии помогают защитить целостность информации в киберпространстве?
2. Что такое кибербезопасность и как она связана с конфиденциальностью, целостностью и удобством использования данных?
3. Каковы альтернативные подходы к кибербезопасности и каковы их преимущества и недостатки?
4. Как измеряется эффективность мер кибербезопасности и как можно улучшить показатели кибербезопасности?
5. Как определить преступление, угрозу, эксплуатацию и уязвимость в контексте кибербезопасности?
6. Какие типы киберпреступников существуют и какие уязвимости они используют для осуществления угроз?
7. Какие технологии мер безопасности доступны для предотвращения или уменьшения вреда угроз?
8. Какова цель управления безопасностью и почему это важно для руководителей организаций?
9. Какие проблемы могут возникнуть, если лидеры делегируют управление безопасностью экспертам без достаточного понимания и сотрудничества?
10. Чем отличаются профессии бухгалтера и кибербезопасности с точки зрения истории, стандартов и доверия?
11. Что такое UCF и как он может помочь менеджерам по безопасности продемонстрировать соответствие различным стандартам безопасности?
12. Каковы преимущества и недостатки использования системы управления информацией о безопасности (SIM) для импорта и анализа данных о безопасности?
13. В чем разница между политикой кибербезопасности и законами и правилами кибербезопасности?

14. Какие факторы влияют на формирование политики кибербезопасности каждой страны?

15. Каковы некоторые примеры глобальных договоров, законов и положений о кибербезопасности?

16. Какова политика кибербезопасности Китая и как она отражена в законах и правилах?

17. Какие ограничения существуют для государственных органов и отраслевых регулирующих органов в создании и применении законов и положений о кибербезопасности?

II ГЛАВА. СПРАВОЧНИК ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ

§ 2.1 Руководство для лиц, принимающих решения.

В настоящее время правительство Великобритании вкладывает значительные средства в кибербезопасность, и теперь министерства обязаны обеспечивать минимальный стандарт кибербезопасности. Департаментыразные по степени зрелости, отделы знают и стремятся достичь этого стандарта и выше.

В этом разделе рассматривается Cyberthreat Intelligence (CTI) и поддерживается современный передовой подход «на основе угроз». Это включает в себя понимание того, кем могут быть субъекты угрозы в отделе, их мотивы и возможности, а затем распространение полезной информации о них. Широкий охват CTI стимулировал создание многих продуктов и услуг от поставщиков. Однако отделы могут иметь ограниченные знания и опыт CTI, что мешает им приобретать соответствующие инструменты и создавать среду, соответствующую передовой практике.

У отделов, поддерживающих CTI, разные области применения, бюджеты и спецификации, а их возможности по внедрению передового опыта различаются.

Целевая аудитория.Это руководство предназначено для лиц, которые контролируют или предоставляют отделу возможности анализа угроз. В этом документе представлена дорожная карта для предоставления возможностей CTI и обзор необходимых действий, результатов и технологий. При необходимости будут включены технические детали.

Являетесь ли вы лицом, принимающим решения, руководителем группы или аналитиком, мы рассмотрели все области. При подробном описании CTI он разделен на следующие разделы в зависимости от жизненного цикла анализа угроз:

- Направление;
- Коллекция;
- Обработка;
- Анализ;
- Распределение.

Дополнительные отделы для постоянного совершенствования

и организации (в том числе ресурсного обеспечения):

— Постоянное улучшение;
— Организация.

Информация о киберугрозах. Cyberthreat Intelligence — это анализ информации о противниках в киберпространстве для распространения информации о воздействии угроз путем понимания мотивов, возможностей и методов действий злоумышленников для информирования о мерах по смягчению последствий кибербезопасности — это процесс обработки, обработки и анализа.

Охота за угрозами. Поиск угроз — это упреждающая, итеративная и ориентированная на человека идентификация киберугрозы, которая является внутренней для ИТ-сети и обошла существующие средства контроля безопасности.

Цифровая угроза и разведка. Это процесс мониторинга, обнаружения и устранения общедоступных угроз путем контроля цифрового следа организации. В этой главе представлены рекомендации о том, как государственные учреждения могут лучше понять и контролировать свой цифровой след, развивая и совершенствуя свои возможности в области цифровых рисков и разведки.

Рекомендации в этой главе разделены на три уровня:

— *Группа разведки угроз*- быстрые, простые в реализации, краткосрочные рекомендации;
— *Департамент правительства*- среднесрочные рекомендации разведывательных групп, повышающие возможности угроз;
— *Межправительственные функции*- долгосрочные рекомендации, позволяющие государственным учреждениям лучше защищать свои цифровые следы в будущем.

Если мы воспользуемся тремя возможностями, мы рекомендуем вам обратить внимание на следующие моменты:

1. Все три возможности подпадают под каждую из возможностей, указанных в минимальном стандарте кибербезопасности. Если минимальный стандарт не соблюдается, считается, что инвестиции в эти области с большей вероятностью окажутся прибыльными, чем эти возможности.
2. Создание зрелых возможностей во всех трех областях представляет собой значительные инвестиции для бизнеса. В

частности, в государственном секторе эти инвестиции будут тщательно проверяться, и мы рекомендуем каждому сектору обеспечить реальную ценность денег. Из всех организаций, с которыми мы работали, ни одна из них не взяла на себя обязательство развивать все три возможности за пределами страны происхождения.

Доступ к данным и видимость данных имеют решающее значение для всех функций, как внутренних, так и внешних. Мы рекомендуем вам ознакомиться с конкретными условиями доступа к данным в вашей организации, прежде чем инвестировать. Другие организации, с которыми были проведены консультации, вложили значительные средства, но не смогли воспользоваться преимуществами из-за отсутствия доступа к данным.

Новые возможности CTI и Threat Hunting следует разрабатывать вместе, если они имеют взаимодополняющие требования. Зрелые возможности поиска угроз без возможностей CTI для предоставления разведывательных данных будут ограничены, и возможности CTI, предоставляющие информацию CSOC без охотников за угрозами, также ограничены в ценности.

Создайте функцию CTI.Департаменты (в настоящее время) не обязаны собирать, интегрировать или анализировать свои сети или данные. Минимальный стандарт кибербезопасности NCSC предусматривает минимальный набор мер (1), в том числе: «Как минимум, отделы могут интегрироваться с общими источниками информации об угрозах, такими как Партнерство по обмену информацией о кибербезопасности (CiSP), для выявления конкретных угроз. должны фиксировать события

Это означает, что разделы данныхдолжны собирать (из собственной инфраструктуры и устройств), но интеграция с CTI необязательна. Тем не менее, в стандарте также говорится, что отделы должны стараться по возможности превысить стандарты, поэтому в настоящее время от организаций не требуется использовать контент с информацией об угрозах, им рекомендуется это делать.

Независимо от минимальных стандартов информация об угрозах уже естьмогут быть полезны для отделов со зрелой системой кибербезопасности. Хотя предпосылки для способности CTI приносить пользу могут варьироваться от отдела к отделу, мы

считаем, что организации могут сделать значительные (т. е. более 5% бюджета безопасности) инвестиции в CTI только в том случае, если они это сделают. рекомендуют рассмотреть или сослаться на реалистичную дорожную карту для достижения всех 10 разделов минимального стандарта кибербезопасности. Бюджет, выделяемый на инвестиции CTI, должен быть обоснован.

Варианты использования CTI.CTI можно использовать несколькими способами. Прежде чем отдел сможет принимать относительно дорогостоящие и долгосрочные решения о том, как улучшить свои возможности CTI, ему необходимо понять варианты использования CTI. Ниже приведены семь ключевых вариантов использования:

Таблица 2.1

Использование CTI

Состояние использования	**Цель**	**Требуется интеллект**
Подтверждение Тревоги/события	Подтверждение сигналов тревоги/инцидентов и передача информации любой группе реагирования на инциденты и выберите, чтобы исправить.	Аналитика угроз: ссылки на данные с отдельными индикаторами, субъектами угроз, методами и т. д.
Улучшение Автоматизированный Отвечать	Автоматизация процесса сортировки Проверки через службу безопасности Уделите приоритетное внимание управлению информацией и событиями (SIEM) и инструментам аналитики, чтобы точно сообщать о предупреждениях и событиях. CTI ведущий/аналитик.	Аналитика угроз: показатели угроз и рейтинги серьезности, связанные с конкретными целевыми атаками по отраслям, приложениям и т. д.

Уведомление ведомственный Профессия риска	Повышение уровня безопасности и контекстного управления процессом управления уровнем риска, сбор разведывательной информации	Данные об угрозах: связанные индикаторы угроз и рейтинги серьезности атаки специального назначения промышленность, приложения и т. д.
Приоритет слабых сторон	Создайте метрику оценки уязвимости, измеряя совпадение между устранимыми проблемами и проблемами с наибольшим влиянием, учитывая доступное время и ресурсы.	Информация об уязвимостях: CVE, связанные с атаками на определенные сети, CVE, связанные с конкретными угрозами, и многое другое.
Поддержка ThreatHunting	Заблаговременно обнаруживайте скрытые атаки на сеть отдела, связанные с текущими событиями или угрозами, направленными на отдел.	Аналитика угроз: контекстуальные индикаторы кампаний, субъекты угроз, методы, история и цели.
Содержит и исправляет атаки	Нарушайте связь/управление и контроль злоумышленника, удаляйте вредоносное ПО.	Аналитика угроз: база данных разведки, включающая информацию о методах, истории и целях различных групп угроз.
Анти-Фишинг	Расширьте существующие возможности защиты почты, дополнив набор данных обнаружения метриками.	Аналитика угроз: контекстуальные индикаторы кампаний, субъекты угроз, методы, история и цели.

Эти примерные варианты использования предоставляют обзор типов действий, которые может выполнять функция CTI. Если у

вашего отдела нет желания предоставлять какие-либо из этих вариантов использования, вам следует подумать, соответствует ли CTI потребностям вашего отдела. В оставшейся части этого раздела описываются эти варианты использования и более широкий раздел возможностей CTI.предоставляет дорожную карту для доставки.

Дорожная карта.Можно предпринять несколько шагов для разработки новой возможности CTI с использованием существующих или минимальных новых ресурсов кибербезопасности.

Оценка угроз предоставляет информацию о вашем профиле угроз и рекомендации о том, сколько людей требуется для выполнения задач функций CTI. Команда CTI нижет**ри**могут начинаться с роли (не трех лиц) или выполняться как функции других ролей:

1.Лидер CTI, который возглавляет и управляет этой функцией, отвечает за реализацию стратегии и по мере необходимости предоставляет информацию совету директоров, высшему руководству и владельцам систем.

2.Аналитик CTI, который собирает, анализирует и обрабатывает данные из неавтоматизированных источников (например, отраслевых документов) и берет на себя ответственность за профилирование действий субъектов угроз, выявленных при оценке угроз.

3.Аналитик CTI, который собирает, обрабатывает и анализирует техническую информацию и обеспечивает выделенную точку контакта с CSOC.

Этот аналитик будет поддерживать профилирование субъектов угроз, но их основная обязанность будет заключаться в поддержании и предоставлении показателей технической разведки CSOC и другим защитникам.

Совершенствование результатов. Цель функции CTI - предоставить информацию, относящуюся к его отделу. Это не требует (особенно в этой новой возможности), чтобы функциональность CTI была на переднем крае анализа разведывательных данных, анализируя атаки нулевого дня от усовершенствованных постоянных угроз (APT).

Автоматизация. Помимо отчетов и брифингов, ключевой частью сбора информации о киберугрозах является предоставление

технических данных CSOC. Основная проблема в том, что в этом пространстве нужно обрабатывать много данных, и ряд отделов не может эффективно справиться с «переключением» контента.

Наша рекомендация состоит из двух методов:

— Изучите полезность технической разведки с использованием технологий с открытым исходным кодом (таких как проект обмена информацией о вредоносных программах (MISP) и существующих возможностей вашего инструмента SIEM. Это поможет вашему отделу понять требования к технической обработке данных и позволит эффективно выявлять нефункциональные аспекты. системы, такие как требования к интеграции и объем данных.

— Максимально используйте централизованные данные с помощью таких платформ, как CiSP, или каналов надежных поставщиков. Текущую ленту угроз следует использовать, чтобы быть в курсе развивающейся картины угроз.

—

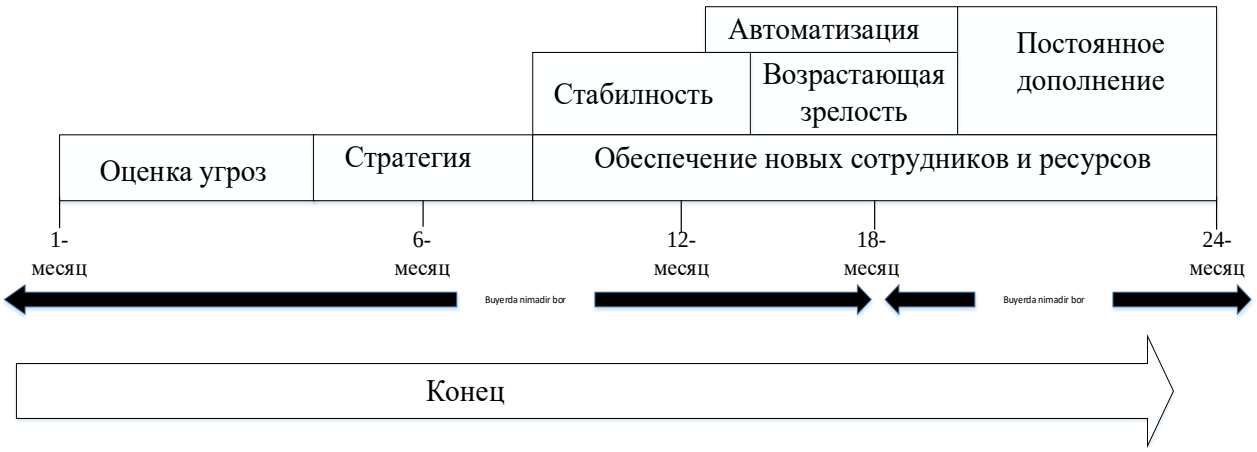


Рисунок 2.1. Дорожная карта развития CTI

Расходы. Cyberthreat Intelligence — это особая возможность, которая развертывается вместе с существующими возможностями безопасности как в кибер-, так и в традиционных ролях безопасности. Как упоминалось выше, CTI позволяет этим функциям лучше защищать отдел и имеет ограниченную ценность, если они уже не находятся в зрелом рабочем состоянии. Следовательно, не рекомендуется перенаправлять бюджет, выделенный на эти функции, на финансирование возможностей CTI. CTI должен финансироваться независимо.

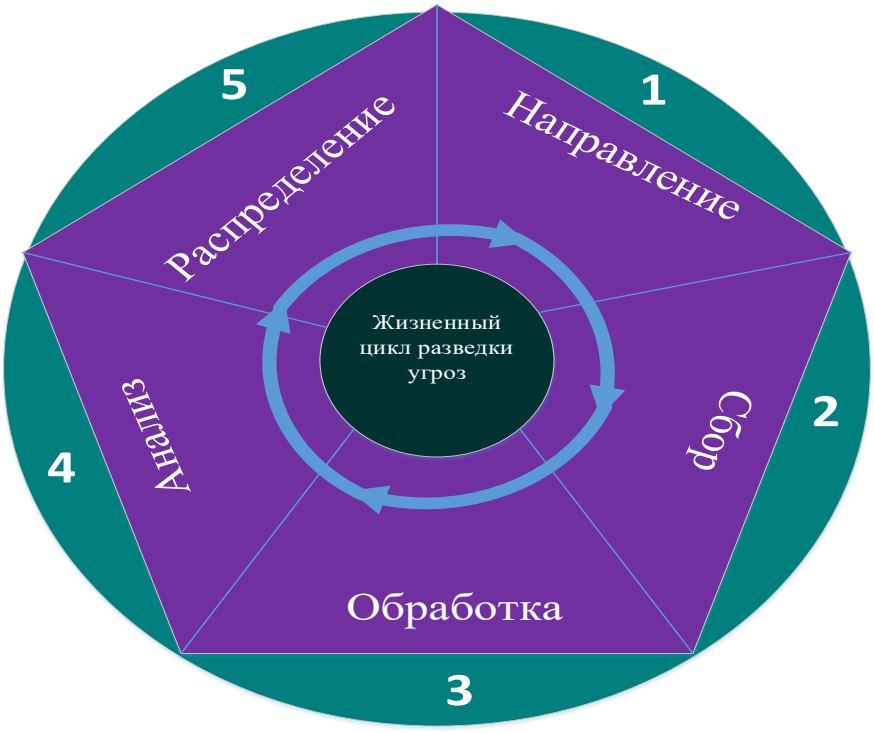


Рисунок 2.2. Жизненный цикл анализа угроз

Определения, область применения и структура. Информация о киберугрозах.

Cyberthreat Intelligence имеет несколько определений имеет, но для целей данного руководства будет использоваться следующее определение:

«Информация о киберугрозах — это понимание мотивов злоумышленников для информирования о мерах по смягчению последствий кибербезопасности,— это процесс сбора, обработки и анализа информации о противниках в киберпространстве с целью распространения информации об угрозах, влияющих на них, путем понимания их возможностей и действий».

Несмотря на ряд изменений, этоВ книге используется 5-этапный жизненный цикл:

— Направление;
— Сбор;
— Обработка;
— Анализировать;
— Распределение.

Организационные уровни доставки.Деятельность организации/отдела обычно делится на три уровня:

— стратегический;
— оперативный;

— Тактический.

В контексте CTI обычно используется четвертый уровень — технический.

Стратегический CTI является высокоуровневым и ориентированным на бизнес, обычно в форме прозы, такой как отчеты или презентации, предназначенные для групп высшего руководства подразделений (SMT).

Цель стратегического CTI — помочь SMT принимать обоснованные бизнес-решения, предоставляя отделу информацию об угрозах, которая затем используется в установленных процессах управления стратегическими рисками и управления ресурсами.

Общие источники стратегических CTI включают геополитические события, отраслевые официальные документы и надежные сети.

Общие источники оперативного CTI включают отчеты об угрозах, отчеты об инцидентах, анализ вредоносных программ, а иногда и социальные сети и чаты.

Направление. В этом разделе представлен обзор первой фазы жизненного цикла анализа угроз — маршрутизации. Можно дать по направлениюбылтребует стратегического, оперативного и тактического уровня от различных клиентов в отделе.

Маршрутизация — самый важный шаг в обеспечении полезной функциональности CTI, так как она направляет все последующие шаги. На следующем этапе следует приложить усилия для правильного сбора требований с самого начала, чтобы свести к минимуму влияние изменений.

Оценка киберугроз. Чтобы понять цели команды CTI, отдел должен сначала получить общее представление о своем профиле угроз. Зрелая оценка киберугроз (TA) должна быть основным руководством для отделов при рассмотрении их стратегии разведки угроз.

Основные различия между предыдущими методами оценки угроз и зрелой оценкой киберугроз показаны в таблице ниже:

Таблица 2.2

Прошлый TA и зрелый КиберTA

Оценка прошлой угрозы	**Оценка зрелых киберугроз**
Независимо от функциональной важности рассматривается	Только угрожающие лица, способные и мотивированные

широкий круг угроз (например, радиолюбители).	для нападения на отдел, будут подвергаться детальной оценке.
Субъекты угрозы делятся на широкие группы (например, «Службы внешней разведки (СФР)» или «Группы организованной преступности (ОПГ)»).	Независимо от какого-либо формального назначения, индивидуальное рассмотрение будет проводиться в зависимости от способностей и мотивации.
Активы ведомства грубо оцениваются с точки зрения степени их подверженности бизнесу.	Существует глубокое понимание бизнеса, и критически важные бизнес-активы рассматриваются индивидуально с учетом конкретных факторов риска и сценариев атак.
Такие угрозы, как FIS, часто считаются «вне официальной сферы».	Общепризнано, что многие группы угроз используют коммерчески доступные обнаруживаемые атаки, и что информация об их возможностях имеет решающее значение.

Процесс оценки угрозы.Первое упражнение состоит в том, чтобы убедиться, что отдел понимает свои критические активы. Для многих крупных отделов эти активы могут включать системы, сети, наборы данных и платформы, которые могут находиться в разных местах и средах. Хотя технически важные активы могут быть зарегистрированы в базе данных управления конфигурацией (CMDB), это упражнение по приоритизации активов должно также включать нематериальные активы и интеллектуальную собственность.

После получения представления об активах отдела можно оценить активы с точки зрения их важности для отдела, что позволяет получить представление о стоимости убытков этих активов.

Таблица 2.3

Оценка угрозы входа.

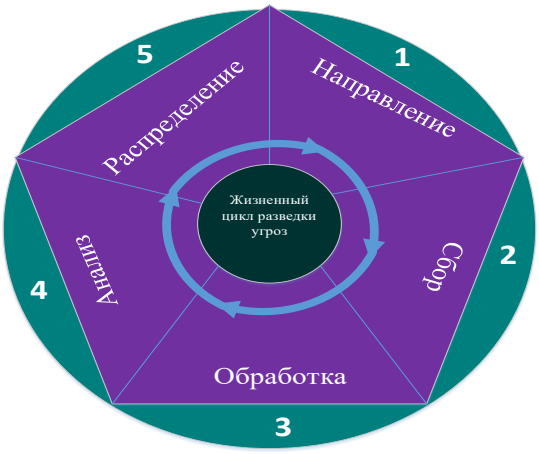
Источник ввода	**Описание**
Отчеты об инцидентах	Важно понимать атакующих, которые добились успеха в прошлом, потому что эти противники, скорее всего, вернутся. Инструменты, методы и процессы из предыдущих атак могут помочь в анализе угроз и дальнейшем снижении рисков. IR-отчеты также могут содержать скомпрометированное содержимое, которое было недавно пропущено или не подтверждено.
Отчеты о тестах на проникновение	Тесты на проникновение (оценка уязвимостей или действия красной команды) направлены на выявление функций или систем, уязвимых для атаки. Эта информация может быть добавлена к более широкой разведывательной картине. Ландшафт угроз и системы отделов со временем меняются, и отделы должны следить за тем, чтобы эти оценки не становились неточными, поскольку каждый тест рассматривает уязвимости системы с течением времени.
Совет эксперта	Как обсуждалось в разделе выше, эксперты CTI могут предоставить непредвзятое представление о ландшафте угроз и устранить ключевые угрозы для вашего отдела. Может использовать опыт из широкого круга отделов и контекстов для отслеживания эффективности и поведенческих моделей малого и среднего бизнеса.
Экспертиза отдела	Те, кто находится на «остром конце» работы отдела, также видят угрозы, стоящие перед отделом, даже те, которые не относятся к конкретным ролям безопасности. Это могут быть разработчики, администраторы, бизнес-менеджеры или юридические лица. Уровень C будет выглядеть так же. Получение информации от этих участников может быть полезным для понимания угроз. Необходимо позаботиться о том,

	чтобы они были правильно интерпретированы и расставлены по приоритетам.
Семинары для заинтересованных сторон	Групповое обсуждение угроз между сотрудниками отдела, поставщиками и внешними сторонами (например, NCSC) может внести полезный вклад в модель угроз и лучше понять сферу деятельности отдела.

Особые запросы клиентов на CTI также стимулируют спрос. Чтобы эффективно управлять этими запросами, процесс RFI должен быть определен с помощью созданного шаблона для сбора всей необходимой информации.

Это может включать такие поля, как:

- данные запрашивающего лица;
- Дата запроса;
- Основание для претензии;
- Сводные требования;
- Подробные требования;
- Эффект задержки;
- Целевое распространение.



Собирать. На этапе направления жизненного цикла Threat Intelligence данные должны быть собраны для выполнения установленных требований. Коллекция – одна из них. Наиболее сложными шагами CTI для правильной работы является обеспечение сбора соответствующих данных в достаточном количестве из множества различных источников. В этом разделе рассматриваются различные методы сбора данных и полезность каждого из них. Этот раздел разделен на две основные области:

— информация, которая обычно собирается вручную;
— информация, собираемая автоматизированными средствами.

Контент CTI должен быть действенным, что, в свою очередь, означает, что он должен быть актуальным, своевременным и точным. Функция CTI может относительно легко получать миллионы IOC, большие объемы данных и данные из каналов, но если это не делается клиентами, это ложится бременем на ресурсы функции. Таким образом, собранный контент является одной из наиболее важных областей, на которую следует обратить внимание при восстановлении функциональности CTI.

Собирать вручную.Существуют различные механизмы ручного сбора данных, но ключом к получению максимальной отдачи является стандартизация процессов сбора. Ключевые элементы данных, собранных вручную, должны быть записаны:

— Дата и время;
— Соответствующее время прогноза;
— Характер собираемой информации;
— Специальные технические примечания.

Сети обмена CTI.Сети обмена CTI относятся к формальному или неформальному обмену информацией об угрозах между практиками.

Это обычная практика в госорганах, например, есть сети между теми, кто раньше работал в армии или спецслужбах, а сейчас работает в частном секторе или госструктурах.

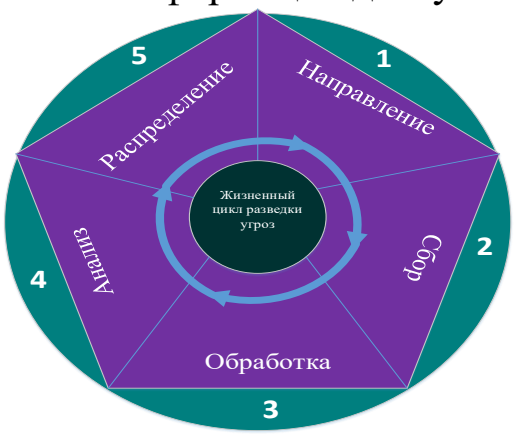
Разведка из открытых источников. Разведка с открытым исходным кодом (OSINT) относится к сбору информации из открытых источников, таких как информация в Интернете или СМИ. Эта информация доступна аналитикам;
OSINT может включать (но не ограничивается):

— Социальные медиа;
— Информацию об угрозах, опубликованную в социальных сетях, можно отслеживать;
— Исследователи;
— Представители коммерческих поставщиков CTI или даже групп угроз.

Информация, собранная из социальных сетей, должна быть проверена, чтобы быть уверенным.

Переработка отходов. Все коллекции данных настолько

хороши, насколько хорош их контент. Переработка содержание собранных данных обогащает содержание, чтобы гарантировать, что наиболее полезная информация доступна для аналитиков.



При обработке контента есть три основных момента:

— Репутация: насколько надежен этот источник информации;
— Релевантность: относится ли контент к вашему отделу;
— Качество: достаточно ли качественного контента, чтобы быть полезным?

В этом разделе описывается, как наилучшим образом обогащать содержимое, чтобы лучше предоставлять информацию для анализа и управлять объемом доступных данных.

Репутация.Вся информация должна обрабатываться в контексте репутации источника. Например, если информация исходит от доверенного контакта, она может быть выше, чем если бы она поступала из непроверенной учетной записи Twitter, и этот принцип следует распространить на ленты угроз. Итак, ключевой вопрос для различения контента: «Насколько надежен источник этой информации?» Чтобы стандартизировать этот процесс, можно создать и агрегировать показатель репутации контента.

Источник CTI оценивается на надежность на основе технической оценки его возможностей или истории. Символ надежности использует один из шести символов от A до F:

A. Полностью надежен: нет никаких сомнений в подлинности, надежности или компетентности; имеет полную историю надежности.

B. В целом надежный: мало сомнений в подлинности, надежности или компетентности; часто есть реальная история данных.

C. Высоконадежный: сомнительно в отношении подлинности,

надежности или компетентности, но в прошлом предоставлял точную информацию.

D. Как правило, ненадежный: есть серьезные сомнения в подлинности, надежности или компетентности, но в прошлом он предоставлял точную информацию.

E. Ненадежный: отсутствие аутентичности, надежности и компетентности; информация об истории отмены.

F. Достоверность не может быть оценена: нет оснований для оценки достоверности источника. Надежность:

Достоверность источника CTI оценивается на основе вероятности и степени подтверждения другими источниками. В символе доверия используется одно из шести чисел от 1 до 6:

1. Подтверждено другими источниками: подтверждено другими независимыми источниками; имеет смысл сам по себе; Соответствует другой информации по теме.

2. Вероятно, верно: не подтверждено; имеет смысл сам по себе; соответствует другой информации по теме.

3. Вероятно, верно: не подтверждено; имеет разумный смысл сам по себе; согласен с другой информацией по теме.

4. Сомнительно: не подтверждено; возможно, но не логично; Больше никакой информации по этому вопросу нет.

5. Невозможно: не подтверждено; не имеет смысла сам по себе; вопреки другой информации по этому вопросу.

6. Об истине судить нельзя: нет оснований для оценки достоверности информации.

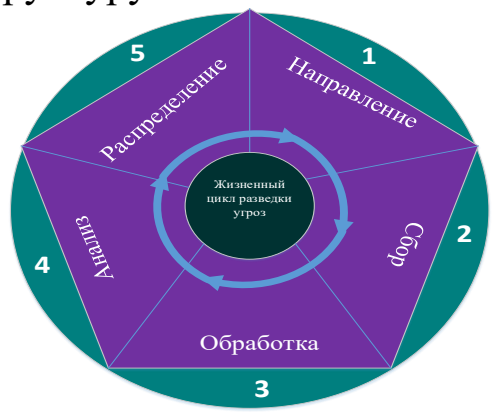
Совместимость. Собранная информация должна быть совместима с функцией CTI и ее требованиями. Даже для соответствующих ресурсов (таких как лента угроз NCSC) не весь предоставленный контент может быть полезен. Аналитикам рекомендуется использовать метрики, подобные репутации, для оценки релевантности для управления кормами, но в системе НАТО нет метрики релевантности. Каналы угроз часто содержат разнообразный контент — например, многие каналы угроз содержат контент, связанный с программами-вымогателями, нацеленными на отдельных лиц, а не на корпорации.

Качество. Последним соображением при обработке CTI является качество собранных данных. Ключевые области, которые необходимо учитывать, включают:

— Формат содержимого, например, адреса IPv4 должен быть XXX.XXX.XXX.XXX;
— Связанный контекст контента;
— Возраст контента;
— Точность содержания, т. е. «истинный» IOC в отличие от ложных срабатываний; Частота обновления ленты.

Следует уделить внимание обеспечению того, чтобы данные собирались в надлежащих форматах. Источники, которые предоставляют искаженные данные, постоянно сопоставляются (и, следовательно,автоматически обработанные) форматы следует рассматривать как более низкое качество, чем те, которые предоставляют контент. Например, указатели всегда имеют специальные правила форматирования; Адреса IPv4 должны быть в формате XXX.XXX.XXX.XXX, а доменные имена всегда содержат @. Связанный с фидом контекст должен способствовать его качеству. Если фид регулярно сообщает только метрики IP-адресов, его следует считать более низким качеством, чем фид, который предоставляет полную контекстную информацию, такую как угрозы, кампании и домены, связанные с метрикой IP.

Возраст содержимого также важен и должен обрабатываться в контексте типа IOC, например, IP-адреса имеют короткое время жизни, хэши имеют более длительное время жизни и т. д. Каналы угроз, которые обычно предоставляют устаревший контент, должны быть лишены приоритета.Это особенно очевидно в контексте облака, где злоумышленники регулярно переворачивают атакующую инфраструктуру.



Анализ. Необходимо проанализировать собранные данные для производства продуктов CTI. Разведка не может обеспечить абсолютную точность. Поэтому важно провести тщательный анализ, чтобы сделать какие-либо выводы..Целью этапа анализа является

получение обработанного контента и преобразование его в действенные интеллектуальные продукты для использования клиентами и партнерами функции CTI.

Распределение. Распределение берет продукты со стадии анализа и распространяет их среди соответствующих клиентов функции CTI на стратегическом, оперативном и тактическом уровнях. Помимо внутренней отчетности, отделы также должны учитывать преимущества обмена соответствующими CTI (особенно операционными и тактическими CTI) извне, чтобы предотвратить атаки внутри отрасли или сообщества. Общая информация об атаке на один отдел, такая как конкретный субъект угрозы, его мотивы, инфраструктура, TTP и принадлежность к IOC, позволяет другим отделам улучшить свою обороноспособность и снизить риск компрометации.

Распространение продукции CTI. Метод и формат распространения будут варьироваться от клиента к клиенту, чтобы соответствовать их индивидуальным требованиям CTI. Например, подробный прозаический отчет о тенденциях правительственных атак может быть отправлен в SMT по электронной почте; Низкоуровневый отчет в формате PDF о TTP соответствующего субъекта угрозы может быть предоставлен группе управления безопасностью и реагирования на инциденты через электронную систему управления документами и записями (EDRMS, например SharePoint); а утвержденные IOC могут быть отправлены в CSOC и Центр сетевых операций (MOC) через STIX/TAXII. Агрессивное внутреннее распространение CTI является ключом к оптимизации преимуществ функции. В одном из обсуждений примерно 25% всех сотрудников назвали отдел, который получил какую-либо форму продукта CTI по электронной почте. Было отмечено, что распределение CTI по всем опрошенным отделам имеет решающее значение для его полезности.

Доверительные отношения. Совместное использование CTI имеет много преимуществ, как упоминалось выше; однако это, вероятно, потребует прямого или косвенного обмена конфиденциальной информацией между отделами. Такое совместное использование требует установления уровня доверия между отделами, при котором совместно используемая информация обрабатывается надлежащим образом и используется только в явно

разрешенных целях. Существует также элемент риска, связанный с обменом знаниями злоумышленников, например, если злоумышленник обнаружит, что TTP был идентифицирован и приняты контрмеры, он может переключиться на новый и неизвестный TTP.

Один из способов завоевать доверие — закрытые форумы по обмену.Например, CiSP выбирает, какие НПО могут быть членами, а MISP позволяет создавать произвольные группы доверия. Несмотря на то, что следует принимать во внимание приведенные выше соображения, ключом к успеху CTI является быстрый обмен контентом, чтобы гарантировать, что все потребители могут использовать его, пока они могут. Для этого может потребоваться создание отношений между компаниями, которые обычно не сотрудничают, например, являются прямыми конкурентами в одних и тех же отраслях.

Протокол светофора. Протокол светофора основан на Координационном центре безопасности национальной инфраструктуры Великобритании, Центре защиты национальной инфраструктуры (CPNI), чтобы поощрять обмен конфиденциальной информацией и способствовать укреплению доверия. Текущий стандарт теперь определяется Форумом для групп реагирования на инциденты и безопасности (FIRST) Standards Definitions and Usage Guide. TLP использует четыре цвета, чтобы определить границы совместного использования и указать, когда и как может быть передана конфиденциальная информация. Он оптимизирован для удобочитаемых данных, но STIX и MISP также включают TLP. Важным принципом TLP является то, что источник отвечает за то, чтобы получатели понимали и соблюдали символы TLP.

Четыре символа TLP:

— TLP: КРАСНЫЙ — только для участников, не для разглашения;
— TLP: AMBER — ограниченное раскрытие информации, ограниченное отделами или организациями участников;
— ТЛП: зеленый- ограниченное раскрытие, ограниченное определенным сообществом обмена информацией;
— ТЛП: БЕЛЫЙ -раскрытие не ограничено.

Соответствие классификации государственной безопасности для CTI.Государственная классификация

безопасности заменяет Схему маркировки государственной защиты (GPMS). GSC указывает на конфиденциальность данных и определяет ключевые меры безопасности (административные, физические и логические), необходимые для надлежащей защиты активов.

GSC имеет три классификации, как описано ниже:

— ОФИЦИАЛЬНО. Большая часть данных генерируется или обрабатывается государственным сектором. Это включает обычные деловые операции и услуги, некоторые из которых могут иметь вредные последствия в случае потери, кражи или публикации в СМИ, но не подвержены высокому риску. Некоторая ОФИЦИАЛЬНАЯ информация является особенно конфиденциальной и требует дополнительных мер контроля для реализации принципа «необходимо знать» — она должна быть помечена как ОФИЦИАЛЬНАЯ КОНФИДЕНЦИАЛЬНАЯ;

— СЕКРЕТ — это очень конфиденциальная информация, которая оправдывает усиленные меры безопасности для защиты от конкретных и высокоэффективных субъектов угроз. Например, когда компромисс может нанести серьезный ущерб военному потенциалу, международным отношениям или расследованию серьезной организованной преступности;

— СОВЕРШЕННО СЕКРЕТНО -Правительство Его Величества(ПЕВ) наиболее конфиденциальные данные, требующие высочайшего уровня защиты от самых серьезных угроз.

Например, в случаях, когда компрометация может привести к массовым человеческим жертвам или создать угрозу безопасности или экономическому благополучию страны или дружественных стран.

GSC предназначен для обеспечения надлежащей защиты государственных данных. Это означает, что обязательные меры контроля требуются пропорционально каждой классификации. Это по замыслу предотвращает совместное использование данных и не требует гибкости в управлении. Поэтому департаментам рекомендуется не определять CTI с помощью GSC в обычном порядке, а вместо этого использовать TLP, если только это не требуется операционными ограничениями.Для этой

инфраструктуры должно существовать специальное правило белого списка, чтобы предотвратить блокировку законной активности.

§ 2.2. Каталогный подход.

Инженерные системы характеризуются высоким уровнем технической сложности, социальной сложности и сложными процессами, направленными на выполнение важных функций в обществе. Учитывая их долговечность, они сталкиваются с большой неопределенностью на стратегическом, тактическом и оперативном уровнях. Инфраструктурные системы играют важную роль в любом современном городе, обеспечивая аварийно-спасательные службы (например, станции скорой помощи, больницы), производство и распределение энергии (например, электростанции и национальная сеть), телекоммуникации (например, сети мобильной связи — это особый класс инженерных систем, которые поддерживаю я). Транспорт (например, аэропорты, дороги, мосты, шоссе) и жилищная деятельность (например, проекты в сфере недвижимости).

Инфраструктурные системы находятся в центре внимания данного методологического руководства. Начальный этап принятия проектных решений по инженерным системам является очень сложной задачей. На рис. 2.3 показаны различные этапы стандартного проектирования и процесса оценки. Это действия по концептуальному проектированию и архитектуре, которые обычно выполняются на этапе разработки системы перед этапом более детального проектирования системной инженерии.

Он начинается с первоначального проекта, затем определяются ключевые факторы неопределенности, влияющие на жизненный цикл, поскольку менеджеры со временем корректируют систему, чтобы приспособиться к изменяющимся условиям.признает адаптацию и опирается на различные показатели для экономической оценки (например, чистая приведенная стоимость или чистая приведенная стоимость) и/или неэкономические показатели (например, время реагирования аварийно-спасательных служб). Такой процесс включает моделирование и оптимизацию крупных инфраструктурных проектов (например, заводов, сетей и т. д.) с учетом нескольких возможных вариантов проектирования на этапе 1 и сценариев неопределенности в долгосрочной перспективе

(например, рыночный спрос, цена, правила) на этапе 2. включает рассмотрение. Как было показано на шаге 3, может быть много архитектур и режимов работы (например, количество и размер заводов, маршрут транспортных средств в дорожной сети и т. д.).

Норма прибыли (IRR), NPV, рентабельность инвестиций (ROI) и т. д., показанные на шаге 4).

Рисунок 2.3. Полная аналитическая задача проектирования инженерных систем в рамках концептуального проектирования

Обычный подход к проектированию и анализу систем заключается в упрощении всей аналитической задачи, что делает ее более решаемой.

Вместо того, чтобы рассматривать несколько сценариев периодических данных, проекты часто оптимизируются для максимального прогноза ключевых факторов неопределенности. Традиционные подходы к оценке проектов, основанные на анализе дисконтированных денежных потоков (DCF), такие как NPV, не учитывают периодическую реакцию менеджеров на повышение производительности системы.

Кроме того, проектные решения часто основываются на одной оценочной метрике, такой как IRR, ROI или NPV. Такая практика может привести к неоптимальному выбору конструкции или полностью исключить потенциальные решения, обеспечивающие хорошую производительность в течение жизненного цикла. За последние два десятилетия были предприняты значительные усилия

по совершенствованию стандартных методов проектирования и оценки проектов за счет более точного учета неопределенности и гибкости при проектировании инженерных систем. Гибкость позволяет системе активно изменяться и адаптироваться к меняющимся условиям, рынкам, нормам и технологиям.

Это может повлиять на распределение возможных результатов, выбрать схемы, которые сводят к минимуму подверженность неблагоприятным условиям (например, покупка страховки) и позволить системе использовать благоприятные возможности (например, колл-опционы на приобретение акций), улучшая ожидаемую производительность жизненного цикла.

Концепция проектирования гибких систем заключается в следующем:

а) стратегия управления неопределенностью (например, постоянный или временный отказ от системы, расширение емкости, изменение проектной конфигурации для улучшения резервирования и т. д.), аналогичная варианту фактического «включения» системы;

б) инструмент, который позволяет проектировать и управлять аналогично реальной опции в системе. Несколько исследований показали улучшение на 10-30% по сравнению с результатами стандартных методов проектирования и оценки в соответствии с традиционной оценкой ROA.

Как можно разработать структурированный процесс, позволяющий выполнять расширенный анализ конструкции инженерных систем с четким учетом неопределенности и гибкости, повышающий эффективность жизненного цикла и аналитически прослеживаемый по сравнению со стандартными подходами к проектированию и оценке?» Второстепенный вопрос: «Какое повышение эффективности жизненного цикла предложенного механизма применительно к анализу типовой технической системы и как оно соотносится с другими конкурирующими методами?»
Предложенное решение*каталог дизайна*на основе концепции.

Каталог состоит из набора операционных планов, которые сочетают в себе гибкую архитектуру проектирования и контрольные реакции, соответствующие шаблонам неопределенности, которые проектировщики хотят ожидать.

Этотпредлагаемый здесь проектный каталог разрабатывается

путем выбора набора оперативных планов или моделей, которые в совокупности рационально учитывают определенные сценарии неопределенности. Это ускоряет анализ наиболее подходящих планов, позволяет аналитикам рассматривать больше вариантов конструкции и находить лучшие проектные решения с улучшенными эксплуатационными характеристиками, не полагаясь на передовые методы, основанные на стохастическом программировании или оптимизации на основе моделирования. Предлагаемое решение представляет собой нечто среднее между простейшим набором допущений, обычно используемых при проектировании и оценке, и полной аналитической задачей, изображенной на рис. 2.3. Это известно разработчикам системы и вероятность (например,

Он опирается на ряд возможных сценариев, которые достаточно малы, чтобы их можно было анализировать, но в то же время достаточно широки, чтобы принимать обоснованные проектные решения. Цель состоит в том, чтобы предоставить аналитикам практический подход к быстрому улучшению жизненного цикла, ограничивая при этом вычислительные затраты, связанные с расширенным анализом, и при этом явно учитывая гибкость.

Процесс оформления каталога.2.4-На рисунке показан предлагаемый процесс на основе каталога, который состоит из пяти шагов, основанных на процессе, описанном на рисунке 2.3, и расширяет его:

1) разработка базовой модели системы измерения эффективности жизненного цикла;
2) найти сценарии неопределенности, оказывающие наибольшее влияние на жизненный цикл,
3) выявление и создание потенциальных источников гибкости в дизайне и управлении;
4) найти наиболее подходящий гибкий план работы для каждого сценария и создать каталог дизайна;
5) оценка жизненного цикла и сравнение с базовым проектом в условиях неопределенности.

Следующее описание предлагает популярные методы, используемые в промышленности и научных кругах. Однако этот выбор в конечном итоге зависит от организации, реализующей

процесс.

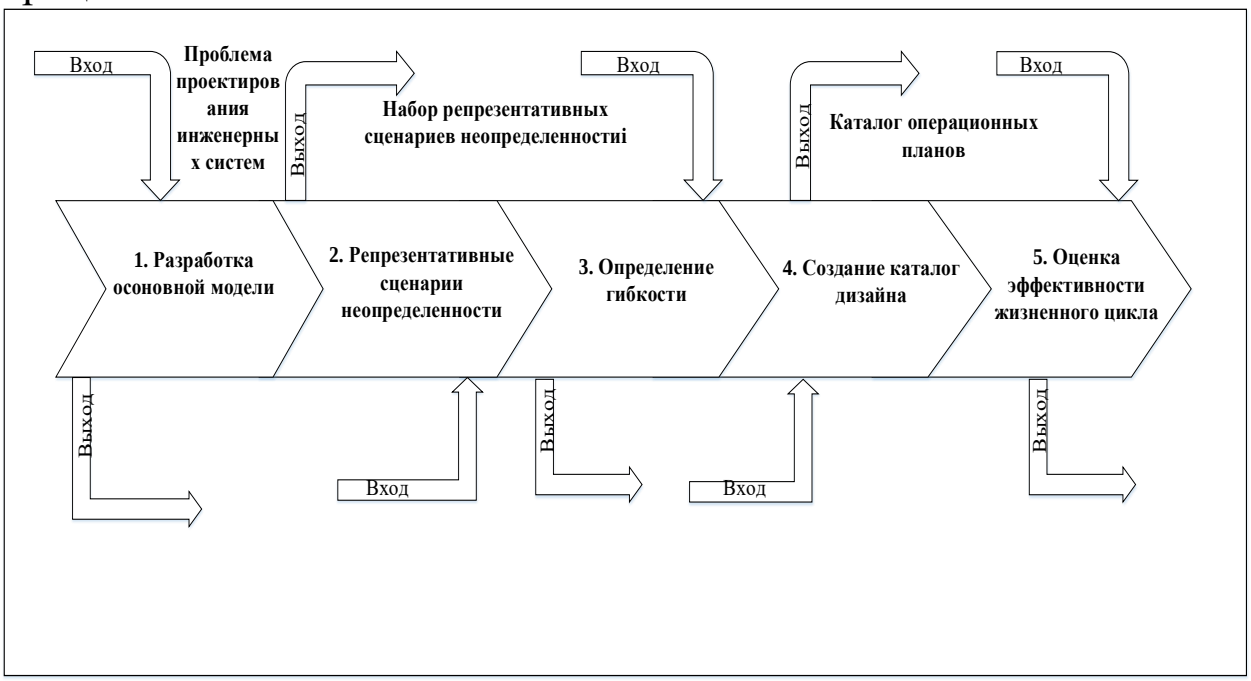


Рисунок 2.4. Подход каталога проектов к проектированию инженерных систем

Целью шага 1 является разработка базовой модели для измерения характеристик жизненного цикла системы при различных сценариях. Этот шаг рассматривается как введение в проблему проектирования инженерных систем и создает модель производительности вместе с идентифицированными факторами неопределенности, которые могут повлиять на жизненный цикл. В промышленности анализ DCF обычно используется для оценки ожидаемых экономических показателей, но могут использоваться и другие методы моделирования, такие как агентное моделирование, организация очередей, автоматизированное проектирование, моделирование дискретных событий и т. д.

Цель шага 2 — найти набор репрезентативных сценариев, охватывающих диапазон факторов неопределенности, влияющих на процесс жизненного цикла.

Входными данными для этого этапа являются ключевые факторы неопределенности, смоделированные как часть модели производительности, а выходными данными является репрезентативный набор таких сценариев, используемых на этапе 3 для создания концепций проектирования гибких систем. Поиск такого репрезентативного набора может быть выполнен с использованием популярных в отрасли методов, таких как планирование сценариев Shell, вероятностный анализ или

рассуждения на основе конкретных случаев, основанные на обсуждениях со специалистами по проектированию в проектной организации и/или с заказчиком. Здесь предлагается систематический процесс, основанный на планировании сценариев – предлагаемые подробности см. в Приложении. Первоначально разработанный и используемый в Shell, он включает в себя модифицированный процесс.

а) определение масштаба проблемы;
б) определить ключевые заинтересованные стороны;
в) выявить ключевые тенденции;
г) выявить ключевые неопределенности;
д) создание начальных тем сценария,
е) разработка количественных моделей и
час) продвижение к принятию решений.

Хотя конкретного метода, представляющего передовую практику, не существует, было предложено несколько методов, основанных на анализе реальных вариантов, предложении, мозговом штурме и/или матрице структуры проектирования (DSM), а литература включает в себя сложные системы, такие как парки беспилотных летательных аппаратов. полученный. подробно обсуждаются самолеты, проекты по развитию недвижимости и инфраструктурные системы преобразования отходов в энергию, что помогает предоставить рекомендации по соответствующим процедурам выбора на основе системного и аналитического контекста.

Целью шага 4 является создание каталога проектов. Входными данными являются интересующая(ие) концепция(и) проектирования гибких систем и расширенная модель производительности, а выходными данными является каталог операционных планов. Предпочтительный гибкий операционный план находится для каждого репрезентативного сценария, чтобы смоделировать способность менеджеров изменить операционный план в условиях неопределенности. Каждый план также моделирует возможную стратегию устойчивости для использования в данном сценарии.

Таким образом, в предлагаемой структуре гибкость применяется на двух уровнях:

— возможность переключения между оперативными планами;
— способность адаптироваться в рамках конкретного

оперативного плана.

Этот шаг концептуально подобен шагу дискретизации, часто выполняемому при решении стохастических программ. На шаге 4 можно использовать несколько механизмов для создания каталога.

Последствия использования различных алгоритмов могут повлиять на качество решения, и/или этот измененный процесс, используемый в Shell, включает:

а) определение масштаба проблемы;
б) определить ключевые заинтересованные стороны;
в) выявить ключевые тенденции;
г) выявить ключевые неопределенности;
д) создание начальных тем сценария,
е) разработка количественных моделей и
час)продвижение к принятию решений.

Необходимо выбрать достаточное количество сценариев, чтобы отразить характер вариантов и диапазон возможных результатов (например, 5-15 сценариев).Чтобы избежать вычислительной нагрузки, связанной с методами моделирования и стохастического программирования, не следует выбирать слишком много сценариев. Этот шаг концептуально основан на методе аппроксимации выборочного среднего, используемого в стохастическом программировании. Он направлен на сокращение количества сценариев, рассматриваемых для оптимизации, и, следовательно, на вычислительную нагрузку.

На шаге 4 можно использовать несколько механизмов для создания каталога. Выбор алгоритма зависит от характера задачи проектирования (например, дискретные или непрерывные переменные, линейная или нелинейная целевая функция, детерминированная или стохастическая).

Последствия использования разных алгоритмов могут повлиять на качество решения и/или требуемые 10 вычислительных уровней. Ссылочные тексты содержат рекомендации по наилучшему алгоритму для использования в зависимости от времени, типа проблемы и ресурсов, доступных аналитику.

Цель шага 5 состоит в том, чтобы сравнить результаты, полученные с использованием каталога, с результатами, полученными для базовой модели на шаге 1, чтобы измерить улучшение, вызванное каталогом дизайна, по сравнению со

стандартным проектом и оценкой, если таковая имеется. Этот шаг считается входом в каталог проектов и создает предпочтительный набор гибких проектов и каталогов, которые повышают ценность, рассматриваемую на этапе детального анализа процесса системного проектирования. Это делается путем моделирования широкого спектра сценариев неопределенности, назначения одного оперативного плана для каждого сценария и измерения производительности системы по каждому плану/сценарию. Этот шаг аналогичен тестированию вне выборки в стохастическом программировании.

Каталогизированный и некаталогизированный анализ для определения ценности гибкости при использовании каталога и гибких операционных планов.можно передать. Распределение результатов можно сравнить, чтобы определить, как устойчивость влияет на предлагаемый дизайн (т. е. защищает ли он от негативных условий, способствует ли он и тому, и другому использованию положительных возможностей?). Многокритериальная оценка помогает сравнивать варианты дизайна или каталоги с учетом разных профилей риска при принятии решений с использованием разных показателей оценки (например, средней эффективности, 5-го или 95-го процентиля и т. д.).

Этот проект развития реальной инфраструктуры был инициирован для удовлетворения потребностей в парковке потенциальных новых клиентов и посетителей торгового центра. Поскольку потенциальный рост клиентов/посетителей неизвестен, проектировщики и архитекторы системы предусмотрели в системе гибкость, позволяющую разместить в торговом центре дополнительные этажи и вместимость, что позволило разместить в торговом центре больше клиентов, чем планировалось изначально.Они предусмотрели больше парковочных мест. Они показали, что гибкий дизайн может создать дополнительную экономическую ценность в условиях неопределенного роста спроса, в отличие от системы, разработанной с оптимальной или стохастически оптимальной фиксированной мощностью.

§ 2.3. Каталог политики кибербезопасности

Проблемы киберуправления.Интернет начинался как Сеть Агентства перспективных исследовательских проектов (ARPANET), финансируемая военными США сеть, предназначенная для

выживания в случае ядерной атаки. Он быстро стал инструментом для обмена информацией между армейскими исследователями компьютерных наук, их подрядчиками и академическими партнерами. Те, кто придумал коммуникационный протокол, приняли его как формальный процесс, управляемый Инженерной группой Интернета (IETF). Они были опубликованы как запросы на комментарии, что позволило другим быстро изучить новые протоколы, а также расширить их.

Несмотря на то, что большая часть инфраструктуры и функций Интернета децентрализована (замысел дизайна Интернета), требуются определенные функции централизованного планирования и координации. Наиболее заметными являются распределение доменов (т. е. http://www.whitehouse.gov) и номеров (т. е. интернет-протокола или IP-адреса). Эти координирующие функции изначально выполнялись Стэнфордским исследовательским институтом (SRI), подрядчиком Министерства обороны США. В 1972 году эти функции были переданы Администрации адресного пространства Интернета (IANA) под руководством Джона Постела из Института информационных наук (ISI) Университета Южной Калифорнии. Это привело к постепенному роспуску ARPANET. В 1995 году были сняты последние ограничения на интернет-трафик.

В 1998 г. Национальное управление по телекоммуникациям и информации (NTIA), агентство Министерства торговли США, начало процесс создания стабильной модели управления функциями IANA, кульминацией которого стало создание в 2000 г. Интернет-корпорации для назначенных Имена и номера (ICANN). 30 января 1998 г. ICANN выпустила зеленую книгу политики с комментариями: «Предложение по улучшению технического управления именами в Интернете». В результате модель ICANN представляет собой уникальную модель управления с участием многих заинтересованных сторон для централизованных компонентов Интернета, в которой правительства, корпорации и отдельные пользователи Интернета работают вместе над созданием политик, регулирующих Интернет снизу вверх.

Легко увидеть параллели между управлением Интернетом и глобальной телефонной системой. Потому что вы можете звонить напрямую на международном уровне, и каждая страна имеет везде

телефонную связь для выполнения своей личной миссии по соединению своих граждан с миром.Существует комитет сотрудничающих телекоммуникационных компаний с общей глобальной целью Эти компании образовали Международный союз электросвязи в 1865 году. В 1947 году МСЭ стал частью тогда еще новой Организации Объединенных Наций (ООН). Организация Объединенных Наций/МСЭ представляет собой модель управления по принципу «сверху вниз», возглавляемую правительством. Напротив, модель ICANN/AoC делает упор на формирование политики снизу вверх. представляет собой «международную модель управления с участием многих заинтересованных сторон», которая поддерживает Правительства стран мира участвуют в модели ICANN через Правительственный консультативный комитет (GAC), который является одним из нескольких консультативных комитетов ICANN, определяющих политику в отношении Интернета. Некоторые утверждают, что модель МСЭ/ООН является правильной моделью управления Интернетом, в то время как другие утверждают, что модель ICANN/AoC оптимальна.

Ключевым вопросом политики кибербезопасности является модель управления Интернетом и, в частности, способ участия мировых правительств. Одной из самых уникальных характеристик Интернета является то, что он распространен по всему миру; любая интернет-машина может взаимодействовать с другой интернет-машиной, и ввод http://www.cnn.com в Канзасе, Сингапуре, Берлине и Москве приведет вас куда-нибудь. Технической причиной такого глобального сотрудничества является наличие централизованных координационных функций. Если правительства расходятся во мнениях относительно централизованных функций координации и начинают использовать разные стандарты/процедуры, Интернет может распасться на множество или частично связанные части. Некоторые правительства обеспокоены цензурой, национальным суверенитетом и оппозицией правлению США.

Кибер-проблемы пользователей.Нетворкинг — это пользователь киберпространства. Около 30% населения мира подключено к Интернету. В дополнение к традиционным деловым отношениям, которые переместились в онлайн, за последние два десятилетия Интернет создал новые бизнес-модели электронной коммерции. К ним относится использование традиционных бизнес-

мест, то есть интернет-магазинов. В то время как реклама электронной коммерции первоначально отражала связи с общественностью и маркетинговую деятельность до Интернета, несколько новых маркетинговых моделей также появились там, где Интернет не вездесущ. Это информационные сервисы, которые собирают данные из одного уголка киберпространства и продают их в другой. Основным заказчиком этих данных является рекламная индустрия.

Проблемы безопасности для киберпользователей в основном возникают из-за их неожиданного подключения к электронной коммерции. Все эти подключения выполняются с помощью программного обеспечения, и это программное обеспечение идентифицирует ошибку или уязвимость, которая позволяет любому злоумышленнику отслеживать поток данных пользователя или компрометировать транзакцию электронной торговли. Мониторинг потока данных через многие из этих конечных точек предоставляет информацию, которую можно использовать для дальнейших атак, таких как отслеживание имен пользователей и паролей, используемых для выдачи себя за другое лицо и кражи личных данных.

Таблица 2.4

Вопросы политики кибербезопасности, связанные с электронной почтой и обменом сообщениями

Политика	Заявление	Причины конфликта
Все организации, участвующие в электронной коммерции, должны предлагать своим клиентам возможность проверки серверов электронной почты с использованием стандартных протоколов.	Эта политика требует, чтобы компании электронной коммерции публиковали ключи для своих почтовых серверов в DNS.	Потребители имеют право убедиться, что сообщения от поставщиков услуг и других поставщиков не являются мошенническими. Потребители обычно не имеют программного обеспечения для проверки почтового сервера и поэтому

		должны полагаться на своего интернет-провайдера или поставщиков услуг хостинга для проверки. Следовательно, это требование лучше оставить на усмотрение сильных мира сего в сфере электронной коммерции.
Все сообщения электронной почты от имени организации или о ней должны отправляться с адреса электронной почты, поддерживаемого организацией.	Требуется, чтобы сотрудники организации использовали системы электронной почты своей организации для ведения бизнеса организации и чтобы они использовали имя организации на сайтах социальных сетей, личных мобильных телефонах и других общедоступных или частных сетях.	Эта политика позволяет контролировать все коммуникации. Это сокращает количество работников, которые могут быть привлечены к административной ответственности. Эта политика ограничивает возможности людей, которые не могут получить доступ к корпоративным услугам из-за командировок или перерывов в общении.
Электронная почта и квитанция о прочтении должны содержать	Различные договоры и постановления требуют от организаций,	Возможность использования электронных квитанций о

подтверждение доставки электронной информации.	направляющих уведомления, доказать, что лицо, которому было отправлено уведомление, действительно его получило.	доставке и прочтении в качестве подтверждения доставки снизит расходы для организаций, несущих юридическую ответственность за уведомление физических лиц в различных секторах, включая банки и Текущие стандарты аутентификации цифровых записей требуют сочетания доказательств управления ключами, криптографических алгоритмов и процедур организационного контроля. Инфраструктура для этого отсутствует
Люди должны иметь возможность размещать свои адреса электронной почты в списке, который запрещает маркетологам отправлять им нежелательные электронные	Это эквивалент национального реестра запрета звонков для запросов по электронной почте. Этот тип списка в настоящее время используется для телефонных номеров.	Чтобы защитить адреса электронной почты от нежелательных запросов, механизм применения политики «не отправлять электронную почту» значительно

письма.	Маркетинговые компании должны удалить телефонные номера из своих списков «не звонить» из своих кампаний по телефонному маркетингу.	сократит количество входящих рекламных объявлений, получаемых в настоящее время по электронной почте. Эта политика должна упростить обнаружение незаконного спама. Принудительное применение политик экономит пропускную способность и ресурсы хранения. Электронная почта — это эффективный способ общения с потребителями, и потребители, которые выразили свои предпочтения в отношении продуктов и услуг посредством различных онлайн-действий, будут продолжать интересоваться этой политикой. Может быть трудно провести черту в отношении того, что представляет собой интерес, и поэтому реализация

		политики будет затруднена. Основным источником дохода для некоторых предприятий электронной коммерции является список адресов электронной почты, который они могут создать на основе своего интернет-трафика. Стоимость этих активов будет значительной
Службы обмена сообщениями в Интернете должны позволять пользователям выбирать сообщество для обмена сообщениями и исключать все сообщения за пределами сообщества.	Это эквивалент отдельного «белого списка» для каждого потенциального получателя электронной почты. Только те, кто находится в списке, могут отправить электронное письмо или сообщение получателю.	Эта политика позволяет пользователям Интернета управлять своими ресурсами и сокращать количество спам-сообщений. Это экономит как пропускную способность, так и ресурсы хранения. Поскольку не существует общепринятого метода проверки подлинности для электронной почты или обмена сообщениями, любой может обойти

		эту политику, выдав себя за любое имя пользователя из белого списка. Поэтому его нельзя реализовать.
Пользователи служб обмена сообщениями должны использовать только те доменные имена в Интернете, которые они зарегистрировали.	Это ограничивает использование адресов «От» в электронной почте адресами, зарегистрированными в ICANN отправителя.	Ограничение адресов ограничивает инновации в маркетинге электронной коммерции, не обеспечивая дополнительной безопасности, поскольку для временного удовлетворения этого требования можно легко использовать добавление льготного периода (AGP).
Некоторые отправители фишинговых сообщений электронной почты подлежат уголовному наказанию, и наказания должны быть пропорциональны преступлениям, совершенным в	Эта политика налагает штраф за кражу личных данных на тех, кто отправляет фишинговые электронные письма.	Фиш-эмейлеры — это небольшая часть крупного организованного преступного сообщества. Хотя их преступление может казаться невиновным, оно является предпосылкой для нападения на человека при

результате потенциальной кражи информации у получателей фишинговых сообщений.		отягчающих обстоятельствах и следует воспринимать так же серьезно, как и само нападение. Отправитель фишинговой электронной почты, скорее всего, является бизнесом, который рассылает массовые электронные письма. для разных клиентов и не может различать законных и незаконных клиентов и не должен нести бремя идентификации интернет-преступников. Кроме того, простая отправка электронного письма не гарантирует взаимодействия с пользователем.

С точки зрения безопасности в среде электронной коммерции существует четыре основных типа пользователей: покупатель, продавец, разработчик и хакер. Цель злоумышленника — получить незаконную прибыль от одного или нескольких из трех других типов пользователей. Вредоносное ПО стремится использовать уязвимости в программном обеспечении, конфигурации приложений, оборудовании и человеческом факторе. Атаки на

электронную торговлю происходят постоянно. На первой странице появляются только самые интересные случаи мошенничества с самыми тяжелыми последствиями для потерпевших. Тем не менее, киберпреступная сеть информационной безопасности имеет ту же повседневную активность, что и незаконный оборот наркотиков. «Угроза нулевого дня» В своей книге два репортера USA Today описывают это явление как продукт трех архитектур: эксплуататоров, активаторов и форвардеров (Acohido and Swartz 2008). Злоумышленники совершают кражу данных и мошенничество.

Экспедиторы — это технологи, которые определяют основную причину с технической точки зрения, но они также могут быть разрушителями или защитниками. может регулярно красть информацию невольных потребителей. Эксплуататоры эксплуатируют не только потребителя, ставшего жертвой кражи личных данных, но и низкоуровневые социальные неудобства. Они используют социальные бестактности, чтобы автоматически снимать наличные деньги клиентов в банкоматах или заказывать предметы роскоши по кредитным картам ничего не подозревающих клиентов. злой вдохновитель, контролирующий три или более уровня организованной преступной структуры над социальными преступлениями, никогда не будет пойман. Потребитель остается с поврежденным кредитом, а также потерянным временем и деньгами, в то время как активист утверждает, что существуют меры риска для защиты бизнеса.

В этом разделе вопросы кибербезопасности пользователей разделены на шесть подразделов: ложная реклама, выдача себя за другое лицо, надлежащее использование, киберпреступность, географическое положение («гео-местоположение») и конфиденциальность.

Ложная реклама — это анаграмма слов «вредоносная» и «реклама».

Выдача себя за другого связана с различными онлайн-мошенничествами, от анонимных публикаций до захвата аккаунта. Оно нацелено на распространенное поведение в Интернете, которое некоторые считают антиобщественным и которое еще официально не рассмотрено законодателями. Киберпреступность фокусируется на организованной преступной деятельности, распространенной в

электронной коммерции. Определение геолокации интернет-пользователей, как потребителей, так и преступников, чрезвычайно сложно и связано с уникальными политическими проблемами. Конфиденциальность — одна из проблем, которая вызывает дебаты о политике кибербезопасности в отношении геолокации, но конфиденциальность — это гораздо более широкий набор вопросов, и поэтому она заслуживает отдельного раздела.

Вопросы киберконфликта.Кибервойна — это общий термин для обозначения конфликтов и принуждения в киберпространстве, где программное обеспечение, компьютеры и сети являются средством или целью. Он шире, чем кибервойна, и включает в себя все конфликты и принуждение между государствами и группами в стратегических целях в киберпространстве, где программное обеспечение, компьютеры и сети являются как средством, так и целью. В киберконфликте участвуют национальные государства, активно сражающиеся друг с другом в киберпространстве в целях национальной безопасности. Не все киберконфликты переходят на уровень вооруженных сил, например крупномасштабный кибершпионаж. Киберконфликт не ограничивается государствами и предприятиями, а любыми отдельными, слабо связанными социальными сетевыми группами и всеми формами и формами. размер может быть между организациями. Когда люди участвуют в киберконфликте в политических целях или для защиты моральных убеждений, это называется активизмом. Ключевым моментом, который следует помнить при любом обсуждении киберконфликта, является то, что речь идет о людях, а не о компьютерах.

Киберконфликт часто ведется в стратегических целях, поскольку национальные государства проводят активные миссии в киберпространстве, чтобы конкурировать за техническое превосходство (Adair, Deibert et al., 2010). Эти конфликты могут обостряться или переходить на уровень вооруженных сил, например, крупномасштабный кибершпионаж или кибервойна. Этот термин киберконфликта позволяет более широко обсудить, как национальные государства и другие организованные группы с крупными операциями в киберпространстве сражаются в киберпространстве, сохраняя термин «война» только для наиболее значительных атак между национальными государствами. Этот термин помогает упростить понятия войны, шпионажа и других

нападений, поскольку он охватывает многие другие враждебные действия, но, тем не менее, идеально подходит для обсуждения роста и характера насилия, совершаемого в киберпространстве или через него. Более ранним термином для кибервойны была радиоэлектронная война, которая была более ограничительной, поскольку обычно использовалась только в ситуациях, когда киберпространство было и инструментом атаки, и целью.

В этом разделе рассматривается одна из основных движущих сил киберконфликтов — претензии на интеллектуальную собственность в киберпространстве. Споры об интеллектуальной собственности могут быть открытыми или скрытыми, и в этом случае они классифицируются как кибершпионаж. Наиболее экстремальной формой киберконфликта является кибервойна.

Таблица 2.5

Вопросы политики кибербезопасности в отношении конфиденциальности

Заявление о политике	Объяснение	Причины конфликта
Национальные правительства принимают законы, гарантирующие, что компании не используют информацию о клиентах иначе, чем это необходимо для проведения транзакций или предоставления услуг, если только клиент не отказался от такого обмена.	Компании обычно продают информацию о своей клиентской базе маркетинговым компаниям и/или настраивают пользовательский опыт на основе данных, собранных или приобретенных по личным характеристикам.	Этот тип опции «Не отслеживать» является важной частью права потребителя на неприкосновенность частной жизни. Эта политика не только обеспечивает конфиденциальность, но и помогает предотвратить распространение данных на дополнительные объекты, скомпрометированные злоумышленниками. Поскольку клиент

		никогда не имел дело со взломанной организацией, данные клиента не должны подвергаться такому риску. Совместное использование данных приносит пользу многим клиентам, поскольку позволяет создавать индивидуальные предложения с учетом интересов клиентов.
Государствам следует включать основные средства защиты конфиденциальности во все свои инициативы в области кибербезопасности.	Инициативы в области кибербезопасности часто сосредоточены на обнаружении и отслеживании активности. Эта политика требует, чтобы эти инициативы соответствовали политике конфиденциальности.	Хорошо продуманные инициативы в области безопасности также могут повысить конфиденциальность, поскольку хакеры и другие злоумышленники больше не имеют доступа к личной информации. Конфиденциальность является более насущной проблемой, чем безопасность для некоторых людей, в зависимости от ситуации. Время от времени будет возникать компромисс между

		безопасностью и конфиденциальностью, и сообщества должны найти наилучший компромисс между этими двумя похвальными целями в каждом конкретном случае.
Международные организации помогают согласовать усилия по классификации данных, чтобы лучше учитывать различия в законах о конфиденциальности между странами.	Разные страны определяют законы о конфиденциальности по-разному, поскольку у каждой страны есть свои законы, традиции и балансы.	Глобальные стандарты могут способствовать лучшему пониманию требований к конфиденциальности, улучшению конфиденциальности для граждан и экономии за счет масштаба. Такая гармонизация может оказаться невозможной, потому что различия, скажем, между США, Китаем и даже союзниками оказывают экономическое влияние на их бизнес в области электронной коммерции, что значительно затрудняет гармонизацию между союзниками. Единый глобальный стандарт

		конфиденциальности может оказаться невозможным и нежелательным; однако международные организации могут помочь договориться об основных принципах
Национальным правительствам следует пересмотреть существующие законы, чтобы определить, как они применяются к кибербезопасности, и определить, есть ли в них пробелы и нужно ли их обновлять (например, сделать более нейтральными в отношении технологий).	Это требует пересмотра законов о кибербезопасности на национальном уровне. Некоторые законы могут нуждаться в обновлении; другие могут предложить новые решения проблем кибербезопасности.	Эта политика позволяет вам устанавливать правила безопасности для защиты конфиденциальности. социологи, а не технологи. Хорошим примером закона, который следует критически пересмотреть в контексте кибербезопасности, является Закон США об оборонном производстве и телекоммуникациях 1934 года. Выводы, выводы и рекомендации, вытекающие из такого обзора, должны информировать сотрудников законодательных органов о новых

		законах или поправках. старые. Часто пересмотр старых законов приводил к конфликту между защитниками конфиденциальности и безопасностью.
Политика конфиденциальности, размещенная на веб-сайте, должна быть запрошена и подтверждена ее соответствие.	Поскольку политика отличается от процесса и процедуры, простое отображение политики конфиденциальности не означает наличия технических средств защиты для ее реализации.	Политика конфиденциальности — это сегодняшняя змеиная нефть. Чтобы они имели хоть какую-то ценность в качестве инструмента потребительской оценки, они должны регулироваться. Политика конфиденциальности не носит договорного характера, а является заявлением о позиции безопасности компании. Условия использования программного обеспечения регулируются лицензионными соглашениями с конечным пользователем.
Надлежащий интернет-администратор должен	Хотя существует множество возможностей для сбора и продажи	Существует множество различных способов профилирования

предоставить людям возможность продавать информацию о себе, и не должно быть никаких торговых площадок для любой другой информации, позволяющей установить личность.	персональных данных, не существует единого инструмента, позволяющего получать от них прибыль.	людей в Интернете, и никому не должно быть позволено делать это без учета рекомендаций таких групп конфиденциальности, как Elektron. Информация об использовании веб-сайта собирается поставщиками электронной коммерции и принадлежит им по праву. Пока индивидуальная атрибуция не осуществляется с использованием имен или адресов (электронной почты), такая информация является ценной.
Каждый веб-сайт, который собирает информацию о пользователях, должен сделать собранные поля доступными для выбора пользователем или позволить ему отказаться.	Эта политика подчиняет все интернет-сайты положениям о конфиденциальност и финансовой информации, таким как Закон Грэма-Лича-Блайли (GLBA), который требует, чтобы информация использовалась только для целей	Политики отказа, реализованные для GLBA, часто были громоздкими и трудными для интерпретации. Уведомления о конфиденциальности, предусмотренные Законом о переносимости и подотчетности медицинского страхования (HIPAA),

	предоставления услуг непосредственно клиенту.	обычно игнорируются, поскольку альтернативой их подписанию является поиск альтернативного поставщика медицинских услуг. Эти политики должны предотвращать сбор информации по умолчанию и не должны требовать действий, если они не одобрены официально. Любая услуга, предлагаемая в Интернете, должна позволять пользователю отказаться от сбора личной информации, и если компании заявляют, что отсутствие доходов от рекламы делает невозможным выполнение этой политики, они могут это сделать.
Агентства по защите прав потребителей должны запретить ненужную персонализацию.	Эта политика требует, чтобы персонализация рассматривалась как личная информация, которая в настоящее	Поскольку посетители веб-сайта не платят за услугу, они не являются клиентами веб-сайта и, следовательно, не

	время сосредоточена в основном на финансовых вопросах.	считаются потребителями веб-сайта. Для агентств по защите прав потребителей приоритеты персонализации по сравнению с конфиденциальность ю включают прозрачность, определяемые пользователем элементы управления, повышенную безопасность, ограничения хранения данных и Согласие пользователя и/или способы раскрытия предоставлены.
Потребительские устройства не должны быть настроены с функциями домашнего телефона.	Такие продукты, как сотовые телефоны, электронные книги и игры, обычно собирают информацию, чтобы предоставить производителю или поставщику услуг информацию о взаимодействии пользователя с устройством или данные на устройстве.	Эта политика позволяет потребителям использовать устройства, не беспокоясь о том, что их личная информация однажды может быть скомпрометирована, даже для предотвращения атаки рекламы на их электронную почту. Многие клиенты

		потребительских устройств готовы позволить своим поставщикам услуг отслеживать их поведение в обмен на более персонализированные услуги. Было бы разумнее потребовать от разработчиков программного обеспечения раскрывать доступные поля данных.
Пользователи, которые добровольно подключаются к безопасным беспроводным услугам, не ожидают конфиденциальности.	Беспроводные услуги часто предоставляются таким образом, что подключенные пользователи могут видеть трафик друг друга. Он также доступен в некоторых предложениях услуг стационарной связи, но пользователи четко не предупреждены о такой возможности, как при подключении к беспроводной сети с помощью стандартных отраслевых методов.	Быстрое внедрение сетевых сервисов затруднило удовлетворение требований к пропускной способности сети. Широкое использование функций безопасности, предотвращающих подслушивание пользователей, замедлится Учитывая, что сетевое взаимодействие все чаще становится требованием конфиденциальности, неэтично предоставлять услуги,

		требующие от пользователей выбора между средствами к существованию и конфиденциальность ю.

Проблемы киберуправления.Несмотря на то, что военные добились бесконечных успехов в организации своих ресурсов вокруг своей миссии, самые продуманные планы развертывания военной киберзащиты могут потерпеть неудачу из-за их непреднамеренной зависимости от гражданской инфраструктуры. Пространства имен и системы нумерации, обеспечивающие инфраструктуру как государственных, так и частных телекоммуникаций, управляются частным сектором. Как профессиональная дисциплина, практика технологий относительно молода по сравнению с другими областями. У архитекторов программного обеспечения нет наставника или системы ученичества, как у архитекторов физических объектов. Консультантам по технологиям не нужно изучать свою профессию с помощью серии экзаменов, как это делают медицинские консультанты. Покупатель остерегается правило дня. Таким образом, область технологической практики неожиданно породила область технологической халатности. Расследования неправомерного использования технологий основаны на подозрении в невнимании руководства к вопросам безопасности. Например, они предоставляют доказательства в судебных делах, связанных с халатностью со стороны Федеральной торговой комиссии США.

Тем не менее, полувековой опыт специалистов по безопасности показал, что накоплен большой объем знаний в области кибербезопасности. Общий опыт работы с аналогичными технологическими архитектурами и операционными процессами привел к лучшим практикам и правилам, которые не следует отбрасывать, поскольку нет научной основы для их всеобщего признания. В этом разделе рассматриваются некоторые вопросы политики, которые регулярно возникают при управлении кибербезопасностью. Кибербезопасность уже давно используется для управления активами, контролируемыми компьютерными системами, и поэтому управление кибербезопасностью привыкло

применять сдержки и противовесы для обеспечения соблюдения фидуциарной ответственности за управление активами. Управление кибербезопасностью часто начинается с изучения технологических возможностей и системных требований. Это зависит от способности организации покупать, создавать или отдавать технологические компоненты на аутсорсинг, поэтому управление цепочками поставок является важнейшим требованием для успешного внедрения технологий. Часто управление кибербезопасностью пытается передать функции безопасности в области управления киберпространством, которые тесно связаны с защищаемыми активами. Однако эти попытки делегирования иногда терпят неудачу из-за отсутствия навыков безопасности в делегируемой области. Часто предлагаемым решением этой проблемы является некоторая сертификация или аккредитация специалистов по безопасности. Эти требования распространяются на поставщиков услуг и оборудования, встроенных в инфраструктуру корпоративного киберпространства. Сдержки и противовесы необходимы для защиты от рисков кибербезопасности. Большое количество исследований в области методов кибербезопасности предоставило успешные решения в области безопасности и побудило профессионалов принять руководящие принципы для разработки и эксплуатации системы безопасности. Однако, как обсуждалось в главе 3, необходимы дополнительные исследования и разработки, чтобы охватить существующие и новые сценарии использования киберпространства. Сдержки и противовесы необходимы для защиты от рисков кибербезопасности. Большое количество исследований в области методов кибербезопасности предоставило успешные решения в области безопасности и побудило профессионалов принять руководящие принципы для разработки и эксплуатации системы безопасности. Однако, как обсуждалось в главе 3, необходимы дополнительные исследования и разработки, чтобы охватить существующие и новые сценарии использования киберпространства. Сдержки и противовесы необходимы для защиты от рисков кибербезопасности. Большое количество исследований в области методов кибербезопасности предоставило успешные решения в области безопасности и побудило профессионалов принять руководящие принципы для разработки и эксплуатации системы безопасности. Однако, как

обсуждалось в главе 3, необходимы дополнительные исследования и разработки, чтобы охватить существующие и новые сценарии использования киберпространства.

Таблица 2.6

Вопросы политики кибербезопасности, связанные с кибервойной

Заявление о политике	Объяснение	Причины конфликта
Международные усилия по контролю над вооружениями должны быть сосредоточены на ограничении распространения технологий кибербезопасности.	Это политика кибербезопасности, как и политика ядерного оружия, распространение которого должно быть остановлено, и, таким образом, мир станет более безопасным местом.	Распространение наступательных кибервозможностей будет трудно, если вообще возможно, остановить. Их трудно обнаружить, они относительно недороги и могут быть разработаны в любом подвале или компьютерной лаборатории. Любое соглашение о прекращении выпаса скота практически невозможно проверить или обеспечить соблюдение. Усилия международного контроля над вооружениями должны быть сосредоточены не на самом оружии, а на ограничении круга допустимых целей и видов использования

		кибератак. Возможные рамки для этого включают существующие ограничения законов о вооруженных конфликтах или новые структуры, которые стремятся ограничить использование киберпространства. Определение терминов «боеприпасы» или «оружие» в кибербезопасности недостаточно понятно для эффективного применения этой политики. Этот тип политики был основой попыток ограничить распространение криптографических технологий в конце 1900-х годов. Эта политика имела непредвиденные последствия
Военное руководство должно обнародовать декларативную политику, которая	Декларативные политики могут включать такие элементы, как запрет на первое использование против	Декларативные политики могут использоваться для ограничения вариантов. Декларативные

поможет установить международные нормы и определить перспективы обороны.	широких общественных целей, отказ от использования вирусов или червей и отказ от атак, исходящих из защищенных объектов (таких как больницы).	политики повышают прозрачность и помогают развивать возможности и доктрину. Если есть доброе слово, то не обязательно отнимают, наоборот, правомерно ограничивают варианты, которые никогда не рассматриваются. Декларативные политики позволяют противникам предвидеть свои действия.
Военное руководство должно разработать и сообщить о стратегии национальной безопасности в киберпространстве, а также поддерживать политику и координировать свои действия с союзниками.	Стратегия национальной безопасности для киберпространства должна выделять ключевые решения и то, как они поддерживают согласованные цели. Необходимо обеспечить баланс между наступлением и обороной, роль ключевых организаций, координацию операций и взаимодействие с гражданскими властями и частными	Стратегии — это эффективные способы для =высшего руководства обеспечить прозрачность своих намерений. и руководит их бюрократией. Национальные стратегии в отношении киберпространства часто могут быть чрезмерно засекречены, что вызывает ненужное беспокойство со стороны, и

	лицами.	чрезмерно милитаризовать киберконфликт, поскольку он рассматривается как проблема, для решения которой лучше всего подходят военные.
Военное руководство должно координировать операции с организациями частного сектора.	Частный сектор доминирует в киберпространстве в отличие от других отраслей. В космосе, в воздухе и даже в открытом океане царит пустота. Даже на суше люди бегут от конфликтов, если могут. Таких возможностей нет в киберпространстве, которому создан и принадлежит сам «Космос».	Организации частного сектора необходимы для обеспечения национальной киберзащиты. Если они не доверяют военным стратегиям или технологиям, они могут вмешиваться в действия национального руководства, чтобы отменить или заблокировать программы, которые им не нравятся. Поскольку будущие киберконфликты могут вестись в их сетях и системах, тесная координация с ними имеет решающее значение для защиты. Военные стремятся засекретить все, и любой мандат на

		работу с частным сектором может привести к аргументам в пользу усилий по классификации, конкурирующих с усилиями частного сектора по обеспечению кибербезопасности для защиты доходов.
Военные должны широко координировать наступательные и оборонительные кибероперации, между кинетическими и кибероперациями, между наступательными и эксплуататорскими действиями, а также с гражданскими коллегами.	Координация с цепочкой поставок и владельцами целевых активов имеет решающее значение для любой военной операции. Это гражданские аналоги киберкоманд.	Каждое из этих действий необходимо из-за уникальной природы киберпространства. Мало того, что это новое и в значительной степени не проверенное, но последствия могут быть каскадными и затронуть непреднамеренные гражданские системы. Любые контратаки могут быть соразмерными со стороны противника, но могут быть направлены непосредственно на критический аспект принимающей страны.

		Координация с потенциально многими людьми из нескольких организаций безусловно, замедлит темпы кибероперацій. Военные кибермиссии не должны затрагивать гражданскую инфраструктуру, не говоря уже о военном киберпространстве. Киберкомандованию не нужно координировать свои действия с частным сектором для выполнения своей миссии, потому что его миссия состоит только в защите военных систем от киберугроз (Александр 2011). У других ветвей власти есть большая хартия, чтобы помочь с кибербезопасностью . Многие компетентные операционные центры киберзащиты

		принадлежат и управляются частным сектором. Если военные с ними не будут координировать свои действия, они проиграют Активная защита вызывает серьезную озабоченность у общественности и групп защиты конфиденциальности, в частности. Если делать неправильно и аккуратно, временной пользы не будет Некоторая государственная инфраструктура может иметь двойное назначение, поддерживая гражданских и военных пользователей. Их военная деятельность может рассматриваться целью или мировым руководством как непропорциональная. Кроме того, если имеется каскад целей, действия могут быть

		фактически непропорциональными и/или незаконными. В любом случае это может привести к дальнейшей эскалации конфликта.
Военные должны реалистично практиковать свои планы киберзащиты, в том числе планы государственного сектора и других стран.	Настольные — это упражнения, которые позволяют участникам пройти через простые сценарии, которые позволяют участникам практиковаться в принятии решений, проверять их на соответствие заданному стандарту реагирования или знакомить участников с планами реагирования. Столешница также используется для изучения новых концепций, чтобы определить, какими могут быть ответы.	Упражнения хорошо может потребовать тщательного планирования заранее. В целом, качество обучения и уроков требует большего планирования и ресурсов. Таким образом, рентабельность учений может не перевешивать альтернативу, а именно изучение текущего состояния кибершпионажа. Результаты этих учений необходимы для обратной связи с национальной стратегией, показателями, планами реагирования на инциденты и военной доктриной. Эти учения должны

		включать в себя как небольшие настольные игры для изучения специфики планов реагирования, так и масштабные национальные военные игры. Учения позволяют участникам практиковать реагирование, принятие решений и координацию в мирное время, давая им возможность совершать ошибки, изучать свои роли и развивать «мышечную память», когда последствия менее важны. Эти уроки можно усвоить относительно недорого. Настольные учения рекламируются как идеальные средства обучения, но ни одному командиру, который понимает свою работу, не нужно собирать множество ценных человеческих ресурсов, чтобы

		играть в игры, чтобы понять, что нужно для защиты киберпространства. Кроме того, наиболее важные лица, принимающие решения, обычно не участвуют в учениях и сводятся к методам генерации данных.
Военным необходимо повысить квалификацию своих кибер-сотрудников, чтобы они включали в себя не только традиционных кибер-специалистов по информационным технологиям, но и персонал, необходимый для миссий в «оспариваемой области». киберпространство.	Часто «киберперсонал» отождествляют с «ИТ-персоналом». Военным требуются кибер-навыки, не связанные с поддержкой обычных информационных технологий, такие как операторы, защитники, военные планировщики, судебные адвокаты и разведывательная поддержка в операциях миссии.	Не должно быть разделения между военной поддержкой информационных технологий и персоналом, необходимым для выполнения задач в киберпространстве. Развертывание военных технологий следует рассматривать как миссию наравне с другими оборонными миссиями. Любой другой подход оставляет ИТ-персонал позади Для управления технологической инфраструктурой требуется другой набор навыков, чем для выполнения военных задач в

		киберпространстве. Эта политика дает военным всестороннее понимание глубины и широты рабочей силы и, соответственно, Сосредоточение внимания на кибер-задачах, порученных персоналу, не связанному с ИТ, может преувеличить важность злоумышленников, которые обычно составляют небольшой процент от общей рабочей силы в киберпространстве. Это может создать ложное впечатление, что их услуги важнее задач киберзащиты.
Военные должны обеспечить дополнительную боевую подготовку рабочей силы, «наиболее подверженной влиянию противника».	Любой, кто играет ключевую роль в атаке или защите от противника, должен иметь такое же боевое мышление, как и его кинетические сверстники.	Поскольку инсайдерские кибератаки являются обычным явлением, невозможно определить, какая часть военного персонала кибербезопасности сталкивается с наибольшим количеством

		противников. Весь киберперсонал должен быть в равной степени способен распознавать враждебные киберугрозы и противостоять им. Потому что для его обеспечения всегда требуется больше обучения, чем ресурсов. обучение следует проводить там, где оно может принести непосредственную пользу.
Военное руководство должно рассматривать киберпространство как новую область, в которой можно вести войну, точно так же, как воздух, землю, космос и традиционные области.	Как и другие области, это место со своей собственной географией, с международными, личными и коммерческими интересами. В отличие от космоса и воздуха, в него очень мало входных барьеров.	Отношение к киберпространству как к домену не только помогает повысить его важность. киберпространстве, но делает его более понятным для неспециалистов. Непреднамеренным последствием классификации киберпространства как военной области является то, что военные операции могут рассматривать его как антивоенную

		область, но забывать об этом. Киберпространство — это домен не больше, чем артиллерия. Это инструмент, используемый для завоевания воздуха, моря и земли.
Военное руководство должно отдавать предпочтение киберзащите, а не наступлению.	Киберзащита — это способность не дать противникам эффективно использовать возможности кибератак. Кибер право (использование некинетических кибервозможностей для атаки противников в киберпространстве) также является важным военным потенциалом.	Без активного киберпространства государства могут быть не в состоянии управлять своей экономикой, принимать политические решения во время конфликта или производить военную мощь. Если они не считаются оборонительными, любой или все из них могут быть сломаны противником. Эта политика имеет смысл только для стран, которые управляют критической инфраструктурой, используя киберпространство. Некоторые союзные нации в мире настолько зависят от

		киберпространства, что их маргинальные доллары в контексте их сообществ верность лучше всего потратить на нападение. Средства защиты могут быть сложными и дорогостоящими, а правонарушения могут быть сдерживающими факторами и, таким образом, способствовать защите. Теоретически некоторых врагов можно остановить
Кибернаступление следует рассматривать как реальный, иногда даже предпочтительный, военный потенциал.	Эта политика отдает приоритет кибератакам по сравнению с традиционными физическими атаками для всех военных операций.	Киберправо эквивалентно ядерному оружию, потому что его применение может несоразмерно повлиять на гражданское население. Критические кибератаки в крупном масштабе инфраструктура, безусловно, может иметь несоразмерное влияние. Хотя кибератаки

		могут иметь непреднамеренные последствия, кибератаки можно использовать больше как некинетические атаки, которые не убивают и не убивают. Вместо объекта, на который нацелена кинетическая железная бомба, кибератака, выводящая из строя сайт противовоздушной обороны, может спасти жизнь операторам сайта. Точно так же кибератака на систему электроснабжения может быть предназначена для причинения более временного и обратимого ущерба, чем аналогичный эффект, вызванный кинетической атакой. Где командиры имеют доступ некинетические и несмертельные способности, эти

		атаки больше подходят для человека.
Военное руководство должно со временем интегрировать свои возможности и средства ведения кибервойны в доктрины и структуры обычных вооружений.	Исторически военные кибервозможности ассоциировались с разведкой, специальными атаками или программами совершенствования информационных технологий. Это ставит кибербезопасность за рамки обычного понимания миссий, выполняемых военными организациями. Эта политика определяет цель реинтеграции.	Сочетание наступательных и оборонительных (и разведывательных) операций дает интегрированный эффект на поле боя, и операции в киберпространстве не должны быть исключением. Специализированные киберорганизации служат важным целям, но их возможности должны быть интегрированы в официальную систему руководства и управления. Наличие различных операций кибербезопасности может быть затруднено Там, где военная организация относительно незрела в интеграции кибервозможностей, интеграция небольших подразделений кибервойны

		нарушает первоначально разработанные миссии и программы защиты, оставляя эти программы с критическим отсутствием поддержки кибербезопасности.
Военное руководство должно уделить первоочередное внимание разработке правил ведения боевых действий для киберпространства, которые отражают другие области, но применимы к реалиям киберпространства.	Правила применения силы определяют, когда и как дружественные силы могут применять силу против других. В кинетической войне они могут быть относительно простыми или (например, во время хаотической войны) очень сложными. В киберконфликтах они технически сложны не только потому, что это новое поле боевых действий. Природа киберпространства.	Это может означать, что правила политического участия изначально слишком ограничительны, какими они должны быть до тех пор, пока политические лидеры, командиры, оперативники и сторонники не станут более знакомыми и осведомленными со временем. В отсутствие правил ведения боевых действий военные могут проводить враждебные и злонамеренные операции в киберпространстве без надзора или знания. Правила ведения боевых действий —

		это то, что удерживает военных на стороне международного права.
Военное руководство должно с осторожностью относиться к конкретным целям и возможностям: упреждающая оборона, экологическая кибер-оперативная подготовка и иностранное нацеливание.	Активная защита обычно относится к способности «возвращать» системы, участвующие в атаках. Киберэлементы проникают в чужие системы перед агрессивной атакой. Иностранные инфраструктуры зависят от иностранных вооруженных сил, и они обычно являются законными целями.	В каждой из этих областей, как правило, совершенно законно заниматься военными. цели и возможности; однако делать это следует очень осторожно. Элементы кибероперативного планирования являются важными навыками для подготовки к наступательным операциям, но они могут усугубляться тем, что противники могут видеть кибернетические средства.
Кибератаки считаются «угрозами или применением силы» или «вооруженным нападением» (согласно Уставу ООН) в зависимости от масштаба, продолжительност	Эти пороговые значения являются ключевыми для определения того, поднимаются ли международные действия до уровня силы, конфликта или войны, и какие действия может предпринять в ответ государство-мишень	Эта политика гарантирует, что только те атаки будут в равной степени затронутыкинетическое оружие считается вооруженным нападением в верхней части военного применения силы, в

и и интенсивности атаки.	или международное сообщество.	то время как угроза силой или ее применение находится в нижней части. Если кибератаки направлены на причинение значительного ущерба, но не достигают своих целей, такие атаки следует рассматривать как военные действия. Их игнорирование дает противнику беспрепятственную возможность улучшить свое положение.
Государства несут ответственность за элементы киберпространства, расположенные в пределах их границ.	Хотя киберпространство обычно считается безграничным, оно укоренено в физическом мире и функционирует в рамках физических инфраструктур и организаций, расположенных за суверенными границами государств.	Соответственно, государства должны взять на себя ответственность за кибератаки, осуществляемые с территории их границ, и, если они могут, остановить атаку. Эта ответственность должна варьироваться в зависимости от масштаба, продолжительности и интенсивности

		нападения. Если государства не выполняют это обязательство, государства-мишени имеют право принять контрмеры (согласно Уставу ООН и законам о вооруженных конфликтах). Если частные группы осуществляют атаки от имени государства, они могут быть привлечены к ответственности, если государство сохраняет полный контроль над группой. (например, предоставление указаний по источникам или целям и оружию) Привлечение государств к ответственности может дополнительно защитить репрессивные страны, ограничивая неприкосновенность частной жизни и свободу выражения

		мнений. Кроме того, в Соединенных Штатах так много интернет-инфраструктуры (и так много незащищенных компьютеров), что требуется много усилий, чтобы остановить множество атак (часто
«Кибертерроризмом» следует считать террористические атаки, осуществляемые через киберпространство.	Такие виды деятельности, как вербовка или распределениепропаганда не является террористической атакой и не должна считаться «кибертерроризмом» только потому, что она происходит в киберпространстве. Кибертерроризмом следует считать только кибератаки, которые выводят из строя, уничтожают или повреждают киберсистемы или данные и направлены на терроризм.	Такое отношение к кибертерроризму значительно упрощает концепцию, исключая многие атаки, которые не имеют ничего общего с терроризмом, но происходят часто. Некоторые организации смогли получить прибыль, назвав этот ярлык «терроризм».

Проблемы с киберинфраструктурой.В этом разделе приведены наглядные примеры проблем киберинфраструктуры, с которыми сталкиваются сети частного сектора. Национальный план защиты инфраструктуры (NIPP) Министерства внутренней безопасности США признает 18 примеров управляемой частным сектором критической инфраструктуры и ключевых национальных ресурсов (CIKR) (DHS 2009). Хотя некоторые из них более активны, чем другие, каждый из этих секторов требует участия в усилиях государственно-частного партнерства для обеспечения национальной инфраструктуры, как и планировалось. В список отраслей входят продовольственные и водные системы, сельское хозяйство, системы здравоохранения, аварийно-спасательные службы, информационные технологии, связь, банковское дело и финансы, энергетика (электричество, ядерная энергия, газ и нефть, плотины), транспорт (воздух, автомагистрали,

В разделе представлены обсуждения и примеры политик обеспечения информации в иллюстративных областях финансовых услуг, здравоохранения и промышленных систем управления. Обратите внимание, что промышленные системы управления не являются отраслью промышленности как таковой, а являются общим термином для типа автоматизированного оборудования, используемого в различных отраслях промышленности.

Таблица 2.6.

Вопросы политики кибербезопасности, связанные с исследованиями и разработками

Заявление о политике	Объяснение	Причины конфликта
Исполнительная власть страны созывает комитет экспертов по кибербезопасности из различных областей для консультирования по вопросам политики кибербезопасности и оценки программ кибербезопасности.	Это требование для исполнительной власти страны (например, президента Соединенных Штатов) выйти за пределы своего узкого круга советников и обратиться за	Масштаб и глубина проблем кибербезопасности выходят за пределы компетенции любого человека. Национальные лидеры должны иметь самые просвещенные взгляды.

	помощью по вопросам стратегии кибербезопасности.	Нет необходимости устанавливать политику на таком высоком уровне. Уже существует несколько способов и процессов, позволяющих национальным лидерам искать и получать советы по важным вопросам. Это включает вопросы кибербезопасности
Национальное правительство поможет финансировать фундаментальные и прикладные исследования рисков, систем и программного обеспечения в области кибербезопасности в соответствии с приоритетами, изложенными в национальной стратегии. Насколько это возможно, такие исследования должны быть совместными, мультидисциплинарными и несекретными.	Эта политика обеспечивает финансирование исследований в области кибербезопасности в области программного обеспечения, тестирования, компьютеров и сетей. Он также должен включать междисциплинарные исследования (с отделами исследований в области безопасности, права и международных отношений), которые имеют	Финансирование исследований и разработок не только создает новые технологии безопасности, которые можно применять к современным угрозам, но и побуждает аспирантов изучать вопросы кибербезопасности и тем самым устраняет будущие угрозы кибербезопасности. Государственное финансирование исследований и разработок иногда может решить

	значение для национальной безопасности.	проблемы, которые считаются более насущными для частного сектора. Кроме того, если исследователи не знают о других исследованиях (например, если они проводились в рамках секретного проекта), финансирование может быть продублировано и потрачено впустую.
Правительство ежегодно пересматривает все инвестиции в исследования и разработки, связанные с кибербезопасностью.	Эта политика требует подготовки годового отчета с описанием того, как расходуются национальные средства на исследования и разработки, выделенные на кибербезопасность.	Без четкой программы исследований в области кибербезопасности такая оценка будет субъективным упражнением, а не информативным отчетом. В лучшем случае это будет простой список информации, которую легко найти в другом месте. Другие области исследований, имеющие стратегическое значение для национального

		правительства, поддерживаются исследовательским и программами, связанными с университетами.
Налоговые льготы предоставляются компаниям частного сектора для проведения исследований в области кибербезопасности.	Компании частного сектора обычно придерживаются стандартов безопасности и используют существующие продукты вместо того, чтобы разрабатывать собственные инновационные решения. Эта политика направлена на поощрение инноваций.	Эта политика увеличивает общий объем исследований в области кибербезопасности за счет привлечения участников на рынок. увеличивается В настоящее время компании, не занимающиеся кибербезопасность ю, могут не привлекаться налоговыми льготами, но такие налоговые льготы могут привести к тому, что компании переклассифициру ют существующие исследования в смежных областях, таких как отслеживание клиентов, в механизмы идентификации кибербезопасности. Этот

		что приводит к общему сокращению налоговых поступлений без льгот по обеспечению безопасности. Эта политика может побудить частные компании инвестировать в исследования в области кибербезопасности, но нет никакой гарантии, что нация получит такую же выгоду, как и они.
Акционерам акционерных обществ предоставляются налоговые льготы за проведение исследований в области кибербезопасности.	Эта политика направлена на повышение приемлемости акций компаний, преследующих цели безопасности.	Инвестиции в исследования в области кибербезопасности следует оценивать на основе рыночных результатов, а не расходов, которые могут не принести реальных преимуществ в плане безопасности. Эта политика побуждает частный сектор финансировать исследования в

		области кибербезопасности. Это может увеличить и повысить их рыночную стоимость.
Национальные конкурсы организуются для награждения талантов и инноваций студентов в области кибербезопасности. Другие конкурсы также могут присуждать известные университеты и исследовательские институты.	Призовые конкурсы направлены на привлечение талантливых студентов к изучению кибербезопасности.	Реализация этой политики должна создать студенческое сообщество Эта программа может вознаграждать студентов за то, что они больше узнают о методах злонамеренного взлома, чем о защитных.
Государствам следует поощрять осведомленность, образование и обучение в области киберзащиты, начиная с начальной или средней школы, и продолжать специальную техническую подготовку для киберзащитников.	Кибербезопасность, кибербезопасность и киберэтика в настоящее время являются предметами пилотных программ в начальных и средних школах, и эта политика переместит их в основную учебную программу.	Эта политика помогает формировать критическое мышление о кибербезопасности в раннем возрасте, тем самым оказывая влияние на будущих лиц, принимающих решения, чтобы они включали этические принципы в будущие системы.

		Эта политика повысит кибербезопасность по всей стране. Широкая общественность лучше понимает, как защитить себя в киберпространстве, чем специалисты по информационной безопасности. ведет к более интуитивному пониманию того, как защитить свои системы и программное обеспечение. Образование — это широкомасштабное мероприятие, потому что многие люди вовлечены в киберпространство и нуждаются в разных уровнях понимания. Это означает потенциально дорогостоящие и долгосрочные усилия. Кроме того, если существуют специальные программы по повышению осведомленности

		об этой технологии («отправляйте факсы, безопасные для детей!»), они будут быстро расти.
Национальные правительства должны предлагать университетские стипендии студентам, которые хотят изучать кибербезопасность, в обмен на государственную службу.	Эта политика предназначена для поощрения студентов к изучению кибербезопасности на уровне колледжа. Учебные программы бакалавриата обычно не включают специальность в области кибербезопасности.	В стране не хватает знающих специалистов по кибербезопасности, чтобы выполнять работу, необходимую для защиты национальных интересов. Национальная стипендиальная программа предоставляет квалифицированных специалистов. Выпускники программ бакалавриата не будут иметь большого опыта в области кибербезопасности. Специальность по кибербезопасности обычно начинается на уровне выпускника, потому что объем базовых знаний, необходимых для применения кибербезопасности

		в любой области, требует концентрации на уровне бакалавриата. Эта политика поощряет создание учебной программы по кибербезопасности и побуждает студентов делать карьеру в области кибербезопасности в правительстве. Это также может стимулировать университеты к разработке программ
Академические сообщества должны возглавлять студенческие отделения ассоциаций кибербезопасности.	Многие отраслевые ассоциации создают студенческие отделения, но профессиональные ассоциации кибербезопасности в настоящее время не добились больших успехов в этом направлении.	Сегодня студенты участвуют в общественных организациях. Важность кибербезопасности — причина отказаться от социальных сетей. Профессиональные организации по кибербезопасности обладают опытом, который студенты должны получить, и они находятся в свободном доступе в Интернете.

Исследования и разработки систем, технологий и операций кибербезопасности должны проводиться в той мере, в какой это необходимо для преодоления разрыва между киберпространством и текущими целями управления безопасностью.	Часто руководство хочет контролировать киберсреду, но не имеет для этого методов, инструментов и процедур. Эта ситуация делает их такими ответственность без полномочий	Эта политика дает менеджерам, ответственным за управление активами, инструменты для осуществления этого в долгосрочной перспективе, даже если только сейчас. Подобные политики можно рассматривать как открытую чековую книжку для всех видов исследований в области кибербезопасности без какой-либо предсказуемой выгоды для организации.
Все разработки программного обеспечения должны использовать лучшие практики для обеспечения жизненного цикла разработки программного обеспечения.	Эта политика требует соблюдения методов безопасного кодирования программного обеспечения, а также тестирования безопасности.	Известно, что методы безопасного кодирования уменьшают уязвимости при внедрении. Инновации требуют постоянных изменений в организационной стратегии и процессах. Методы

		безопасного кодирования слишком статичны, чтобы идти в ногу с темпами развития технологий.
При разработке всех систем следует использовать лучшие практики для обеспечения жизненного цикла разработки системы.	Эта политика аналогична приведенной выше, но использует подход ко всей системе, а не к безопасности отдельного программного компонента.	Требования передовой практики безопасности, которые являются требованиями безопасности системы учитываться на ранних этапах процесса разработки и интегрироваться в функции продукта. Требования безопасности не должны иметь приоритет над другими

Контрольные вопросы.

1. Что такое анализ дисконтированных денежных потоков (DCF) и каковы его ограничения?
2. Что такое гибкость применительно к проектированию инженерных систем?
3. Каковы преимущества использования метода ROA при оценке проектов по сравнению с традиционными показателями?
4. Какие ключевые элементы должен включать структурированный процесс проектирования гибкой системы?
5. Как называется минимальный стандарт кибербезопасности, требуемый государственными органами Великобритании?
6. Что такое CTI и какова его цель?

7. Каковы ключевые факторы, определяющие профиль угроз противника в киберпространстве?

8. Какие области составляют жизненный цикл анализа угроз?

9. Какие дополнительные направления необходимы для постоянного совершенствования и организации КТИ?

10. Что такое знак доверия и какое значение он может иметь при оценке надежности источника CTI?

11. Какие критерии используются для определения достоверности информации, подтвержденной другими источниками?

12. Что означает совместимость информации с функцией CTI и ее требованиями?

13. Почему не вся информация в каналах угроз NCSC полезна для аналитиков CTI?

14. На какие основные области следует обратить внимание при оценке качества собранных данных?

15. Почему важно обеспечить правильный формат данных при сборе CTI?

Глава III. Политика кибербезопасности: подход США

3.1-§. Федеральная стратегия кибербезопасности США

В этой главе рассматривается политика кибербезопасности, принятая федеральным правительством США, со стратегической точки зрения. До начала 1990-х годов политика кибербезопасности США была прямым ответом на распространение электронных записей, как описано в главе 2. Здесь мы представляем недавнюю историю проблем кибербезопасности на федеральном уровне, которые повлияли на стратегию и соответствующую политику. В этой главе объясняются действия правительства в ответ на исторические события и предлагаются области, в которых правительство могло бы рассмотреть будущие действия. Он начинается с краткого исторического обзора наиболее важных событий последних двух десятилетий, которые сформировали сегодняшние политические дебаты в Вашингтоне. Хотя большинство видов деятельности явно ориентированы на кибербезопасность, некоторые из них не сразу заметны с точки зрения их вклада в политику кибербезопасности. Мы начнем этот исторический обзор с террористических атак на Соединенные Штаты в начале 1990-х годов и перейдем к действиям, предпринятым последующими администрациями. Глава завершается общими мыслями о стратегии и политике на примере истории.

Политическая реакция федерального правительства США на кибербезопасность варьировалась от приверженности строгим стандартам, разработанным Национальным институтом стандартов и технологий (MSTI) и Агентством национальной безопасности (АНБ), до полного игнорирования серьезности ситуации. В настоящее время в Сенате и Палате представителей США несколько десятков законопроектов, связанных с кибербезопасностью, находятся на разных стадиях разработки. Многие из этих законопроектов представляют собой переписанные версии инициатив, инициированных предыдущими Конгрессами, а некоторые представляют собой совершенно новые инициативы. Ни один из разрабатываемых законодательных актов сам по себе не «решит» проблемы кибербезопасности, с которыми сталкивается наша страна. Действительно,

Конечно, было много попыток сформировать политику

кибербезопасности с помощью действий Конгресса или прямых государственных органов. Существует также много предположений и неверных представлений о пересечении политики и стратегии. Чистая стратегия — это схема того, как лицо, принимающее решения, хочет, чтобы все работало. Для реализации стратегии политика сочетается с процессом, процедурным отношением, стандартами и исполнением. В зависимости от стратегии список вещей, необходимых для ее создания, может быть неполным. Более того, даже хорошо спланированные и осуществленные усилия по реализации стратегии иногда могут не привести к достижению стратегических целей. Это особенно верно в среде, которая развивается по мере реализации стратегии.

Например, в 2006 году стало ясно, что проблема кражи персональных данных станет темой государственной политики. В то время крупнейшие компании, выпускающие кредитные карты, которые могли стать мишенью любого потенциального законодательства, сформировали Совет по стандартам безопасности индустрии платежных карт, который, в свою очередь, разработал Стандарт безопасности данных индустрии платежных карт. Стандарты были приняты, чтобы продемонстрировать соблюдение существующих политик защиты финансовой конфиденциальности и опровергнуть представление о необходимости принятия каких-либо дополнительных законов, как могли бы предположить недобросовестные из нас. Однако даже после принятия стандартов все еще существуют большие группы, соответствующие стандартам, созданным отраслью. lov были источником массовых утечек данных, ведущих к краже личных данных. Аналогичная попытка саморегулирования предпринимается в индустрии онлайн-рекламы путем добровольного принятия стандартов конфиденциальности, запрещающих отслеживание действий потребителей (Wyatt, 2012). Эти примеры показывают, что стандарты и политики — это очень разные вещи, и что стандарты, разработанные для обеспечения соответствия политикам, не обязательно таковы. Аналогичная попытка саморегулирования предпринимается в индустрии онлайн-рекламы (Wyatt, 2012). Эти примеры показывают, что стандарты и политики — это очень разные вещи, и что стандарты, разработанные для обеспечения соответствия политикам, не обязательно таковы. Аналогичная попытка саморегулирования предпринимается в

индустрии онлайн-рекламы (Wyatt, 2012). Эти примеры показывают, что стандарты и политики — это очень разные вещи, и что стандарты, разработанные для обеспечения соответствия политикам, не обязательно таковы.

Рост киберпреступности.В любой культуре есть преступники, которые используют в своих интересах менее удачливых, доверчивых и тех, кто не заботится о своей личной безопасности. Интернет-культура ничем не отличается, за исключением того, что многие преступники могут заниматься своим ремеслом практически неизвестно и вне досягаемости большинства правоохранительных органов. В целом интернет-преступления сосредоточены на краже кредитных карт, мошенничестве, онлайн-азартных играх и порнографии, а также на обмане пользователей с помощью поддельных электронных писем и поддельных веб-сайтов. Другие преступления включают кражу интеллектуальной собственности, в том числе одноранговый обмен файлами и продажу или распространение пиратского или пиратского программного обеспечения.

В 1990-х годах многие эксперты по безопасности считали, что мы находимся на пороге серьезных потрясений в Интернете — «кибер-Перл-Харбора». Однако в конце 2003 г. и начале 2004 г. возникла еще одна угроза, которая с тех пор доминирует на сцене. Организованная преступность осознала большую ценность Интернета и не может его игнорировать. Это делает всех онлайн-пользователей жертвой нового преступления, и большую часть времени они даже не знают, были ли они ограблены или обмануты.

Хуже того, быстрое развитие технологии «веб 2.0» (вики, одноранговые сети, социальные сети и другие формы самовыражения) еще больше упростило преступникам возможность воспользоваться ничего не подозревающими жертвами. Ситуация еще хуже на промышленных предприятиях — многие из этих новых технологий заменяют старые системы по мере их модернизации. Внедряя технологии Web 2.0 для мониторинга и эксплуатации систем ICS/SCADA, мы можем открыть наши внутренние сети контроля для внешнего преступного сообщества. Система управления критической инфраструктурой чрезвычайно важна, и преступные группировки по всему миру могут воспользоваться любой маленькой ошибкой, которую вы сделаете, всего за

миллисекунду.

Каждый год, начиная с 2008 года, Verizon публикует отчет о расследовании утечек данных (DBIR), который включает в себя исследовательский анализ последовательности событий, которые приводят к крупным утечкам данных. Год за годом команда Verizon заявляла, что большинство всех крупных утечек данных были вызваны преступными намерениями. Последние статистические данные, основанные на почти 800 нарушениях, расследованных в 2010 г. (в скобках указано процентное изменение по сравнению с 2009 г.) и опубликованных в 2011 г. (Бейкер, Хаттон и др., 2011 г.):

- 92% зависят от внешних факторов (+22%);
- 17% вовлеченных инсайдеров (-31%);
- 9% участвовали несколько сторон (-18%);
- 50% использовали какой-либо вид взлома (+10%);
- 49% установленных вредоносных программ (+11%);
- 29% связаны с физическими атаками (+14%);
- 17% - результат нецелевого использования привилегий (-31%);
- 11% использовали социальные тактики (-17%);
- 83% жертв были жертвами возможности;
- * 92% атак были не очень изощренными (+7%);
- 76% всех данных было взломано с серверов (-22%);
- 86% идентифицированы третьей стороной (+25%);
- 96% нарушений удалось предотвратить с помощью простых или промежуточных контролей;
- 89% жертв PCI-DSS не соблюдали требования (+10%).

Борцы с преступностью быстро учатся выявлять и преследовать преступников в результате кибератаки, но победить в этой битве непросто. Сегодня явное преимущество на стороне преступников. Будем надеяться, что через несколько лет преимущество окажется в надежных руках, а пока Интернет такой же, как Дикий Запад 150 лет назад.

В последние несколько лет появился еще более зловещий преступный метод: контрафактное компьютерное и сетевое оборудование, произведенное в Юго-Восточной Азии и предназначенное для американского рынка. Расследования, проведенные Федеральным бюро расследований и другими правоохранительными органами, показали, что примерно 10% всей

электроники, поступающей в США, содержат контрафактные или значительные количества контрафактных деталей. Хуже того, появляется все больше свидетельств в поддержку теории о том, что иностранные правительства преднамеренно устанавливают черный ход и другой скрытый доступ к продуктам, производимым в их собственных странах и продаваемым на открытом мировом рынке. Министерство обороны,

Шпионаж и действия национальных государств.Во время холодной войны и столетия назад страны подвергались большому риску, вербовав и обучая шпионов для работы за границей. Сегодня Интернет сделал шпионаж таким же простым, как открытие веб-браузера, а затем вход в поисковую систему, что сводит риск смерти почти к нулю. Конечно, эта теория хороша только для отслеживания стран с хорошими связями.

Помимо правительств, многие компании занимаются так называемой «конкурентной разведкой» — эвфемизмом для корпоративного шпионажа. Он стал настолько популярен, что даже All Corporate Strategic and Competitive Intelligence Spies, или SCIP (официально известная как Общество специалистов по конкурентной разведке), сменила название в мае 2010 года; http://www.scip.org.)

В конце 1990-х несколько государственных систем США были подвержены скрытым учетным записям и многочисленным несанкционированным действиям. По мере продолжения расследования было обнаружено, что все больше компьютеров и систем, не принадлежащих федеральному правительству, имеют несанкционированные учетные записи. Новым модным словом стала «фильтрация данных», а не «вторжение» или «вторжение». Целями были большие базы данных, содержащие атмосферные данные, батиметрические данные и другие данные, собранные за десятилетия. Происхождение атак было неясным — злоумышленники использовали сложные методы для маршрутизации атак через несколько скомпрометированных компьютеров и «сайтов восстановления» в качестве точек сбора украденных данных. позаимствованно из Ни в одном случае признаков ухудшения не наблюдалось. Все это выглядело как электронный шпионаж, классический случай кражи интеллектуальной собственности, только через Интернет, а не с

помощью микрофильма и шпионской камеры, как у Джеймса Бонда.

Во времена холодной войны шпионское сообщество явно сосредоточилось на шпионаже США против СССР. Но в последние годы внимание переключилось с постсоветских стран на Китай. В Китае культура поддерживает академические достижения. Многие студенты и преподаватели относятся к Интернету как к эксперименту и постоянно заходят в удаленные системы или находят ошибки в уязвимом программном обеспечении только в академических целях. Их выводы публикуются в научных статьях, и исследователи переходят к следующему проекту. Однако некоторые нашли в этом исследовании невероятную ценность и начали делать из него бизнес, продавая свои результаты правительствам, преступным группировкам и даже террористам.

В 2003 году было обнаружено, что серия кибератак, предположительно совершенных китайцами, была нацелена на американские компьютерные системы. Расследование нападения министерства обороны, получившее название «Титаник Дождь», оставалось засекреченным до тех пор, пока история не была опубликована в прессе. После утечки в прессу выяснилось, что злоумышленники имели доступ ко многим компьютерным сетям, включая Lockheed Martin, Sandia National Laboratories, Redstone Arsenal и NASA. Хотя названия следствия менялись с годами, слежка продолжается и по сей день.

Китайский кибершпионаж стал достоянием общественности весной 2006 года, когда системный администратор частного сектора заметил, что многие из его пользователей получают сообщения электронной почты с вложениями Microsoft Word, содержащими китайский язык. При открытии Word произошел сбой, и появилось диалоговое окно с вопросом, хочет ли пользователь поделиться данными с Microsoft. Системный администратор связался с SANS Internet Storm Center, который, в свою очередь, опубликовал журнал о проблеме. Несколько дней спустя проблема была обнаружена в уязвимости нулевого дня в Word. Злоумышленники могут использовать уязвимость в продуктах Microsoft Office для записи данных в определенную область памяти с помощью расширений Object Link Extensions (OLE) и изменения документов Word. нашел способ изменить его. Этот метод предоставил злоумышленникам возможность установить вредоносный код по своему выбору,

начиная от простых кейлоггеров и заканчивая полными пакетами руткитов, которые дают злоумышленнику полный контроль над скомпрометированным компьютером.

Но Китай — не единственный подозреваемый в продуктах информационных технологий, модифицированных для шпионажа или кибервойны. Возможно, лучшим (и самым страшным) примером этой тенденции было обнаружение червя Stuxnet в середине 2010 года. Программное обеспечение, которое, как полагают, было написано одной или несколькими западными странами, было разработано для физического повреждения частей иранских объектов по переработке ядерного топлива. Вместо того, чтобы распространяться по сети, такой как Интернет, Stuxnet был разработан для преодоления «воздушных промежутков» в сети путем заражения традиционных накопителей памяти с универсальной последовательной шиной (USB). Происхождение Stuxnet остается загадкой.

Политический ответ на растущую угрозу шпионажа: киберкомандование США.В 2009 году Киберкомандование обороны (USCYBERCOM) взяло на себя функции JTF-GNO, «временной» организации, созданной в 1998 году для борьбы с растущей угрозой иностранных кибератак. Изощренные атаки конца 2000-х заставили Белый дом переосмыслить, как реагировать на растущую угрозу, и навсегда институционализировать кибербезопасность в своих военных планах и операциях. Сегодня USCYBERCOM руководит операциями и защитой большинства подразделений Министерства обороны, а также может проводить «полные» военные операции в киберпространстве по указанию президента. Однако,

По данным Министерства обороны, USCYBERCOM объединяет все операции Министерства обороны в киберпространстве, а также планирует, координирует, интегрирует, синхронизирует и выполняет действия, которые включают: управление повседневной защитой информационных сетей Министерства обороны; координация операций Министерства обороны в поддержку военных миссий; Управление операциями и защита отдельных информационных сетей Министерства обороны и; проводить полный комплекс боевых действий в киберпространстве и по указанию руководства. Объединение

существующих ресурсов киберпространства в команду, доступную в настоящее время

USCYBERCOM централизует командование кибернаступательными операциями, укрепит потенциал кибернаступательных действий Министерства обороны, а также интегрирует и укрепит опыт Министерства обороны в области кибербезопасности. При этом USCYBERCOM повышает стабильность, надежность и возможности информационных и коммуникационных сетей Министерства обороны для противодействия угрозам кибератак и обеспечения кибервторжений. Усилия USCYBERCOM также поддерживают способность вооруженных сил надежно проводить быстрые и эффективные операции, а также защищать системы командования и управления и инфраструктуру кибератак, которые поддерживают платформы систем вооружения, от сбоев, вторжений и атак.

USCYBERCOM является подразделением Стратегического командования США (USSTRATCOM). Элементы службы включают Киберкомандование Сухопутных войск (MARFORCYBER); 24-й армейский корпус США; Киберкомандование флота (FLTCYBERCOM); и Киберкомандование корпуса морской пехоты (MARFORCYBER).

Еще неизвестно, насколько эффективно USCYBERCOM сможет улучшить безопасность наиболее уязвимых сетей страны. Одной из самых серьезных проблем будет давний «дымоходный» менталитет военных организаций — что мое, то мое, и никакая другая группа или командование не должны иметь никакой власти над тем, что у меня на тарелке. Из-за миллисекундного характера киберпространства и осознания того, что угрозы, исходящие от одной группы, могут быстро повлиять на другие группы, это отношение должно измениться, если uscybercom хочет добиться успеха.

К сожалению, организации, которые отказываются сотрудничать или объединять свои средства защиты, более уязвимы для враждебных групп, которые научились использовать слабые места за пределами этих границ.

Действия Конгресса.На момент написания этой книги в Сенате и Палате представителей США находилось несколько законопроектов на разных стадиях разработки. Многие из этих

законопроектов представляют собой переписанные версии инициатив, инициированных предыдущими Конгрессами, а некоторые представляют собой совершенно новые инициативы. Ни один из разрабатываемых законодательных актов сам по себе не «решит» проблемы кибербезопасности, с которыми сталкивается наша страна. На самом деле, любой эксперт по политике кибербезопасности, вероятно, не верит, что акт Конгресса будет иметь большое значение для обеспечения безопасности киберпространства.

111-й Конгресс (2009–2010 гг.) подготовил более 50 отдельных «киберзаконопроектов», в которых предпринимались попытки законодательно решить вопросы кибербезопасности. Два законопроекта, законопроект Либермана/Сноу (Комитет национальной безопасности) и законопроект Рокфеллера/Коллинза (Комитет по торговле), вызвали большую часть дебатов в Сенате. Предыдущий законопроект ввел понятие «резак», которое широко высмеивалось в СМИ и в Вашингтоне. В конечном итоге он был исключен из формулировки законопроекта, но эта концепция послужила напоминанием о том, как далеко Конгресс планировал зайти в своей законодательной повестке дня. Кибербезопасность перед промежуточными выборами 2010 года, чтобы продемонстрировать двухпартийную поддержку в борьбе с растущей национальной угрозой

На момент написания этой статьи 112-й Конгресс (2011–2012 гг.) внес как минимум дюжину законопроектов о кибербезопасности как в Сенат, так и в Палату представителей. Большинство из этих законопроектов являются повторениями законопроектов, внесенных на 111-м Конгрессе, но некоторые из них представляют собой новое начало. Однако, поскольку Конгресс сосредоточен на бюджете и экономических вопросах, всеобъемлющий закон о кибербезопасности вряд ли будет принят в ближайшее время. Большинство в Палате представителей может быть подходом в пользу разработки и принятия небольших законодательных актов, направленных на решение конкретных проблем.

Некоторые законопроекты, связанные с кибербезопасностью, уже отклонены. Например, Закон о прекращении пиратства в Интернете (SOPA, HR 3261) и Закон о предотвращении реальных онлайн-угроз экономическому творчеству и краже

интеллектуальной собственности (Закон о защите интеллектуальной собственности или PIPA, S. 968) были законопроектами Конгресса, направленными на расширение возможностей законодательства США. правоохранительные органы для борьбы с онлайн-продажами охраняемой интеллектуальной собственности. Авторские права. имущества и контрафактных товаров. Оба эти законопроекта подверглись широкой критике в техническом сообществе и в конечном итоге были отклонены Конгрессом после того, как влиятельные интернет-сайты, такие как Wikipedia, были закрыты на день в знак протеста.

На момент написания этой книги в Сенате и Палате представителей США находилось несколько законопроектов на разных стадиях разработки. Многие из этих законопроектов представляют собой переписанные версии инициатив, инициированных предыдущими Конгрессами, а некоторые представляют собой совершенно новые инициативы. Ни один из разрабатываемых законодательных актов сам по себе не «решит» проблемы кибербезопасности, с которыми сталкивается наша страна. На самом деле, любой эксперт по политике кибербезопасности, вероятно, не верит, что акт Конгресса будет иметь большое значение для обеспечения безопасности киберпространства.

Два законопроекта Палаты представителей, HR 3523 (представленный конгрессменом Майком Роджерсом и конгрессменом Холландом Рупперсбергером, «Закон о замене и защите от кибератак 2011 г.») и HR 3647 (представленный конгрессменом Дэниелом Лунгреном, «Содействие кибербезопасности и обмену информацией»). «Закон о создании и улучшении»). меньше аргументов. В первом законопроекте рассматриваются конкретные юридические ограничения, которые не позволяют частному сектору и правительству обмениваться критически важной и срочной информацией о кибербезопасности. Последний законопроект гораздо более всеобъемлющий, включая положения о новой организации по обмену информацией, о назначении главного сотрудника по кибербезопасности DHSDA, поощряет исследования в DHS для поиска новых решений технических проблем кибербезопасности и поручает DHS разработать национальный план реагирования на инциденты

кибербезопасности вместе с критически важными инфраструктурными активами частного сектора. владельцы.

Важным аспектом законодательства о кибербезопасности Палаты представителей и Сената является концепция «закрытой критической инфраструктуры» — или того, к каким частям частного сектора применяется законодательство. Один из законопроектов Палаты представителей определяет атаку, которая в случае взлома или уничтожения средствами киберзащиты может привести к значительным человеческим жертвам, серьезным экономическим потрясениям, массовой эвакуации крупных населенных пунктов или серьезному нарушению возможностей национальной безопасности. Несколько отраслей добиваются конкретных «исключений» из этого определения, чтобы оставаться вне какого-либо нового государственного надзора или регулирования. Их аргумент в том, что

По мнению ряда сенаторов, основным мотивом действий является опасение, что атаки на критически важную инфраструктуру США через Интернет не только возможны, но и вероятны в ближайшем будущем. Конгресс не хочет сидеть сложа руки, предпочитая показать, что он действовал до кризиса, а не быть обвиненным в игнорировании проблемы. Частный сектор, с другой стороны, предпочитает сначала навести порядок в своем доме, прежде чем правительство введет какие-либо регулирующие или карательные рамки для бизнеса. Отрасль предпочитает государственные стимулы для повышения безопасности, такие как снижение нормативного бремени, снижение налогов на бизнес и кредиты или гранты для компенсации затрат. Тем не менее, бюджет В сегодняшнем сфокусированном мире маловероятно, что Конгресс примет закон о кибербезопасности, который стоит денег налогоплательщикам. Нейтральный с точки зрения затрат стимул — это то, что необходимо определить, а затем можно найти золотую середину.

Краткое описание.Политическая реакция федерального правительства США на кибербезопасность варьировалась от приверженности строгим стандартам, разработанным NIST и АНБ, до полного игнорирования серьезности ситуации. В этой главе была предпринята попытка показать, как политика федерального правительства изменилась за последние два десятилетия в ответ на

новые угрозы и растущую зависимость от киберпространства. По мере развития Интернета и кибератак развивалась и политика правительства в области кибербезопасности за последние 20 лет. К сожалению, угрозы кибератак и уязвимости развиваются быстрее, чем государственная политика (Brenner, 2011). Максимальное количество ходов могло только замедлить атаки или ограничить количество наносимого урона.

Политика кибербезопасности не является статичной и должна быть такой же гибкой, как кибератака, для защиты и управления которой она предназначена. Правительства часто не в состоянии адаптироваться к быстрым изменениям и быстро отстают с точки зрения государственной политики, стратегий, контрмер, а также образования и осведомленности людей по мере того, как они продолжают развиваться. Возможно, собственная организация федерального правительства слишком иерархична и линейна, чтобы быть злейшим врагом самому себе, когда дело доходит до защиты компьютеров и компьютерных сетей. Напротив, можно ожидать, что противоборствующие сети будут управляться очень слабо связанным административным руководством и разнообразными операционными структурами, способными к стратегически скоординированным атакам (Robb 2007). Киберпространство сложно и взаимосвязано. у него нет единой точки власти или контроля. Для обеспечения безопасности сетей также может потребоваться децентрализованный и неиерархический подход к организационному управлению (Brafman and Beckstrom, 2006). Некоторые компании частного сектора перешли к плоской, децентрализованной организационной структуре и, таким образом, смогли противостоять внешним силам. Возможно, пришло время переосмыслить модели государственных организаций, чтобы сделать их более похожими на кибератаки. tdy и тем самым удалось противостоять внешним силам. Возможно, пришло время переосмыслить модели государственных организаций, чтобы сделать их более похожими на кибератаки. tdy и тем самым удалось противостоять внешним силам. Возможно, пришло время переосмыслить модели государственных организаций, чтобы сделать их более похожими на кибератаки.

3.2-§.Политика кибербезопасности: российский подход

Конвенция о международной информационной безопасности

В Екатеринбурге (21-22 сентября 2011 г.) в рамках второй международной встречи высоких представителей по вопросам безопасности российской стороной была представлена концепция Конвенции о международной информационной безопасности.

Предметом регулирования конвенции является деятельность государств по обеспечению международной информационной безопасности..

Целью настоящей Конвенции является противодействие использованию информационно-коммуникационных технологий в целях нарушения международного мира и безопасности, а также определение мер по обеспечению деятельности государств в информационном пространстве:

1) способствовал общему социально-экономическому развитию;

2) осуществляется в соответствии с целями поддержания международного мира и безопасности;

3) соблюдение общепризнанных принципов и норм международного права, в том числе принципов мирного урегулирования конфликтов и споров, неприменения силы, невмешательства во внутренние дела, уважения прав человека и основных свобод;

4) что каждый имеет право искать, получать и распространять информацию и идеи, изложенные в документах ООН, принимая во внимание, что такое право может быть ограничено законом в целях защиты интересов национальной и общественной безопасности каждого государства; а также предотвращение неправомерного использования информационных ресурсов и несанкционированных вмешательств;

5) свобода технологического обмена и гарантированная свобода обмена информацией при уважении суверенитета государств и их существующих политических, исторических и культурных особенностей.

В качестве основных угроз, ведущих к нарушению международного мира и безопасности в информационном пространстве, рассматриваются следующие:

1) использование информационных технологий и средств для осуществления враждебных действий и действий вторжения;

2) целенаправленное деструктивное воздействие на важные структуры другого государства в информационном пространстве;

3) неправомерное использование информационных ресурсов другого государства без согласия государства, в информационном пространстве которого эти ресурсы находятся;

4) действия в информационном пространстве, направленные на нанесение ущерба политической, экономической и социальной системам другой страны, психологическое манипулирование населением, дестабилизацию общества;

5) использование международного информационного пространства государственными и негосударственными структурами, организациями, группами и отдельными лицами в террористических, экстремистских и иных преступных целях;

6) трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальному законодательству государств;

7) размещать этническую, расовую или межрелигиозную ненависть, расистские или ксенофобные письменные материалы, изображения или любое другое изложение идей или теорий, которые разжигают, пропагандируют или разжигают ненависть с использованием информационной инфраструктуры для распространения вредоносной информации; дискриминация или насилие в отношении любого лица или группы лиц по признаку расы, цвета кожи, национального или этнического происхождения или религии;

8) манипулирование информационными потоками в информационном пространстве других стран, дезинформация и сокрытие информации в целях разрушения психологической и духовной среды общества, разрушения традиционных культурных, нравственно-этических и эстетических ценностей;

9) использование информационно-коммуникационных технологий и средств в информационном пространстве, наносящее ущерб основным правам и свободам человека;

10) бороться с использованием новейших информационных и коммуникационных технологий, создавать условия для технологической зависимости в сфере информации в ущерб другим

странам;

11) распространение информации, получение контроля над национальными информационными ресурсами другого государства.

Дополнительные факторы, повышающие риск этих угроз, включают:

1) неопределенность в определении источника враждебных действий, особенно с учетом возрастающей активности отдельных лиц, групп и организаций, в том числе преступных организаций, выполняющих посреднические функции при осуществлении деятельности в интересах других лиц;

2) потенциальный риск внедрения в информационные и коммуникационные технологии незаявленных подрывных возможностей;

3) различия в уровне информационно-коммуникационных технологий и их безопасности в разных странах («цифровой разрыв»);

4) различия в национальном законодательстве и практике формирования защищенной и быстровосстанавливаемой информационной инфраструктуры.

Основные принципы международной информационной безопасности

Информационное пространство является общим достоянием человека. Его безопасность является основой обеспечения устойчивого развития мировой цивилизации.

В целях создания и поддержания атмосферы доверия в информационном пространстве государства-участники должны придерживаться следующих принципов:

1) деятельность каждого государства-участника в информационном пространстве должна осуществляться таким образом, который способствует социально-экономическому развитию и соответствует задачам поддержания международного мира и безопасности, в соответствии с общепризнанными принципами и нормами. международное право, включая принципы мирного урегулирования конфликтов и конфликтов, неприменения силы в международных отношениях, невмешательства во внутренние дела других государств, уважения суверенитета государств, основных прав и свобод человека;

2) государства-участники придерживаются принципа

неразрывности безопасности в процессе формирования международной системы информационной безопасности, то есть безопасность каждого из них неразрывно связана с безопасностью всех других государств и мира. защищает общество в целом и не укрепляет собственную безопасность в ущерб безопасности других стран;

3) каждое государство-участник должно стремиться к устранению различий в уровне оснащения национальных информационных систем современными информационно-коммуникационными технологиями, к сокращению «цифрового разрыва» с целью снижения общего уровня угроз в информационном пространстве;

4) все государства-участники информационного пространства пользуются суверенным равноправием, имеют одинаковые права и обязанности, являются равноправными субъектами информационного пространства независимо от экономических, социальных, политических и иных различий;

5) каждое государство-участник имеет право устанавливать суверенные нормы и управлять своим информационным пространством в соответствии с национальным законодательством. Суверенитет и законы применяются к информационной инфраструктуре, расположенной на территории Государства-участника или иным образом подпадающей под его юрисдикцию. Государства-члены должны стремиться к гармонизации национального законодательства, различия в котором не должны создавать препятствий для создания надежной и безопасной информационной среды;

6) каждое государство-участник должно придерживаться принципа ответственности за свое информационное пространство, в том числе за его безопасность и содержание размещаемой в нем информации;

7) каждое государство-участник имеет право свободно развивать свое информационное пространство без вмешательства извне, и каждое другое государство должно уважать это право в соответствии с принципом равноправия народов и самоопределения, закрепленным в Уставе Организации Объединенных Наций;

8) каждое государство-участник может свободно и самостоятельно определять свои интересы в обеспечении

информационной безопасности на основе суверенного равенства с учетом законных интересов безопасности других государств, а также свободно выбирать способы обеспечения собственной информационной безопасности;

9) государства-участники признают агрессивную «информационную войну» преступлением против международного мира и безопасности;

10) информационное пространство государства-участника не должно быть объектом оккупации другим государством в результате угроз или применения силы;

11) каждое государство-участник имеет неотъемлемое право на самооборону в случае агрессивных действий против него в информационном пространстве, если достоверно установлен источник агрессии и адекватны меры реагирования;

12) каждое государство-участник определяет свой военный потенциал в информационном пространстве на основе национальных процедур с учетом законных интересов безопасности других государств, а также необходимости содействия международному миру и безопасности. Ни одна из стран-участниц не будет пытаться получить превосходство над другими странами в информационном пространстве;

13) государство-участник может разместить свои силы и средства для обеспечения информационной безопасности на территории другого государства на добровольной основе в ходе переговоров, а также в соответствии с соглашением, разработанным в соответствии с нормами международного права;

14) каждое государство-участник принимает необходимые меры для обеспечения невмешательства в деятельность международных информационных систем управления транспортом, финансовыми потоками, средствами связи, международными СМИ, включая научный и образовательный обмен. может оказать негативное влияние на информационное пространство в целом;

15) государствам-участникам поддерживать и поощрять научно-технические разработки в области развития информационного пространства, а также образовательную и обучающую деятельность, направленную на формирование глобальной культуры кибербезопасности;

16) в рамках имеющихся средств каждое государство-участник

обеспечивает соблюдение основных прав и свобод человека и гражданина в своем информационном пространстве, прав на интеллектуальную собственность, включая патенты, технологии, коммерческую тайну, товарные знаки и авторские права;

17) каждое государство-участник гарантирует свободу слова, выражения мнения в информационном пространстве, защиту от незаконного вмешательства в частную жизнь граждан;

18) каждое государство-участник стремится поддерживать баланс между основными свободами и эффективной борьбой с использованием информационного пространства террористами;

19) государства-члены не вправе ограничивать или нарушать доступ граждан к информационному пространству, кроме как в целях защиты национальной и общественной безопасности, а также предотвращения неправомерного использования и несанкционированного вмешательства в национальную информационную инфраструктуру;

20) страны-участницы поощряют партнерство бизнеса и гражданского общества в информационном пространстве;

21) страны-участницы признают свои обязательства по обеспечению осведомленности своих граждан, общественных и государственных органов, других стран и мирового сообщества о новых угрозах в информационном пространстве и определенных способах повышения их безопасности.

Основные меры по предотвращению военных конфликтов в информационном пространстве. Государства-участники обязаны активно выявлять возможные конфликты в информационном пространстве, а также принимать меры по их предотвращению, осуществлять совместные усилия по разрешению кризисов и конфликтов мирным путем.

С этой целью страны-участницы:

1) обязуются сотрудничать друг с другом в области международной информационной безопасности в целях поддержания международного мира и безопасности, содействия международной экономической стабильности и развитию, общего благосостояния народов и международного сотрудничества, свободного от дискриминации;

2) принимает все необходимые меры для предотвращения деструктивного воздействия информации с использованием его

территории или информационной инфраструктуры, находящейся под его юрисдикцией, а также для выявления источника компьютерных атак, осуществляемых с использованием его территории, против этих атак обязуется сотрудничать в предотвращении и устранение последствий;

3) воздерживается от разработки и принятия планов и доктрин, которые могут привести к нарастанию угроз в информационном пространстве, а также к напряженности отношений между государствами и возникновению «информационных войн»;

4) воздерживается от любых действий, направленных на полное или частичное нарушение целостности информационного пространства другой страны;

5) обязуется не использовать информационно-коммуникационные технологии для вмешательства в дела, входящие во внутреннюю компетенцию другого государства;

6) воздерживается от угрозы или применения силы в отношении любой другой страны с целью нарушения ее информационного пространства или в качестве средства разрешения споров в международных отношениях;

7) обязуется воздерживаться от организации каких-либо иррегулярных формирований или поощрения их к организации противоправной деятельности в информационном пространстве другого государства;

8) обязуется воздерживаться от клеветнических высказываний, а также оскорбительной или враждебной пропаганды в целях вмешательства или вмешательства во внутренние дела других государств;

9) имеет право и обязуется бороться с распространением ложных или искаженных сообщений, которые могут рассматриваться как вмешательство во внутренние дела других стран или нанесение ущерба международному миру и безопасности;

10) принимает меры по ограничению распространения «информационного оружия» и технологий его создания.

Меры, направленные на разрешение военных конфликтов в информационном пространстве:

1) Государства-участники разрешают споры в информационном пространстве преимущественно путем переговоров, запросов, посредничества, примирения, арбитража,

судебного разбирательства, обращения в региональные органы или соглашения либо иными мирными средствами, не создающими угрозы международному миру и безопасности.

2) В случае любого международного конфликта право государств-участников конфликта на выбор методов или средств ведения «информационной войны» ограничено действующими нормами международного гуманитарного права.

В целях противодействия использованию информационного пространства в террористических целях страны-участницы:

1) принять меры против использования информационного пространства в террористических целях и признать необходимость совместных решительных действий;

2) стремится выработать единые подходы к пресечению деятельности террористических интернет-ресурсов;

3) понимает необходимость налаживания и расширения обмена информацией об угрозах компьютерных атак, признаках, фактах, способах и средствах использования сети Интернет в террористических целях, стремлениях и деятельности террористических организаций в информационном пространстве. , а также обмен опытом и передовым опытом в области мониторинга информационных ресурсов в сети Интернет, поиска и мониторинга содержания террористических сайтов, проведения криминалистических компьютерных экспертиз в данной сфере, правового регулирования и организации деятельности по борьбе с использованием информационного пространства. террористические цели;

4) принимает правовые документы и иные меры, необходимые компетентным органам для проведения следственных, обыскных и иных процессуальных мероприятий, направленных на предупреждение, пресечение и ликвидацию последствий террористических актов в информационном пространстве, а также наказание виновных. лица и организации для них;

5) принимает необходимые законодательные и иные меры, гарантирующие законный доступ к некоторым частям информационно-коммуникационной инфраструктуры на территории государства-участника, в отношении которых имеются законные основания полагать, что они используются для осуществления террористической деятельности или для их

реализации. деятельность, способствующая осуществлению террористических актов или деятельности террористических организаций, групп или отдельных террористов в информационном пространстве или с их использованием.

Международное сотрудничество в области международной информационной безопасности

*Страны-участницы будут обмениваться передовым опытом в области предупреждения, судебного расследования и ликвидации последствий преступной деятельности, в том числе террористической, с использованием информационного пространства на добровольной и взаимной основе.*Обмен может осуществляться как в двустороннем, так и в многостороннем порядке. Государство-участник, предоставляющее информацию, может устанавливать требования конфиденциальности. Государство-участник, получившее такую информацию, может использовать ее в качестве аргумента в своих отношениях с государством-участником, предоставившим ее, при обсуждении вопросов взаимной помощи.

Каждое Государство-участник стремится установить меры укрепления доверия при использовании информационного пространства в военных целях, включая:

1) обмен национальными концепциями по обеспечению безопасности в информационном пространстве;

2) оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах по их устранению и нейтрализации;

3) консультации по деятельности в информационном пространстве, которая может касаться государств-участников, и сотрудничество по урегулированию конфликтных ситуаций военного характера.

Основы государственной политики Российской Федерации в области обеспечения международной информационной безопасности до 2020 года.

Утверждена Президентом Российской Федерации В. Путиным 24 июля 2013 г. приказом PQ-1753.

Реализация документа стратегического планирования Российской Федерации, определяющего основные угрозы в сфере международной информационной безопасности, цели, задачи и

приоритеты государственной политики Российской Федерации в области международной информационной безопасности, а также механизмы их защиты.

Эти фундаменты предназначены для:

а) продвижение российских инициатив на международной арене в области формирования международной системы информационной безопасности, в том числе совершенствование ее правового, организационного и иных видов обеспечения;

б) на формирование межгосударственных целевых программ в области обеспечения международной информационной безопасности, а также государственных и федеральных целевых программ в этой сфере, в реализации которых участвует Российская Федерация;

в) организация межведомственного взаимодействия при реализации государственной политики Российской Федерации в области обеспечения международной информационной безопасности;

г) достижение и поддержание технологического паритета с ведущими странами мира за счет более широкого использования информационно-коммуникационных технологий в реальном секторе экономики.

Под международной информационной безопасностью понимается такое состояние глобального информационного пространства, при котором существует возможность нарушения прав личности, общества и государства в сфере информации, а также деструктивного и противоправного воздействия на элементы информационного пространства. национальная важная информационная инфраструктура. Исключенный.

В рамках Международной системы информационной безопасностиотносится к совокупности международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства.

Международная система информационной безопасности направлена на противодействие угрозам стратегической стабильности и развитие равноправного стратегического партнерства в глобальном информационном пространстве.

Основной угрозой в сфере международной информационной безопасности является использование информационных и

коммуникационных технологий:

а) осуществление враждебных действий и актов агрессии, угрожающих международному миру, безопасности и стратегической стабильности, дискредитирующих суверенитет, нарушающих территориальную целостность государств, как информационное средство в военно-политических целях, противоречащих международному праву;

б) в террористических целях, включая деструктивное воздействие на элементы важной информационной инфраструктуры, а также пропаганду терроризма и привлечение новых сторонников к террористической деятельности;

в) вмешательство во внутренние дела суверенных государств, нарушение общественного порядка, разжигание национальной, расовой и межконфессиональной вражды, пропаганда расистских и ксенофобских идей или теорий, вызывающих ненависть и дискриминацию, подстрекательство к насилию;

г) совершение преступлений путем создания, использования и распространения вредоносных программ для ЭВМ, в том числе преступлений, связанных с неправомерным доступом к компьютерным данным.

Цель государственной политики Российской Федерации - заключается в содействии установлению международно-правового режима, направленного на создание условий для формирования международной системы информационной безопасности.

Достижению цели государственной политики Российской Федерации будет способствовать участие Российской Федерации в решении следующих задач:

а) формирование двусторонней, многосторонней, региональной и глобальной системы международной информационной безопасности;

б) создание условий для снижения риска использования информационно-коммуникационных технологий для осуществления враждебных действий и агрессивных действий, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и создание угрозы международному миру, безопасности и стратегической стабильности;

v) формирование механизмов международного сотрудничества в сфере противодействия угрозам использования информационно-

коммуникационных технологий в террористических целях;

г) создание условий для противодействия угрозам использования информационно-коммуникационных технологий в экстремистских целях, в том числе вмешательства во внутренние дела суверенных государств;

д) повышение эффективности международного сотрудничества в сфере борьбы с преступностью в сфере использования информационно-коммуникационных технологий;

е) обеспечить технологический суверенитет государств в сфере информационных и коммуникационных технологий и создать условия для ликвидации информационного разрыва между развитыми и развивающимися странами.

Основные направления государственной политики Российской Федерации, связанные с решением проблемы формирования системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях:

а) создать условия для продвижения российской инициативы на международной арене в случае необходимости разработки и принятия государствами-членами ООН Конвенции об обеспечении международной информационной безопасности;

б) Поддержать российские инициативы в области формирования международной системы информационной безопасности в итоговых документах, выпущенных по результатам работы правительственной экспертной группы по достижениям в области информатизации и телекоммуникаций ООН. Содействие в разработке правил поведения под эгидой Организации Объединенных Наций в сфере международной безопасности, а также международной информационной безопасности, отвечающих национальным интересам Российской Федерации;

в) проведение регулярных двусторонних и многосторонних экспертных консультаций с государствами-членами Шанхайской организации сотрудничества, государствами-членами Содружества Независимых Государств, государствами-членами Организации Договора о коллективной безопасности, государствами-членами БРИКС, согласование позиций и планов действий. государства-члены, страны Азиатско-Тихоокеанского экономического сотрудничества, «Группы восьми», «Группы двадцати», другие

страны и международные организации в области международной информационной безопасности;

г) продвижение российской инициативы по интернационализации управления информационно-телекоммуникационной сетью «Интернет» на международной арене и повышение роли Международного союза электросвязи в этом контексте;

д) организационное и кадровое укрепление структурных подразделений федеральных органов исполнительной власти, осуществляющих реализацию государственной политики Российской Федерации, а также совершенствование координации деятельности федеральных органов исполнительной власти в этой сфере;

е) создание механизма участия российского экспертного сообщества в совершенствовании аналитического и научно-методического обеспечения продвижения российских инициатив в области формирования международной системы информационной безопасности;

ж) создание условий для заключения международных договоров о сотрудничестве в области обеспечения международной информационной безопасности между Российской Федерацией и иностранными государствами;

з) укрепление взаимного сотрудничества в рамках Соглашения о сотрудничестве в области международной информационной безопасности между правительствами государств-членов Шанхайской организации сотрудничества и содействие расширению сферы членства настоящего Соглашения;

и) использование научного, исследовательского и экспертного потенциала Организации Объединенных Наций и других международных организаций для продвижения российских инициатив в области формирования международной системы информационной безопасности.

Основные направления научных исследований в области информационной безопасности Российской Федерации:

Утвержден Секретарем Совета Безопасности Российской Федерации. Патрушевым 31.08.2017 г.

Общенаучные проблемы обеспечения информационной безопасности Российской Федерации:

1 Общие методологические проблемы защиты информации:

1.1. Проблемы формирования понятийного (терминологического) аппарата в области информационной безопасности.

1.2. Проблемы развития информационного поля как системообразующего фактора жизни общества.

1.3. Проблемы противодействия угрозам и угрозам информационной безопасности личности, общества, государства и международного сообщества.

1.4. Проблемы развития системы информационной безопасности Российской Федерации.

1.5. Проблемы влияния информационного сектора на конкурентоспособность России на современном этапе.

1.6. Проблемы оценки информационной безопасности личности, общества и государства.

1.8. Проблемы сохранения духовно-нравственных ценностей многонационального русского народа.

1.9. Проблемы выявления, выявления, классификации, оценки угроз информационной безопасности.

2. Проблемы развития нормативно-правового и нормативно-технического обеспечения информационной безопасности

3. Проблемы безопасности личного, группового и массового сознания:

3.1. Проблемы обеспечения безопасности личности, общества и государства от воздействия деструктивной информации.

3.3. Проблемы противодействия информационному влиянию на граждан России, в том числе проблемы нарушения исторических основ и патриотических традиций, связанных с защитой Родины.

3.4. Проблемы противодействия использованию информационных технологий для пропаганды терроризма, привлечения новых сторонников к террористической деятельности, планирования и организации террористической деятельности.

4. Проблемы противодействия использованию информационных технологий в преступных целях.

5. Проблемы прекращения и предотвращения военных конфликтов, которые могут возникнуть в результате агрессивного и иного враждебного использования информационных технологий.

Научно-технические проблемы обеспечения информационной

безопасности Российской Федерации:

— современные информационные технологии, научно-технические проблемы развития информатизации, телекоммуникаций и средств связи местной промышленности;

— научно-технические проблемы защиты информационных ресурсов, информационных систем и сетей связи;

— научно-технические проблемы использования информационных технологий в оперативно-розыскной деятельности;

— проблемы информационной безопасности персонала Российской Федерации;

— проблемы формирования международной системы информационной безопасности;

— проблемы снижения риска использования информационно-коммуникационных технологий при осуществлении враждебных действий и актов агрессии, угрожающих дискредитацией государственного суверенитета, нарушением территориальной целостности государств, международного мира, безопасности и стратегической стабильности.

1. Проблемы установления международно-правового режима нераспространения «информационного оружия», снижения риска его применения.

2. Проблемы формирования универсального института «мер доверия» в сфере противодействия угрозам использования информационно-коммуникационных технологий для осуществления враждебных действий и агрессии, обеспечивающего приемлемый уровень открытости в международно-правовой системе. военная активность в информационном пространстве.

3. Проблемы адаптации и развития международного права по прекращению и предотвращению межгосударственных конфликтов с применением «информационного оружия».

4. Проблемы квалификации враждебного использования информационно-коммуникационных технологий и модели межгосударственной системы мониторинга угроз в сфере международной информационной безопасности.

5. Проблемы противодействия использованию информационно-коммуникационных технологий в

террористических целях.

6. Проблемы обеспечения информационной безопасности важных трансграничных информационных инфраструктур.

7. Проблемы обеспечения равноправного участия государств в решении вопросов безопасной и стабильной работы информационно-телекоммуникационной сети «Интернет».

8. Проблемы формирования и реализации межгосударственной системы мер против использования глобальной информационной инфраструктуры в экстремистских целях, в том числе вмешательства во внутренние дела суверенных государств.

9. Проблемы создания международного механизма постоянного контроля за предотвращением использования информационно-коммуникационных технологий в экстремистских целях, в том числе вмешательства во внутренние дела суверенных государств.

10. Проблемы обеспечения сбалансированности мер по обезличиванию действий, угрожающих стабильной и безопасной работе интернет-информационно-телекоммуникационной сети, соблюдению прав и свобод каждого человека на поиск, получение и распространение всех видов информации и идей, особые обязанности и особая ответственность при использовании этих прав и свобод, а также их правовые ограничения, необходимые для уважения прав и репутации других лиц и обеспечения национальной безопасности, общественного порядка, здоровья и нравственности населения с учетом возможности. .

11. Проблемы борьбы с преступностью при использовании информационно-коммуникационных технологий.

12. Проблемы совершенствования аналитического и научно-методического обеспечения продвижения российских инициатив в области формирования международной системы информационной безопасности.

13. Проблемы выявления новых угроз в сфере международной информационной безопасности при внедрении предсказуемых технологических новшеств.

14. Проблемы обеспечения баланса мер по защите технологического суверенитета государств и ликвидации информационного разрыва между развитыми и развивающимися странами в сфере информационно-коммуникационных технологий.

15. Проблемы совершенствования международного сотрудничества правоохранительных органов государств в области использования информационно-коммуникационных технологий в сфере борьбы с преступностью, в том числе вопросы повышения эффективности обмена информацией между правоохранительными органами государств в период расследование преступлений. совершенствование механизма обмена информацией в сфере использования информационно-коммуникационных технологий, а также о методах следственной и судебной практики рассмотрения дел, связанных с данной категорией преступлений.

Проблемы информационной безопасности: алогизмы развития. В начале 1990-х годов, когда термин «информационная безопасность» только начинал появляться в политологических трудах, определяемая им сфера отношений понималась как антитеза информационной войне. Кроме того, само информационное противоборство определялось в то время только в стиле межгосударственного силового противостояния. Не исключалось, что участниками конфликта могли быть и негосударственные акторы, но под ними обычно понимались внутриполитические силы, которым противостояла вооруженная борьба за власть. Тогда такие конфликты называли «невоенными конфликтами», часто имея в виду гражданские войны, борьбу за национальную независимость и автономию и тому подобное.

В то время только США были активными сторонниками борьбы с информационной угрозой. Первые разработки в области военно-информационных операций велись также в США, где с 1993 г. начали готовиться различного рода воинские уставы, инструкции и доктрины ведения информационных операций.

В 1998 году Объединенный комитет начальников штабов опубликовал основополагающую работу под названием «Совместная доктрина информационных операций», в которой информационная война получила описание практического предмета. В то время по понятным причинам никто не задумывался о значении Интернета и социальных сетей для активного противостояния в информационном пространстве, а психологические операции, как тактические, так и стратегические, были непосредственно связаны с информационной сферой. Тем не менее, спустя годы, в 2004 году, представитель США в Группе правительственных экспертов ООН по

международной информационной безопасности заявил, что угрозы информационной войны нет, а сама информационная война не более чем химера. С точки зрения Вашингтона, киберпреступность следует считать серьезной угрозой. И все еще,

С тех пор многие страны и международные организации начали заниматься проблемой информационной безопасности. Тем временем завершила свою работу четвертая Группа правительственных экспертов ООН по международной информационной безопасности (ГГЭ ИИС).

С 1998 г. Генеральная Ассамблея ООН принимает резолюцию «Достижения в области связи и информации в контексте международной безопасности», непосредственно посвященную этой проблеме, почти всегда на основе консенсуса. Кроме того, данная резолюция принимается первым комитетом по вопросам международной безопасности. Третий комитет продвигал резолюцию «Культура кибербезопасности» в течение трех лет.

Вопросы информационной безопасности и информационного общества заняли постоянное место в повестке дня. Международного союза электросвязи (МСЭ) под его эгидой в 2003 и 2005 годах в два этапа. состоялся крупнейший современный форум в области информационной безопасности – Всемирный саммит по информационному обществу.

Информационная безопасность и кибербезопасность являются одними из наиболее важных вопросов для таких международных организаций. Такие как ШОС, БРИКС, Организация по безопасности и сотрудничеству в Европе (ОБСЕ), Форум региональной безопасности (АРФ) Ассоциации государств Юго-Восточной Азии. НАТО и Организация Договора о коллективной безопасности (ОДКБ) активно работают над военными аспектами этой проблемы. Борьба с терроризмом уже давно сводилась к использованию Интернета в пропагандистских целях, вербовке новых членов и организации терактов. Вопросы киберпреступности не покидают заголовки основных СМИ. Конференции, симпозиумы, семинары, так или иначе тематически связанные с повесткой информационной безопасности,

Проблемы информационной безопасности актуализировались после сообщений о том, что такие вредоносные программы, как Stuxnet, Duqu, Flame, Gauss, могут работать в различных

программных средах, распространяться через Интернет и наносить серьезный физический ущерб различным, в том числе критическим, программам. и особо опасных производственных, транспортных, энергетических объектов. Информационные системы управления критическими инфраструктурами стали не только объектом защиты, но и объектом атак. Специалисты предвидели и реализовали эту угрозу еще 20 лет назад, но не смогли объяснить мировому сообществу необходимость национальной и международной защиты всего информационного пространства (не только сетей связи и аппаратно-программных продуктов, таких как Интернет).

Постепенно и политологам, и политикам становится ясно, что постиндустриальному обществу нужен не только мирный атом, но и мирное информационное пространство. Договор о нераспространении ядерного оружия (ДНЯО) стал поворотным пунктом в истории военных ядерных технологий. Конечно, в постиндустриальном обществе такое соглашение заключить сложно, но борьба с информационной угрозой по-прежнему требует многосторонних усилий аналогичного масштаба и глубины. Если это удастся сделать, можно будет сказать, что человечество осознало бесперспективность насилия в международных отношениях.

Но сегодня не у всех одинаковое понимание сущности и формирования такой задачи. Сегодня в общем дискурсе международной информационной безопасности четко обозначились три направления, которые можно с некоторой долей традиционализма охарактеризовать как либеральное, консервативное и прагматическое.

1) Либералы.Их также можно назвать «Защитниками свободы Интернета». Большинство людей, интересующихся информационной безопасностью сегодня, попадают в эту широкую группу.

Большинство либералов — молодые люди. Сейчас с появлением планшетов даже использование клавиатуры стало для многих из них интеллектуальным вызовом — проведите пальцем по экрану, вместо того, чтобы писать письмо, можно поделиться фотографиями, сделанными с тех же гаджетов. Вот как эта группа рассматривает обмен информацией и доступ к ней.

Вторая по величине часть этой группы - активные пользователи Интернета, которые по роду своей основной деятельности имеют

дело с важными инфраструктурами, деятельностью армии, силовых и правоохранительных органов, вопросами, составляющими государственную тайну - и вообще с вопросами государственной деятельности. и безопасность. Конечно, эта группа тоже неоднородна, но с точки зрения нашей проблемы ее объединяет приверженность одному тезису - глобальная сеть должна, прежде всего, обеспечивать свободу использования информации и свободу распространения информации. .

Сторонники свободы Интернета считают, что безопасность может быть достигнута только через абсолютную, неограниченную свободу от кого бы то ни было. Однако сторонники либерального подхода защищают не свободу и безопасность, а приказы тех, кто реально контролирует и использует интернет, детскую порнографию и теракты, торговцев оружием и распространителей опаснейших вещей, политические и финансовые интересы. товары и услуги.

Интересно, как изменится их риторика в будущем, когда Интернет будет разделен на несколько глобальных сетей - будет ли в их понятие свободы входить свобода новых сетей, которые смогут конкурировать друг с другом? Если задать вопрос таким образом, ответ не будет ясен. Другой альтернативой может быть фрагментация сети, предполагающая формирование множества зеркал отдельных доменов или их групп, теоретически локализованных в одной стране.

2) Консерваторы, сторонники бумажной информации. Эти, вероятно, настроены сохранить свое сознание на уровне начала 19 века, в пользу безопасного обмена информацией, предоставляя возможность ограничить доступ к документам. Однако надо признать, что сегодня их количество очень мало и оно все больше сокращается. Как ни странно, понимание этой информации - как документа - устанавливает основную часть правовых норм как в России, так и в других странах.

Консерваторы тоже не всегда знают, чего хотят. Никто не может понять, что это за документ - текстовая бумага или что-то другое? Каков его достаточный символ, регистрационный номер или текст? А как же рисунки и картины? И подобных вопросов много: как определить, есть ли в документе единичная цифра, есть ли смысл в тексте или в рисунке в документе, и в итоге, что надо сохранить и что должно быть? заменены при работе с документом?

3) прагматики,те, кто понимает важность рассмотрения всех форм существования и движения информации и связывает информацию с фундаментальными, имманентными категориями существования. Первоначально эти позиции заняли военные, которые называли средствами радиоэлектронной борьбы информационные средства, бомбы - электрические выключатели, химические и биологические средства, выводящие из строя электронную аппаратуру, психотропные средства и т. д. Решающим фактором здесь является принцип воздействия на информацию, системы ее обработки, в том числе на человеческое сознание, а также системы ее передачи и хранения.

В этом случае данные следует определять гораздо шире. В частности, следует признать, что такая информация не имеет прямого отношения к физическому лицу. Информацию следует рассматривать не только как смысловой результат мозговой деятельности, генерируемый и локализующийся в нем, но и как коммуникативную основу любого взаимодействия. Тогда оказывается, что оно обменивается со всеми объектами материального и вообще идеального мира, способно взаимодействовать, может передаваться и приниматься в разное время, связано с явлением. , его можно познать теологически (через веру). Носители в компьютерных сетях и сетях связи содержат информацию, которую необходимо защищать.

Три подхода, отличающиеся своим подходом к проблеме и выдвигающие на первый план разные ее стороны, отражают естественный процесс познания, который не обязательно является линейным и последовательным.

Сторонники первого подхода.Стремление консолидировать или перераспределить права на контроль над Интернетом, сохраняя при этом или перераспределяя значительные финансовые потоки, связанные с владением этими правами. Поэтому ключевую роль здесь играет один из крупнейших игроков на этом рынке, компания XEI. Поэтому, не скрывая своих интересов, ему противостоят США, которые создали Интернет, в основном его контролируют и, естественно, не хотят уступать свои естественные права на него.

Второй подходкак и на выборах, это представляет собой старую и, возможно, умирающую тенденцию перекачивать голоса оппозиции, а не предлагать свой собственный путь.

Сторонники третьего, прагматичного подходапротивостоять первым двум. На Всемирном форуме по информационному обществу представители почти всех стран проголосовали за интернационализацию управления Интернетом, и продвигала эту идею не Россия, а Евросоюз. При этом представителей ЕС не остановил прямой конфликт по этому поводу с присутствовавшей на форуме делегацией «старшего брата».

Интернационализация управления Интернетом, безусловно, хороший и позитивный процесс, но проблема не в нем. Информационное (не только кибернетическое) пространство само по себе не должно быть уязвимым и в то же время не должно быть источником или каналом реализации военных, террористических или криминальных (неразрывная триада) угроз другим сферам общественной деятельности человека. А государство должно быть гарантом информационной безопасности и нести ответственность за действия, осуществляемые с его территории или информационного пространства. Это касается, в первую очередь, активного противодействия в информационной сфере, то есть угрозы военных действий. Общество возложило на государство функцию обеспечения не только внешней, но и внутренней безопасности.

Противники введения в информационное пространство каких бы то ни было правил, норм и иных ограничений часто ссылаются на права человека, в частности на статью 19 Всеобщей декларации прав человека, которая гласит: «Каждый человек имеет право на свободу убеждений». . и выражение; это право включает свободу придерживаться своего мнения и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ.

При этом в предпоследней статье 29 той же Декларации ясно, что свобода одного человека заканчивается там, где начинается свобода другого, что ускользнет от доводов «правозащитников в Интернете». В частности, статья содержит следующие положения, которые не носят ограничительного характера, но должны быть процитированы полностью для понимания демократического контекста:

1. Каждый человек имеет обязательства перед обществом, только так его личность может развиваться свободно и всесторонне.

2. При осуществлении своих прав и свобод каждый подвергается установленным законом ограничениям только в целях обеспечения должного признания и уважения прав и свобод других лиц, выполнения справедливых требований нравственности и общественного порядка. и общее благосостояние в демократическом обществе.

3. Осуществление этих прав и свобод ни в коем случае не должно противоречить целям и принципам Организации Объединенных Наций.

Здесь можно выделить следующие алогизмы.

Алогизм один:военная составляющая ушла из дискурса информационной безопасности. Не вызывает споров, но в то же время не рассматривается по существу. Вместо принятия мер по его предотвращению ведутся дискуссии о повышении доверия к образованию, увеличении возможностей компьютеров, сокращении цифрового разрыва и т. д. Возможно, есть более важные и насущные проблемы, чем начало 1990-х годов. Проблемы. Необходимо сохранить статус-кво в сложившейся расстановке сил в сфере военного информационного развития, производства и внедрения средств информационного воздействия, интернационализации управления Интернетом и снять с повестки дня вопросы управления потоками. связанные с ним деньги, распространяемые через контролируемую «универсальную сеть» сохранить возможность секретности. » социальным группам, средствам массовой информации и общественному сознанию, широкой пропаганде их идей и ценностей.

Среди всех подходов к рассмотрению проблемы военных информационных угроз выделяется обсуждение применения международного гуманитарного права к конфликтам в информационном пространстве. Россия всегда придерживалась позиции, что действующее законодательство распространяется на информационные операции, но оно нуждается в совершенствовании, поскольку формировалось в годы, когда информационные угрозы не рассматривались юридически. Напротив, в документе Пентагона, изданном в 1999 г. и переизданном в 2000 г., четко говорится, что «в настоящее время нет никаких ограничений на информационные операции в соответствии с международным правом».

На конференции НАТО в Стокгольме осенью 2004 г. по

предложению российской делегации тот же тезис был убедительно обоснован европейскими военными юристами. Но в 2009 г. во время второй ГПЭ МИБ эксперт правительства США упомянул о другом подходе, подчеркнув принципы jus ad bellum.

Второй алогизм:На сегодняшний день информационная безопасность делится на две части: информационная безопасность бизнеса, информационная безопасность культуры и т.д.

Информационная безопасность стала брендом. Это отвлекает от сути проблемы и создает иллюзию знания информационной безопасности, ложный смысл.

Алогизм третий.Как отмечалось выше, самая многочисленная армия «борцов за информационную безопасность» выступает за свободу Интернета, яростно отстаивая идею о том, что глобальная сеть — это новый мир, сформировавший новую интернет-культуру. Но кто граждане этого мира? Прогрессивный человек сейчас ассоциируется с блогером, у каждого уважающего себя человека, включая президента, есть блог, хотя лет пять назад в лучшем случае у него была домашняя страница и вообще никто о блогах не знал . Формируется представление о том, что весь мир подключен к Интернету и блогосфере. Однако в серьезной дискуссии все специалисты по информационной безопасности в один голос говорят о том, что Интернета нет ни в одной из критических инфраструктур — даже в серьезном бизнесе, где отношения с заказчиком заканчиваются. И интернет, в общем,

Алогизм четвертыйзаключается в том, что все пытаются обеспечить информационную безопасность, но никто не пытается понять, что это за информация, где и как она существует. Например, в «Новой философской энциклопедии» статья «Информация» ограничивается ссылкой на статью «Теория информации». Делается акцент на анализе аспектов. Ни слова о такой информации.

Аналогичная ситуация наблюдается и за рубежом. Хотя в электронном словаре Министерства обороны США перечислены термины «информационная безопасность», «информационная атака», «информационная операция» и т. д., термина «информация» не существует.

Пятый алогизм.В концепции демократического общества информационная безопасность часто воспринимается как антипод выражения свободы использования и распространения информации.

Однако не следует забывать, что любое общество становится организацией лишь тогда, когда его члены начинают действовать в рамках выработанной этим обществом правовой системы. Основой организации всегда являются нормы поведения и их осознанное восприятие. Что мы реально видим в вопросе информационной безопасности, особенно в ее международной составляющей? Отказ от возможности введения норм и правил поведения государств и других субъектов отношений в информационном пространстве. Вместо этого предлагается культура кибербезопасности.

Шестой алогизм -в современном международно-политическом дискурсе по непонятным причинам противопоставляются идеи суверенитета государства в информационном пространстве и ответственности государства за свои действия из информационного пространства. Какова логика тех, кто выступает за ответственность и отвергает суверенитет? Известно, что обязанности могут основываться только на правах и наоборот. Как вы можете нести ответственность за то, над чем у вас нет контроля, а если нет суверенного контроля, ответственность лежит не только на вас? Если идентифицированный злоумышленник создал ботнет, расположенный в десятках стран, для атаки на Интернет, должны ли эти страны также нести ответственность за его действия? Как создавать ботнеты особенность в том, что владелец ресурсов не знает об их использовании злоумышленником. Чтобы такой пользователь был привлечен к ответственности, как минимум, государство должно иметь право внедрять культуру кибербезопасности и соответствующие меры контроля, которые могут помешать бизнесу пользователя, но все же обязаны (по закону) их соблюдать.

Наоборот, не означает ли суверенитет, что суверен несет ответственность за любые действия в сферах, в которых осуществляются суверенные права? Стоит отметить, что здесь было бы очень уместно принятие кодекса поведения стран в информационном пространстве. Идея разработки такого кода также содержится в Международной стратегии действий в киберпространстве, разработанной администрацией США и представленной Бараком Обамой 22 мая 2011 года. В основу кодекса могут быть положены правила поведения в сфере международной информационной безопасности, предложенные странами ШОС на

66-й сессии Генассамблеи ООН. Такой документ может стать основой для внедрения культуры кибербезопасности на международном уровне, которая естественным образом проецируется на национальный уровень. Однако эта идея

Алогизм седьмойзаключается в интересном противоречии идей теоретиков либерального лагеря. Либералы категорически выступают против включения социальной сферы в сферу информационной безопасности, но при этом делают упор на Интернет и социальные сети. Никто не сомневается, что демократическое государство существует для обеспечения безопасности государства и общества, в частности, надежной работы важных инфраструктур - это его основные задачи, права, данные ему обществом, и вопрос о суверенитете не ставится. в этом случае.

Поэтому предложение об устранении государства в отношении информационной безопасности опасно, оно может привести к анархии в сети.

Можно продолжать, но и без этого понятно, что создание логичной и адекватной концепции информационной безопасности для использования в международных и общественных отношениях еще не завершено.

3.3-§.Политика кибербезопасности: подход Узбекистана

В данной теме о разработке политики обеспечения информационной безопасности на территории Республики Узбекистан, «учитывая основные принципы и порядок разработки и реализации политики обеспечения информационной безопасности в органах государственного и хозяйственного управления, а также в органы местного самоуправления (в следующих местах) выходим

В этой теме выбор практических мер по управлению безопасностью в организации также является основой для обеспечения целостности, удобства использования и конфиденциальности информации при обмене информацией между организациями.

В этой теме используются термины и определения согласно УзДСт 1047:2003 [1], УзДСт 2927:2015 [2], УзДСт ИСО/МЭК 27000:2014 [5].

Политика информационной безопасности организации представляет собой совокупность документально оформленных

инструкций, правил, процедур и практик в области обеспечения информационной безопасности в деятельности организации.

Целями разработки и реализации политики являются:

— определить и защитить ключевые информационные системы и ресурсы;

— формирование организационно-методической основы внедрения системы управления информационной безопасностью (далее - ИСБТ).

Основными задачами, которые предстоит решить при разработке политики, являются:

— защита информационных активов от угроз, вызванных неправомерными действиями злоумышленников;

— управление непрерывной работой системы;

— снизить риск возникновения аварий, умышленных неправильных действий работников, технических сбоев, неверных технологических и организационных решений при обработке, передаче и хранении информации и уменьшить возможный ущерб, обеспечить нормальное функционирование технологических процессов;

— разработка модели нарушения информационной безопасности организации;

— разработать перечень потенциальных угроз информационной безопасности организации и проанализировать их;

— классификация информационных ресурсов объекта и управление ими;

— Формулировка требований к ИСБТ;

— определение обязанностей работников по обеспечению информационной безопасности.

Для разработки политики приказом руководителя организации утверждается рабочая группа, в состав которой должны быть включены следующие лица:

— представитель руководства организации;

— ответственный за информационную безопасность, начальник отдела кадров (кадровой службы);

— представитель технического персонала (администратор информационной безопасности, администратор сети, администратор базы данных или иной уполномоченный персонал (сотрудник)).

При необходимости могут быть привлечены другие работники организации, сторонние специализированные организации или специалисты.

Процесс разработки политики делится на следующие этапы:

Первый этап.

Первичный аудит безопасности, включающий первичную проверку и инвентаризацию ситуации с информационной безопасностью, выявление угроз безопасности организации, выявление ресурсов, нуждающихся в защите, выявление рисков.

В процессе аудита анализируется текущее состояние информационной безопасности, выявляются существующие уязвимости, наиболее важные направления деятельности и наиболее чувствительные процессы организации к угрозам безопасности.

Проведение аудита поможет выявить угрозы и недостатки информационной безопасности организации, а также получить исходную информацию для разработки политики.

В ходе проверки организации осуществляется:

— изучать и анализировать соответствие организации требованиям законодательства Республики Узбекистан, указов и постановлений Президента Республики Узбекистан и Кабинета Министров Республики Узбекистан и согласовывать ее по категориям;

— Согласование нормативно-правовых документов Республики Узбекистан, а также нормативно-правовых документов, документов, регламентирующих вопросы информационной безопасности в организации;

— проведение первичного осмотра компьютеров и серверов организации, то есть анализ используемых операционных систем, настроек программ;

— анализировать сайт организации на наличие угроз и уязвимостей информационной безопасности;

— анализ принимаемых мер по обеспечению физической защиты территории, периметра и зданий организации, то есть анализ системы безопасности, средств контроля доступа, системы пожарной безопасности и т. д.;

— оценка осведомленности работников организации о правилах информационной безопасности, установленных в организации, путем проведения собеседования;

— анализ категоризации и инвентаризации информационных и материальных ресурсов организации.

Второй этап.

Разработка проекта политики информационной безопасности организации.

При разработке политики необходимо соблюдать следующие основные правила:

— полис должен полностью соответствовать действующему законодательству и требованиям государственных стандартов;

— текст политики должен содержать четкие и недвусмысленные формулировки, не допускающие двойного толкования.

В целом политика должна иметь четкое представление о необходимом поведении пользователей, администраторов и других специалистов в процессе реализации. Использование информационных систем и средств защиты информации, а также операции по обмену и обработке информации. Политика — это общедоступный документ, который может быть предоставлен всем заинтересованным сторонам в организации без ограничений.

Третий этап.

Согласование и реализация политики информационной безопасности организации. Разработанный проект политики будет направлен в Министерство по развитию информационных технологий на согласование в установленном порядке.

Вступает в силу приказом руководителя организации после взаимного согласования и согласования между Республикой Узбекистан и уполномоченными органами. В то же время необходимо разработать утвержденную политику, чтобы полностью ее реализовать. Должностные инструкции сотрудников, положения о подразделениях, договорные (договорные) обязательства организации должны включать обязательства и обязанности по обеспечению информационной безопасности.

Необходимо обеспечить процедуру ознакомления всех работников организации и проводить регулярные разъяснения по требованиям и положениям утвержденной политики, а также по обеспечению информационной безопасности.

Если требования политики остаются внешними по отношению к организации, договорные обязательства с третьими сторонами должны включать требования информационной безопасности.

Пересмотрите и обновите политику информационной безопасности организации.

Политика должна пересматриваться не реже одного раза в год, а также в следующих случаях:

— в изменении и утверждении новых нормативных правовых документов и нормативных документов по информационной безопасности;

— при изменении, добавлении или удалении конфигурации;

— при изменении конфигурации и параметров технических средств защиты данных объекта;

— должностные лица - при изменении содержания и задач пользователей.

Политика должна полностью пересматриваться при изменении технологии обработки информации или при использовании новых средств защиты информации. Действия организации в области информационной безопасности должны регулярно проверяться на соответствие политике. Актуализация политики и оценка ее эффективности осуществляется путем проведения внутренних и внешних аудитов на предмет соответствия информационной инфраструктуры организации утвержденным требованиям и регламентам политики.

Частота аудита определяется политикой, внутренний аудит должен проводиться не реже одного раза в шесть месяцев, а внешний аудит — не реже одного раза в год.

Порядок выдачи политики информационной безопасности

Структура политики информационной безопасности

Структура политики и ее детали могут различаться в зависимости от особенностей организации, но в их основе должна быть типовая структура, включающая следующие разделы:

— Введение;

— Нормативные ссылки;

— Понятия и определения;

— Символы и сокращения;

— Область применения;

— Цели и задачи;

— Основные моменты;
— объекты обороны;
— модель рисков и угроз информационной безопасности;
— модель нарушения информационной безопасности;
— Меры защиты информации;
— Реагирование на инциденты информационной безопасности;
— Обеспечение безопасности каналов связи;
— Распределение обязанностей;
— Процедура обзора и обновления политики;

Кроме того, политика может содержать или содержать ссылки на следующие документы, утвержденные в установленном порядке руководством организации:

— Положение об организации локальной (корпоративной) сети и защищенных сетевых соединений;
— Положение об обеспечении информационной безопасности на уровне сетевой инфраструктуры и межсетевого экрана;
— Инструкция для системного администратора локальной (корпоративной) сети;
— Регламент обновления системного и прикладного программного обеспечения, а также резервного копирования и восстановления данных;
— Инструкции по защите паролем;
— Руководство по защите от вирусов;
— Инструкции по обеспечению безопасности при работе с устройствами хранения данных, мобильными устройствами, устройствами хранения данных;
— Правила разработки матрицы доступа к информационным ресурсам автоматизированной системы;
— Список разрешенных к использованию программ;
— Инструкции по работе с Интернетом и корпоративной электронной почтой;
— Порядок управления информационными активами организации;
— Инструкция по организации технической защиты информации;

— Инструкция по организации защиты криптографической информации;

— Порядок работы с информацией, подлежащей защите;

— План обеспечения непрерывной работы и восстановления организации в аварийных (нештатных) ситуациях.

Содержание разделов Политики

Введение должно содержать общую информацию об организации. Раздел «Нормативные документы» должен включать список всех нормативных документов, на которые ссылается политика. Определения всех используемых терминов должны быть включены в раздел «Термины и определения». Раздел «Символы и сокращения» должен включать все символы и сокращения, используемые в политике. В разделе Scope нужно указать область действия документа и пределы его действия. Основные цели и задачи политики должны быть перечислены в разделе о целях и задачах. Принципы, методы и меры обеспечения информационной безопасности в организации должны быть указаны в разделе основных правил. Средства безопасности limi необходимо указать защищаемые активы организации. В активы организации входят:

— работники организации, информационные ресурсы, чувствительные к случайным и несанкционированным воздействиям и нарушениям их безопасности, в том числе общедоступная информация, предоставляемая в виде документов и массивов данных, независимо от формы и вида представления;

— программные ресурсы - операционные системы и прикладные программы, средства разработки и утилиты, серверные приложения и сервисы;

— физические ресурсы - компьютерное и коммуникационное оборудование, носители информации, здания и т.д.

В разделе модели рисков и угроз информационной безопасности необходимо представить основные принципы анализа рисков информационной безопасности в организации, в том числе связанных с взаимодействием со сторонними организациями. Если для деловых целей требуется доступ третьих лиц к информационным активам организации и средствам обработки информации, а также при получении товаров и услуг от третьих лиц, следует проводить анализ рисков для определения возможных последствий для

требований информационной безопасности и контроля. Такая деятельность должна быть согласована и указана в договорах, заключенных со сторонней организацией.

Если есть необходимость разрешить внешним организациям доступ к средствам обработки информации или информационным активам организации, необходимо определить риски, чтобы установить требования к конкретным средствам контроля. При определении рисков, связанных с доступом третьих лиц, следует учитывать средства обработки данных, к которым необходим доступ третьих лиц.

Организации могут столкнуться с рисками, связанными с процессами управления внутренними коммуникациями организации, если используется высокий уровень аутсорсинга или если задействовано несколько третьих сторон.

Средства контроля описывают соглашения с различными третьими сторонами, такими как:

— поставщики услуг, такие как интернет-провайдеры, телефонные службы, службы технического обслуживания и поддержки;

— управляемые службы безопасности;

— аутсорсинговые объекты или операции, такие как системы информационных технологий, услуги по хранению информации, колл-центры;

— персонал, обслуживающий аппаратное и программное обеспечение;

— работники, занятые уборкой, охраной, общепитом и другими бытовыми услугами;

— временные сотрудники, студенты и контрактники (клиенты).

Эти соглашения помогают снизить риски, связанные с третьими лицами.

Потенциальные угрозы информационной безопасности делятся на два вида по характеру их возникновения: естественные (объективные) и искусственные (субъективные). Источники угроз самой информационной системе могут быть внешними и внутренними.

Все источники угроз делятся на классы в зависимости от типа носителя угрозы (источника угрозы):

— источники угроз, возникающих в результате действий субъекта (человеческий фактор), которые можно квалифицировать как умышленные или случайные нарушения;

— источники техногенных технических угроз определяются технократической деятельностью человека;

— естественные источники угроз, возникающих в результате природных явлений, которые непредсказуемы или предсказуемы, но не могут быть предотвращены на современном уровне человеческих знаний и возможностей.

Классификация нарушителей информационной безопасности приведена в разделе нарушители информационной безопасности. Нарушители информационной безопасности делятся на две группы по принадлежности: внутренние и внешние. Внутренними потенциальными нарушителями являются сотрудники организации, имеющие доступ на территорию информационных объектов.

Основные меры по обеспечению информационной безопасности организации делятся на следующие:

— правовые меры;

— морально-этические меры;

— организационные меры;

— технологические мероприятия;

— инженерная деятельность;

— программно-аппаратные меры;

— меры безопасности в отношениях с внешними пользователями.

К правовым мерам обеспечения информационной безопасности относятся законы Республики Узбекистан и иные нормативные правовые документы, регламентирующие правила работы с информацией, определяющие права и обязанности участников информационных отношений в процессе обработки и использования информации, а также определить ответственность за нарушения. Этика и меры включают в себя нормы поведения, которые традиционно формировались или развивались с распространением информационных технологий. Эти нормы часто носят необязательный характер, так как являются нормативными документами, утвержденными законом, однако их несоблюдение может привести к снижению репутации человека, группы лиц или организации в целом. Морально-этические нормы тоже не писаны,

также неписаны, т. е. оформлены в определенном законе или своде правил (уставе). Морально-этические гарантии носят превентивный характер и требуют постоянной работы по созданию здоровой этической среды в коллективе организации.

Организационные мероприятия в основном направлены на работу с работниками, выбор мест и расстановку объектов защиты, организацию систем физической и противопожарной защиты, контроль за выполнением принимаемых мер, определение персональной ответственности за выполнение мероприятий охраны. Применяются меры по снижению количества внутренних антропогенных и техногенных факторов.

Организационное устранение угроз является наименее затратной мерой защиты информации. К мерам технологической защиты относятся различные технологические решения и приемы, основанные на определенных видах резервирования (конструктивном, функциональном, информационном, временном и т.

Эти меры включают:

— использовать ответственные процедуры двойной записи;

— приступать к ответственным операциям только при наличии согласия нескольких лиц;

— процедуры проверки деталей исходящих и входящих сообщений и т. д.

Инженерно-технические методы направлены на оптимальное строительство зданий, сооружений, инженерных сетей и транспортных коммуникаций с учетом требований по обеспечению информационной безопасности.

Инженерная деятельность включает в себя:

— обеспечение электрозащиты оборудования и зданий;

— осмотр помещений;

— защита зданий от разрушения;

— оптимальное размещение оборудования;

— оптимальное размещение инженерных коммуникаций;

— использование средств защиты зрения;

— акустическая обработка зданий;

— использование систем кондиционирования.

Технические мероприятия основаны на использовании специальных технических средств защиты информации, контроля

обстановки и направлены на устранение угроз, связанных с попытками внешних угроз воздействовать на информацию с использованием технических средств.

Некоторые из этих мер позволяют устранить влияние техногенных источников угроз и снизить влияние объективных, субъективных и случайных уязвимостей.

К техническим мерам относятся:

— резервирование технических средств обработки;

— резервирование каналов связи;

— использование выделенных каналов связи;

— создание резервной копии (дубликата) информационных ресурсов;

— создание системы пространственного шума;

— создание акустико-виброшумовой системы;

— экранирование агрегатов и оборудования;

— использование гарантированных источников питания;

— управление каналами связи для передачи информации;

— контроль отсутствия электронных устройств для сбора информации в информационных объектах.

Программно-технические средства предназначены для устранения проявления угроз, непосредственно связанных с процессом обработки информации. Реализация программно-технических мероприятий позволит значительно снизить воздействие внутренних техногенных источников угроз. Группа программно-аппаратных мер объединяет следующие меры:

— ограничение использования средств обработки информации (программных, аппаратных средств);

— ограничение доступа к защищаемым объектам (защищаемой информации);

— контролировать доступ к сущностям (пользователям);

— управление внешними и внутренними информационными потоками;

— скрыть структуру и цель;

— подтвердить достоверность данных;

— хранение данных при преобразовании (шифровании, кодировании);

— блокировать неиспользуемые услуги;

— целостность программного обеспечения, мониторинг конфигурации программного и аппаратного обеспечения;

— защита от вируса;

— мониторинг событий и инцидентов информационной безопасности;

— отслеживание действий пользователей корпоративной сети.

При предоставлении доступа к информации и организационным активам третьим лицам необходимо обращать внимание на все установленные требования информационной безопасности и принимать меры безопасности при работе с внешними пользователями.

Прежде чем предоставить третьим лицам доступ к любому из активов организации, следует рассмотреть следующие требования информационной безопасности (в зависимости от типа и уровня предоставленного доступа могут применяться не все из них):

— процедуры защиты активов организации, включая информацию и программное обеспечение, и управления известными уязвимостями;

— процедуры определения того, были ли активы скомпрометированы, например, в результате потери или изменения данных;

— целостность активов;

— ограничения на копирование и разглашение;

— описание предоставляемых товаров и услуг;

— различные условия доступа клиентов, требования и преимущества.

Контракты на управление доступом включают в себя:

— управлять и использовать авторизованные методы доступа и уникальные идентификаторы пользователей и пароли;

— Привилегии и процесс авторизации;

— принцип запрета любого доступа, который прямо не разрешен;

— процесс отзыва прав доступа пользователя или блокировки доступа;

— Процедуры оповещения, оповещения и проверки фактов нарушения информационной безопасности и обнаружения слабых звеньев в системе безопасности;

— описание каждой службы для доступа;

— запланированные уровни обслуживания и неприемлемые уровни обслуживания;

— право контролировать и отменять любую деятельность, связанную с активами организации;

— соответствующие обязательства организации и клиента;

— обязательства в отношении юридических вопросов и способы соблюдения правовых требований, таких как законы о защите данных, с учетом различных национальных правовых систем, если контракт предполагает сотрудничество с зарубежными клиентами;

— защита прав интеллектуальной собственности и авторских прав, а также любых совместных работ.

Требования информационной безопасности, предъявляемые к сторонним сотрудникам, имеющим доступ к активам организации, могут существенно различаться в зависимости от классификации предоставляемой информации и средств ее обработки. Эти требования безопасности могут быть отражены в договоре с сотрудником сторонней организации, который включает в себя все известные риски и требования по информационной безопасности.

Контракты с третьими лицами могут иметь другие требования безопасности. В соглашении о праве доступа третьих лиц должно быть указано разрешение на привлечение других соответствующих лиц, а также условия их доступа и участия.

Раздел реагирования на инциденты ИБ должен включать описание процесса реагирования на инциденты ИБ, включая средства системного аудита для автоматизированных областей обработки информации, а также процедуры отчетности об инцидентах ИБ для всех сотрудников организации и другие статусы, которые включают защиту данных. системы.

В данном разделе должны быть описаны механизмы реагирования на инциденты, например, информация об обнаружении инцидентов нарушения ИБ будет доведена до руководства и будет доведена до администратора ИБ в установленном порядке. Запрещаются самостоятельные и

несанкционированные действия, не регламентированные документами или соответствующими инструкциями.

При выявлении каналов утечки информации принимаются меры по локализации зоны обработки информации с целью предотвращения дальнейшей утечки, а в организации останавливаются процессы, связанные с обработкой защищаемой информации. В случае заражения вредоносными программами будут приняты меры по устранению причиненного ущерба в соответствии с «Инструкцией по защите от вирусов организации».

Для эффективного управления инцидентами в организации в этом разделе должны быть описаны обязанности и процедуры для эффективного и оперативного разрешения инцидентов и уязвимостей информационной безопасности. В ответ должны быть реализованы процессы постоянного улучшения, мониторинга, оценки и общего управления инцидентами информационной безопасности.

Процедура управления инцидентами должна быть разработана и утверждена для обеспечения быстрого, эффективного и организованного реагирования на инциденты информационной безопасности. Помимо сообщений, необходим мониторинг событий и уязвимостей информационных систем, систем оповещений и уязвимостей для выявления инцидентов информационной безопасности. Цели управления инцидентами ИБ должны быть согласованы с руководством, а приоритеты организации по разрешению инцидентов должны быть доведены до сведения сотрудников, ответственных за управление инцидентами ИБ.

Раздел «Обеспечение безопасности каналов связи».

Каналы связи должны быть направлены на снижение возможности несанкционированного доступа к информации путем подключения к информационным кабелям или удаление ложных электромагнитных излучений и информации путем наводки в других кабелях, а также на обеспечение защиты кабельного оборудования от электромагнитных помех и механических повреждений.

Защита беспроводных каналов связи должна быть направлена на снижение таких атак, как прослушивание трафика, отказ в обслуживании, несанкционированное подключение.

Раздел «Распределение обязанностей». Этот раздел является одним из важных разделов политики и должен отражать принципы

управления информационной безопасностью организации путем руководства, разделения обязанностей и координации вопросов информационной безопасности. В этом разделе должны быть четко определены все обязанности по обеспечению информационной безопасности.

Для обеспечения надлежащей защиты информационных ресурсов организация должна вести учет всех информационных ресурсов. Для этого должны быть идентифицированы и сформированы все ресурсы, а также актуализирован реестр информационных ресурсов автоматизированных систем организации (далее - Реестр).

Реестр должен содержать всю информацию, необходимую для аварийного восстановления, включая тип ресурса, формат, местоположение, информацию о резервном копировании и категории. Этот регистр не должен без необходимости дублировать другие регистры, но их содержание должно быть согласованным. Для этого после регистрации ресурса в кабинете данный номер удаляется в реестре автоматизированной системы, где находится ресурс.

Реестр представляет собой документ (на бумажном или электронном носителе), который регистрируется в офисе организации и содержит все информационные ресурсы организации, подлежащие защите. По решению руководителя организации реестр может вестись в отношении всей организации или ее структурного подразделения.

За всеми информационными ресурсами должны быть закреплены их владельцы, которые несут ответственность за обеспечение безопасности этих ресурсов.

Владелец ресурса несет ответственность за правильную категоризацию ресурса, а также за определение и периодическую проверку категорий и прав доступа к этому ресурсу. При необходимости владельцы ресурсов могут делегировать обязанности по контролю и обслуживанию другому персоналу в организации, но ответственность за обеспечение адекватной защиты ресурса остается за владельцем ресурса. При инвентаризации информационных ресурсов проверяется их хранение по данным реестра и их фактическое наличие в месте, указанном в реестре.

Инструкция по организации технической защиты информации должна содержать сведения о методах и средствах технической защиты информации, применяемых в организации. Инструкция по организации криптографической защиты информации должна содержать сведения о методах и средствах криптографической защиты информации, применяемых в организации.

Порядок работы с информацией, подлежащей защите, включает перечень информационных ресурсов, ненадлежащее обращение с которыми может нанести вред организации, требования к работе с этими информационными ресурсами, ответственность за нарушения и выполнение этих требований, должен включать соглашение (обязательство) о

Перечень нормативно-правовых документов и нормативных документов, регламентирующих деятельность в области обеспечения информационной безопасности:

УзДСт 1047:2003 Информационные технологии. Понятия и определения.

УзДСт 2927:2015 Информационные технологии. Информационная безопасность, термины и определения.

УзДСт 2814:2014 Информационные технологии. Автоматизированные системы.

Классификация по уровню защищенности от несанкционированного доступа к информации

УзДСт 2815:2014 Информационные технологии.

УзДСт ИСО/МЭК 27000:2014 Информационные технологии. Методы безопасности. Системы управления информационной безопасностью. Обзор и глоссарий.

УзДСт ИСО/МЭК 27001:2009 Информационные технологии. Методы безопасности. Системы управления информационной безопасностью. Требования.

УзДСт ИСО/МЭК 27002:2008 Информационные технологии. Методы безопасности. Практика управления информационной безопасностью.

УзДСт ИСО/МЭК 27003:2014 Информационные технологии. Методы безопасности. Руководство по внедрению системы управления информационной безопасностью.

УзДСт ИСО/МЭК 27005:2013 Информационные технологии. Методы безопасности. Управление рисками информационной безопасности.

УзДСт ИСО/МЭК 27007:2015 Информационные технологии. Методы безопасности. Руководство по аудиту систем управления информационной безопасностью.

УзДСт ИСО/МЭК 27008:2015 Информационные технологии. Методы безопасности. Руководство аудитора по средствам контроля информационной безопасности.

УзДСт ИСО/МЭК 27010:2015 Информационные технологии. Методы безопасности. Руководство по управлению информационной безопасностью в сетях и организациях.

УзДСт ИСО/МЭК 27035:2015 Информационные технологии. Методы безопасности. Управление инцидентами информационной безопасности.

УзДСт ИСО/МЭК-1:2008 Информационные технологии. Методы безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

УзДСт ИСО/МЭК-2:2008 Информационные технологии. Методы безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Требования функциональной безопасности.

УзДСт ИСО/МЭК-3:2008 Информационные технологии. Методы безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Требования к обеспечению безопасности.

3.4-§. Геополитика и кибербезопасность

Что касается отношений между национальными государствами, ответ на кибератаку особенно важен и растет. Одним из важнейших пунктов анализа геополитики является возможный ответ на кибератаку и то, как будет принята та или иная мера. Учитывая диапазон ответов, упомянутых ранее, национальные лица, принимающие решения, должны оценить, как отреагируют национальные государства, поэтому геополитика подчеркивает важность понимания как реальных ответов, так и реакций на эти ответы.

Следующие примеры кибератак и действий подчеркивают

важную взаимосвязь между кибербезопасностью и геополитикой:

Пример 1: Некоторые подозревают российское правительство в нападении или поощрении организованной преступности против официальных грузинских веб-сайтов во время военного конфликта 2008 года, который привел к вторжению России в Грузию.

Пример 2: В 2009-2010 годах предполагалось, что Stuxnet, сложный компьютерный червь, созданный правительством, был выпущен для вывода из строя иранских ядерных центрифуг, которые могли использоваться для производства обогащенного урана оружейного качества. Неизвестные источники и спекулянты предположили, что червя могли разработать и распространить правительства США и Израиля.

Пример 3: Министерство обороны США создало структуру киберкомандования, которая формулирует основанные на Интернете оборонительные и наступательные киберстратегии как неотъемлемую часть военного планирования и ведения войны.

Пример 4: В мае 2014 г. пятерым китайским военным чиновникам были предъявлены обвинения в западной Пенсильвании во взломе компьютеров, шпионаже и других преступлениях, направленных против шести жертв из США, включая атомную электростанцию, металлургию и производство солнечных батарей. Обвинение последовало за многолетними разоблачениями того, что китайские военные и другие агенты взламывали компьютеры крупных американских корпораций и медиа-компаний, чтобы украсть коммерческую тайну и узнать, над какими материалами работали журналисты.

Пример 5: В октябре 2014 года было обнаружено, что российские хакеры использовали уязвимость в Microsoft Windows для слежки за НАТО, правительством Украины и западными компаниями.

Пример 6. Известный институт Ponemon сообщил в сентябре 2014 года, что 43% фирм в США в прошлом году столкнулись с утечкой данных. В частности, за последний год усилились сбои в розничной торговле. Одна из самых серьезных утечек была обнаружена в июле 2014 года в JP Morgan Chase & Co., где были скомпрометированы данные 76 миллионов домохозяйств и 7 миллионов малых предприятий. Чиновники администрации Обамы задались вопросом, не является ли нарушение местью путинского

режима в России за события, произошедшие на Украине.

Пример 7: Виды эксплуатации людей, имеющиеся сегодня в качестве доказательств, включают украденные национальные идентификационные номера, украденные пароли и платежную информацию, удаленные онлайн-идентификации и все онлайн-чаты и нажатия клавиш, и даже беспилотные автомобили. Есть шпионские инструменты, которые записывают.

Пример 8. За несколько дней до публикации этого отчета система облачного хранения данных Apple iCloud стала объектом атаки в Китае, направленной на кражу паролей пользователей и слежку за их учетными записями. Некоторые активисты и эксперты по безопасности подозревали, что атаку организовало китайское правительство, возможно, потому, что iPhone 6 был доступен в стране. Другие считали, что атака была недостаточно изощренной, чтобы ее инициировала правительство.

Геополитика относится к отношениям между национальными государствами и их отношениям к более широкому глобальному сообществу, с особым акцентом на отношениях между географией и политикой национального государства:

«Геополитика ставит своей задачей подрыв геополитических дискурсов: продвигать политику географической спецификации политики, а не географию политики в заранее заданных или общих местах. Безопасность и геополитика действуют дуалистически. С одной стороны, дипломатия и внешняя политика С другой стороны, в дискурсе безопасности и геополитики, помимо опоры на специальный язык, большое значение придается общим нарративам о местах и идентичностях. Большинство геополитических дискурсов носят практический, а не формальный характер. основанный на здравом смысле, а не на доказательствах».

В этой теме рассматривается взаимосвязь между кибербезопасностью и геополитикой посредством тематических исследований, иллюстрирующих сложность их взаимосвязи. Анализ касается международного права, особенно самообороны и соразмерности. Принятие решений национальным государством, отражающее предсказуемость и последовательность, значительно укрепляет глобальный порядок. Однако угрозы — реальные или воображаемые — оказывают огромное влияние на региональную и глобальную стабильность. В этом контексте оценка того, как

национальные государства реагируют на конкретные кризисные точки в одностороннем, двустороннем или многостороннем порядке, имеет решающее значение для понимания практических последствий геополитических соображений.

Эффективная геополитика требует столкновения теоретического и практического. Первый требует от национальных лидеров понимания широкого круга вопросов, включая международное право, международные отношения, финансы, географию и военную мощь, особенно ее пределы. Последнее требует реализации этих конкретных дисциплин с учетом как внутренней политики, так и мирового сообщества, признавая важность тактических и стратегических вопросов. Хотя prima facie тактические и стратегические соображения предполагают диссонанс, эффективные национальные лидеры способны включить и то, и другое в свой процесс принятия решений.

Как упоминалось ранее, геополитика — это отношения между национальными государствами и их отношения с более широким глобальным сообществом, с особым акцентом на отношения между географией и политикой национального государства. Ориентация на географию и более широкое глобальное сообщество играет решающую роль в геополитике.

Подумайте о следующем: в 1924 году в Азии произошло разрушительное землетрясение, затронувшее сотни тысяч людей и вызвавшее цунами за тысячи километров. Однако из-за отсутствия информационных систем нет адекватного способа предупредить тех, кто находится на пути цунами, или позвать на помощь пострадавшим от землетрясения.

Теперь рассмотрим 2020 год, быстрее не только информировать других на пути цунами, но и просить других о помощи для пострадавших от землетрясения. Однако просьба об этом не всегда может сработать. Мы живем в мире новостей, и у нас есть постоянная информация. Из-за этого происходит постоянное осознание бесконечных зверств и несправедливостей, которые происходят каждый день в разных уголках мира. Каждый день случается кризис с беженцами, медицинский вирус, физическая катастрофа или техногенная атака.

Таким образом, с геополитикой все более глобализированный мир, в котором мы живем, находится под сильным влиянием

отношений между национальными государствами и их отношений с более широким сообществом. Рассмотрим последствия все более глобализированного мира с точки зрения кибербезопасности.

Как показано в Примере 2, вирус Stuxnet был отправлен, чтобы вывести из строя ядерный потенциал Ирана. Внедрение этого вируса широко освещается на новостных каналах и признается людьми во всем мире. Мало того, чья-либо способность внедрить вирус в ядерный потенциал страны возможна только благодаря инновационным методам, адаптированным киберпространством.

В Иране другие страны, вероятно, узнали о его ядерных возможностях из своих собственных отчетов или, возможно, из записей наблюдения за строящимися или существующими ядерными объектами. Эта технология пришла в виде дронов или другого спутникового наблюдения. Таким образом, во все более глобализированном мире страны были встревожены, узнав, что такая страна, как Иран, обладает такими возможностями.

Кроме того, если бы ввод данных, связанных с ядерным объектом, произошел в 1924 году, можно ли было бы уничтожить или серьезно скомпрометировать ядерные объекты, как это метко сделал вирус Stuxnet? Таким образом, введение данных не только значительно изменило наше представление о геополитике, но и то, как мы взаимодействуем с этими данными, играет еще большую роль.

Тактическое мышление отражает только непосредственно ориентированное принятие решений, тогда как стратегическое мышление отражает глубокое понимание и оценку долгосрочной перспективы, лишенной немедленных результатов и эффектов. Возможно, обстоятельства оправдывают или диктуют узкую точку зрения. Мировое сообщество предусматривает расширение сотрудничества по широкому кругу вопросов, включая финансы, безопасность, пограничный контроль, окружающую среду, здравоохранение и природные ресурсы. Национальные лидеры по понятным причинам в первую очередь делают упор на внутренние соображения; тем не менее, эффективная геополитика предполагает, что национальные интересы значительно усиливаются, когда международные дела учитываются при принятии внутренних решений. Вместе тщательный геополитический анализ национальных государств и корпораций включает в себя отношения

между и наличие обязанности защищать корпорацию в рамках национального государства. Более того, некоторые национальные государства в частности и международное сообщество в целом сталкиваются с дилеммой относительно пределов суверенитета перед лицом реальных или предполагаемых угроз.

Например: Проблемы, возникающие в связи с приверженностью Ирана развитию ядерной программы, вынудили международное сообщество рассмотреть конкретные варианты, касающиеся суверенитета Ирана и ограничений международного вмешательства. Большая часть международного сообщества признает региональные и международные угрозы ядерного Ирана. Тем не менее опасения вооруженного нападения на Иран во многом способствовали введению обширных экономических и дипломатических санкций, эффективность которых остается открытым вопросом.

При определении надлежащего ответа на угрозу ядерного Ирана международное сообщество продемонстрировало дополнительный дискомфорт в связи с военными действиями. Хотя это и понятно, возникает более широкий вопрос: международное сообщество не должно препятствовать реализации Ираном его ядерной программы. То, как национальные лидеры участвуют в процессах принятия решений и решают их, имеет решающее значение для понимания практической реализации геополитики.

Например, в северокорейской кибератаке на Sony заинтересованы три разные страны.

Требуется решить, похожа ли кибератака на акт обычной войны. В обычной войне состояние a атакует физические цели в состоянии b с помощью танков и самолетов, тогда как кибератака — это, прежде всего, атака на частную или общественную инфраструктуру. Последствия атаки могут выходить за рамки физической атаки: возможно, эффект отключения сети или системы не повредит конкретному зданию, даже если люди будут убиты. Таким образом, уязвимость корпораций и их отношение к национальному государству свидетельствует о возросших обязательствах их корпораций перед национальными государствами.

Значительное воздействие кибератак и их уязвимость оправдывают пересмотр основных принципов, включая масштабы и

пределы угроз, самозащиту и ответные действия. Один из наиболее важных вопросов в контексте геополитики заключается в том, оправдывает ли кибератака физический ответ; в случае реструктуризации национальное государство может физически атаковать хакерское государство или лицо, ответственное за кибератаку.

Учитывая слияние геополитики, кибербезопасности и самообороны, кибератака представляет угрозу для отдельных лиц, корпораций и национального государства. Хотя это узаконивает самооборону, вопрос соразмерности. Согласно статье 51 Устава ООН, национальное государство имеет право на самооборону после нападения:

"Ничто в настоящем Уставе не затрагивает права на индивидуальную или коллективную самооборону в случае вооруженного нападения на члена Организации Объединенных Наций до тех пор, пока Совет Безопасности не примет необходимые меры для поддержания международного мира и безопасности. Меры самообороны принятые членами при осуществлении права на это, должны быть немедленно доведены до сведения Совета Безопасности и никоим образом не затрагивают полномочий и обязанностей Совета Безопасности в соответствии с настоящим Регламентом в любое время, которое он может счесть необходимым для сохранения или восстановление международного мира и безопасности».

Когда была основана Организация Объединенных Наций, после Второй мировой войны, у национальных государств в основном не было конфликтов с негосударственными субъектами и террористическими организациями. Однако в последующие десятилетия конфликт перешел от национальных государств к конфликтам национальных государств против национальных государств. Соответственно, важным моментом в расследовании после успешной кибератаки является определение того, является ли ответственная сторона национальным государством или негосударственным субъектом, действующим от своего имени или от имени национального государства.

Есть четыре разных варианта, которые определяют, как и когда государство реагирует на кибератаку.

Вариант 1: действовать от имени негосударственного актора:

если агрессор создает непосредственную или будущую угрозу, то национальное государство может определить это лицо как легальную мишень. Выявление будущей угрозы требует достаточной разведки, чтобы оправдать решение национального государства «задействовать» этого человека.

Вариант 2: Негосударственный субъект-государство, действующий в качестве доверенного лица (канала) от имени нации: подвергшееся нападению государство-государство является законной целью негосударственного субъекта или национального государства, от имени которого была совершена атака. вне со стороны негосударственного актора.

Вариант 3: национальное государство участвует в кибератаке: если национальное государство участвует в кибератаке, это можно рассматривать как акт войны, и в ответ национальное государство должно действовать в соответствии с руководящими принципами ООН.

Вариант 4: национальное государство, выступающее в качестве представителя (проводника) от имени другого национального государства.

С перечисленными выше вариантами полезно применить каждый вариант в реальной ситуации, чтобы понять, как они работают. Вариант 1 предполагает, что негосударственный субъект действует от своего имени. Это происходит, когда корпорация Sony запускает кибератаку против другой страны. Это изменение ролей по сравнению с ситуацией, которую мы обсуждали в Северной Корее или взломе Sony. Тем не менее, важно подумать об этом. Если Sony предпримет кибератаку на Северную Корею, будут ли они считаться законной угрозой, что позволит Северной Корее защищаться в соответствии с Уставом ООН? У Северной Кореи должно быть достаточно интеллекта, чтобы оправдать свое решение задействовать Sony, но если они это сделают, то умрут.

Вариант 2 фокусируется на негосударственном субъекте, выступающем в качестве доверенного лица (канала) от имени национального государства. Например, если Apple будет действовать под руководством правительства США, она получит доступ к телефонам тысяч пользователей в Китае. Согласно Уставу ООН, Китай может нанести ответный удар США, мотивируя это тем, что это самооборона. Китай должен был определить, была ли цель

оправдана Apple или правительством США. Для этого требуется достаточный интеллект, как того требует вариант 1, и дополнительное разрешение, чтобы определить, кто является подходящей законной целью.

Вариант 3 нацелен на фактическое национальное государство, проводящее кибератаку. Этот сценарий кажется самым простым для установления того, что подвергшееся нападению государство может вступить в бой с другим национальным государством под видом самообороны. Если бы реальное национальное государство столкнулось с кибератакой, это, вероятно, было бы расценено как акт войны, и государство, подвергшееся нападению, могло бы действовать в соответствии с директивами ООН.

Последний вариант, Вариант 4, обсуждает парадигму, если национальное государство выступает в качестве представителя или канала для другого национального государства. Например, США начали кибератаку против России, действуя против Украины. Или надо проводить ответный удар по Украине согласно Уставу ООН, потому что США действовали за Украину. Это ставит более сложный вопрос и, как и все варианты, требует достаточного уровня интеллекта, прежде чем прибегать к какой-либо форме самообороны.

Например, если не в сфере кибербезопасности: несколько лет назад теракт в Израиле унес жизни невинных людей; организация, ответственная за нападение, оказалась в Сирии. Хотя ВВС Израиля (IAF) атаковали тренировочные базы террористических организаций в Сирии, израильские официальные лица заявили, что ни Сирия, ни сирийский суверенитет не были намеченной целью. Важным вопросом является вопрос о том, действовала ли террористическая организация сама по себе или в качестве посредника для Сирии или Ирана. Решение атаковать тренировочную базу, по-видимому, обошло более широкий вопрос о возможной роли Сирии или Ирана. Тем не менее,

Суверенитет Сирии был явно нарушен сирийским авиаударом ВВС, и этот аргумент мог бы показаться в лучшем случае ложным.

Напротив, ВВС атаковали объект, имеющий решающее значение для усилий Сирии по развитию своего ядерного потенциала, в то время как первый рейд был нацелен на базы террористов (расположенные в Сирии), а второй был нацелен на

конкретные сирийские цели. Тем не менее обе атаки нарушили суверенитет Сирии; возникает вопрос, оправдывает ли терроризм или контртерроризм нарушение суверенитета национального государства, когда национальное государство не является предполагаемой целью.

Нападение Северной Кореи на Sony: если бы негосударственный субъект (Группа X) осуществил нападение от имени Северной Кореи, Соединенным Штатам пришлось бы решить следующие вопросы при определении того, кто несет ответственность за нападение: Группа X несет ответственность для атаки, и если разведывательное сообщество определило это, может ли оно идентифицировать действующих лиц или они являются законными целями.

Если Соединенные Штаты считают Северную Корею ответственной за нападение на Sony, то решение о нападении на Северную Корею потребует выявления атаки на Sony Pictures, что будет равносильно нападению на Соединенные Штаты. Однако геополитические и военные реалии нападения на группу X отличаются от нападения на Северную Корею. Хотя Sony, несомненно, является важной и важной корпорацией для нападения на ее интеллектуальную собственность, это не равносильно совершению акта физического терроризма против американских гражданских целей. Стоит отметить, что читатель, прочитавший предыдущий проект, не согласен с этим утверждением, и что нападение на корпорацию равносильно нападению на национальное государство, поскольку корпорации необходимы для национальных государств. Кибертерроризм,

Как показывают предыдущие примеры, будь то традиционный терроризм, Северная Корея или Sony, определение законной цели часто является наиболее спорным вопросом. Однако он не только самый спорный, но и самый важный. Чтобы быть отзывчивым и пропорциональным, этот ответ должен быть направлен против законной цели. Давайте рассмотрим следующие примеры, чтобы продолжить обсуждение того, что составляет законную цель.

Учтите следующее: вы часто путешествуете по работе; на этой неделе вы будете сидеть в аэропорту имени Даллеса в Вашингтоне и пользоваться услугами бесплатного трансфера. Это привилегия, которую многие аэропорты внедрили за последние несколько лет, и

многие путешественники не только часто ею пользуются, но и извлекают из нее большую выгоду. Многие путешественники используют это время, чтобы наверстать упущенное по работе, ответить на корреспонденцию или посмотреть последнюю серию своего любимого шоу Netflix.

Тем не менее, многие эксперты говорят, что свободные зоны являются горячими карманами для кибер-хакеров. Говорят, что при бесплатном доступе вы одновременно открываете входную дверь и позволяете кибер-злоумышленникам получить доступ к вашей компьютерной системе. Теперь представьте, что кибер-злоумышленник получает доступ к вашей информации через бесплатную службу в Вашингтонском аэропорту им. Даллеса, используя свой рабочий компьютер в своем офисе.

Законную цель трудно идентифицировать не только из-за предыдущего примера, но и из-за невозможности идентифицировать кибер-злоумышленника. Проверьте следующее. Представьте, что вы стали жертвой кражи личных данных. Как показывают примеры, приведенные далее в книге, это очень распространенная проблема в Соединенных Штатах, где люди крадут чужой номер социального страхования и используют эту информацию для открытия кредитных карт, банковских счетов, получения кредитов и кражи. использовать человека.

Как только это происходит, сложность заключается в компенсации. Представьте, что ваши данные были скомпрометированы в результате кибератаки против цели, популярного универмага. За последние несколько лет Target стал жертвой нарушения кибербезопасности, в результате которого 70 миллионов человек потеряли информацию о своих кредитных картах из-за хакеров.

Реакцией Америки на нападение на Sony стала киберконтратака, атака, которая поразила интернет-инфраструктуру Северной Кореи дважды в течение как минимум двух дней, согласно надежным источникам. Таким образом, ответом на кибератаку является не физическое преследование лица, ответственного за первоначальную атаку, а киберконтратака. Эта модель имеет важные геополитические последствия, поскольку она освещает различия между обычным оперативным реагированием на терроризм и кибер-самообороной по сравнению с обычной самообороной.

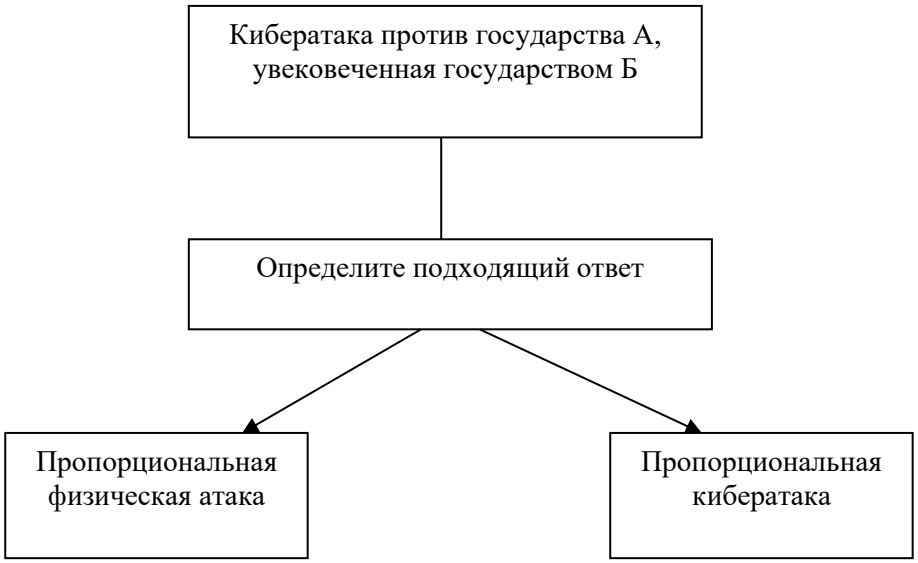


Рисунок 3.1. Варианты ответа

Противодействие кибертерроризму направлено не на лицо, ответственное за террористическую атаку, а на инфраструктуру атакующей организации или государства.

Если целью является корпорация, то атака на интернет-инфраструктуру национального государства несоразмерна; такая контратака может серьезно повлиять на больницы, системы водоснабжения и виды транспорта. В контексте геополитики такая контратака опасно повышает ставки. В контексте международного права это предполагает несоразмерный ответ. Тем не менее, национальное государство имеет право и обязанность реагировать: вопрос в том, каковы допустимые пределы реагирования на кибератаку. Очерки геополитики и международного права показывают, что процессу принятия решений присущи стратегические и юридические ограничения.

Отражая деликатность более широких геополитических соображений, есть три возможных ответа: прямая атака на цели Северной Кореи, которая нанесет значительный ущерб инфраструктуре, сообщение с ограниченным ущербом инфраструктуры или прямая атака на Северную Корею — неправда, но атака на Дочерняя компания или канал в Северной Корее.

Прямые удары по целям в Северной Корее, наносящие огромный ущерб инфраструктуре. В этом сценарии США запускают кибератаку на ключевую инфраструктуру Северной Кореи. Сюда могут входить электрические сети, системы водоснабжения, средства управления транспортными средствами (будь то самолеты

или автомобили) и ряд других опций, которые сильно влияют на повседневную жизнь жителей Северной Кореи. Таким образом, эффект более значителен, чем ограниченная физическая контратака, направленная на конкретных лиц.

Отвлекает от контратаки на Северную Корею и фокусируется на контратаке на филиал или канал Северной Кореи. В этом сценарии Соединенные Штаты действуют от имени Sony. В общем, Северная Корея не пришла после США, вместо этого они пришли после Sony. Таким образом, США будут действовать от имени Sony в ответ на такие действия. Следовательно, третий вариант предполагает, что Соединенные Штаты будут преследовать аналогичную северокорейскую дочернюю компанию или канал, например Sony. Это вызывает те же вопросы, что и второй вариант. В общем, этот вариант создает ряд опций, которые трудно упорядочить.

СТАКСНЕТ

Согласно достоверным источникам, иранский ядерный объект был атакован очень сложным компьютерным вирусом под названием Stuxnet. Большинство экспертов говорят, что вирус был завезен Израилем или США.

Зарождающаяся атомная промышленность Ирана требует, чтобы Америка и Израиль определили, представляет ли она угрозу для всего мира. На момент написания этой статьи ведутся сложные переговоры о ядерном потенциале Ирана. Переговоры, вне зависимости от их исхода, не решат вопросы международного права и геополитики, связанные с оперативным реагированием на иранскую угрозу. На протяжении многих лет лидеры Ирана неоднократно угрожали напасть на Израиль с применением ядерного оружия.

Премьер-министр Нетаньяху ясно предупредил, что Израиль, не колеблясь, заранее успокоит мировых лидеров и что переговоры об ограничении ядерного потенциала Ирана имеют решающее значение. Согласно международному праву, основанием предупреждения Нетаньяху было право Израиля на самооборону. Хотя Нетаньяху сослался на статью 51, основа для переговоров отражает обеспокоенность тем, что угрозы и предупреждения будут иметь реальный эффект и, таким образом, окажут значительное влияние непосредственно на регион и международное сообщество в

целом.

Эффективная геополитика демонстрирует важность сдерживания угрозы в контексте кризисного управления и ликвидации последствий. Однако, хотя региональная стабильность имеет первостепенное значение, главная ответственность национального руководства заключается в обеспечении безопасности и благополучия своего гражданского населения. Следовательно, существует естественное противоречие между национальной безопасностью, определяемой и реализуемой отдельными государствами, и более широкими региональными и международными интересами, выходящими за рамки конкретного национального государства. Кибер значительно освещает это напряжение:

«Хотя вопрос кибербезопасности имеет большое значение в американо-китайских отношениях, шаги по его решению остаются примитивными по своему характеру. 13 апреля 2013 года госсекретарь США Джон Керри заявил, что стороны договорились о создании рабочей группы по Неделю спустя председатель Объединенного комитета начальников штабов США генерал Мартин Демпси созвал совместную конференцию с китайским генералом Фан Фэнхуэй, который пообещал сотрудничать с США, поскольку последствия крупной кибератаки могут быть такими же серьезными, как ядерная Генерал Фанг, начальник штаба Народно-освободительной армии и член Центральной военной комиссии, выразил готовность создать механизм кибербезопасности, предупредив, что прогресс может быть не быстрым.

Интервью с ведущими экспертами проливают свет на изощренность и изощренность Stuxnet. Однако технические аспекты компьютерного вируса находятся вне нашего контроля; представляет интерес природа киберконфликта. В этом контексте, в то время как впечатляющая технология Stuxnet привлекла значительное внимание, более широкое исследование было сосредоточено на ее происхождении и последствиях. В связи с этим решение начальника штаба Армии обороны Израиля (ЦАХАЛ) подполковника В. Генерал Гади Эйзенкот отражает угрозы и опасности кибервойны и терроризма для создания киберотделения. Эта ветвь сочетает в себе оборонительные и наступательные возможности, что отражает резко возросшее стратегическое

значение безопасности кибервойны и терроризма.

Сочетание возможностей нападения и защиты предполагает, что в контексте принципа соразмерности международного права атака на компьютерную систему национального государства является законной формой самообороны, если цель представляет угрозу для жизни. Предупреждение: воздействие компьютерного вируса и других дополнительных мер направлено на цель, вызывающую предполагаемую угрозу. В случае Ирана внедрение компьютерного вируса отражает пропорциональность, если мера самообороны связана с ядерной промышленностью, которая может быть использована в наступательных и агрессивных целях.

«Помещение кибератаки в контекст принятия военных решений (и предположение, что государственные и негосударственные субъекты в целом имеют схожие процессы военного планирования) имеет последствия для использования кибератак. После Stuxnet страны будут использовать кибератаку, которая вызывает физический ущерб Соединенным Штатам или их союзникам, скорее всего, не начнут, и они не перестанут использовать кибертехнологии для шпионажа и политического принуждения. шпионажа и преступности) против США и их союзников, мы не видели никаких физически опасных атак, потому что они оценили риск насильственного ответа слишком высоко.Это та же самая причина, которая удерживает их от запуска самолетов или ракет против США, но международная практика и закон не оправдывают применение силы в ответ на шпионаж и преступления, что делает риск насильственного ответа небольшим и приемлемым.

К чести разработчиков Stuxnet, он был тщательно написан, чтобы избежать побочного ущерба. Другие злоумышленники могут быть не столь осторожны, но это не имеет никакого отношения к проникновению в код Stuxnet. Потенциальные противники по-прежнему проводят те же расчеты выгоды и риска при принятии решения о применении силы против США, и их удерживает военный ответ США с использованием всех военных средств, а не только кибератаки. Теперь они могут ссылаться на stuxnet как на часть оправдания любой массовой атаки, но это будет оправданием, а не частью их решения. Страны больше не будут проводить кибератаки против США или их союзников после Stuxnet.

Хотя степень участия США в Stuxnet неясна, более широкая

картина национальной безопасности США предполагает, что развитие Ираном ядерной державы затронет жизненно важные интересы Америки. Прямо и, возможно, резко, национальные лидеры Израиля постоянно заявляют, что ядерный Иран представляет собой экзистенциальную угрозу безопасности Израиля. Несмотря на то, что это открытый вопрос, который является предметом интенсивных дебатов и различных мнений, введение Stuxnet ясно иллюстрирует оперативные последствия взаимосвязи между киберпространством, геополитикой и самообороной.

Предупреждение подчеркивает предполагаемую угрозу. Тогда возникает дополнительный вопрос: как определить предполагаемую угрозу? Есть много вещей, которые могут быть восприняты как угроза, но если страны будут реагировать на что-либо, что может быть воспринято как угроза, у них закончатся время и деньги.

Можно убедиться, что компьютерный вирус действительно является предполагаемой угрозой. Также возникает вопрос, есть ли у кого-то доступ к технологиям и данным, необходимым для ввода и запуска компьютерного вируса, который может обнаруживать угрозу и фактически улучшать указанную угрозу? Мы живем в технологическом мире, который постоянно адаптируется и развивается, и чтобы оставаться на вершине этого, нужны усердие и деньги. Часто число тех, кто способен выполнить требуемый компьютерный вирус или метод, сужено до нескольких человек.

Контрольные вопросы.

1. Как федеральное правительство США устанавливает политику кибербезопасности?
2. Насколько важен Конгресс в формировании политики кибербезопасности?
3. Как интернет-преступность влияет на кибербезопасность?
4. Когда и где проходила Конвенция о международной информационной безопасности?
5. Каковы основные угрозы в сфере международной информационной безопасности?
6. Каковы основные принципы международной информационной безопасности?
7. Каковы важные принципы среди стран-участниц в области международной информационной безопасности?

8. Какие основные факторы учитывают страны-участницы при обеспечении международной информационной безопасности?

9. Какие меры принимаются для предотвращения атак и «информационной войны» в сфере международной информационной безопасности?

10. Каковы шаги и реформы Российской Федерации в области государственной политики международной информационной безопасности?

11. Какие шаги необходимо предпринять для создания политики кибербезопасности?

12. Что будет установлено в результате аудита, проведенного в процессе создания политики кибербезопасности?

13. Как разрабатывается политика в процессе создания политики кибербезопасности?

14. Что необходимо для координации и реализации политики в процессе создания политики кибербезопасности?

15. Когда необходимо обновление политики в процессе создания политики кибербезопасности?

16. Какие проверки проводятся в процессе создания политики кибербезопасности?

17. Как проводятся внутренние и внешние аудиты в процессе создания политики кибербезопасности?

18. Каковы этапы процесса выпуска политики информационной безопасности?

19. Какие есть примеры кибербезопасности и геополитики?

20. Какие переменные важны для оценки связи между кибербезопасностью и геополитикой?

21. Как национальные государства должны реагировать на взаимосвязь между кибербезопасностью и геополитикой?

22. Какие процессы должны быть реализованы в отношениях между кибербезопасностью и геополитикой?

ГЛАВА IV. ПРИМЕНЕНИЕ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ

4.1-§. Внедрение и разработка политики кибербезопасности

Несмотря на широко распространенную практику формулирования и использования политик информационной безопасности, а также выделение организациями значительных ресурсов для управления информационной безопасностью, разработка эффективной и целенаправленной политики безопасности остается сложной задачей. Например, политики могут быть выпущены, но не пересмотрены для включения новых нормативных требований или изменений в бизнес-процессы, что приводит к игнорированию юридических обязательств и устаревших политик. Основная цель этой темы — предоставить дорожную карту для разработки политики информационной безопасности, обеспечивающей устойчивость. В этой теме рассматривается современная литература по методам разработки политики и сравниваются различные подходы. По результатам сравнения, Предлагается жизненный цикл разработки политики информационной безопасности (ISP-DLC). Рекомендуемый подход к жизненному циклу гарантирует, что политика безопасности организации является всеобъемлющей, эффективной и устойчивой.

Сегодня организации всех форм и размеров должны с готовностью осваивать информационные системы и технологии, если они хотят выжить и процветать в условиях растущей конкуренции. Следовательно, важно внедрить меры безопасности, чтобы гарантировать целостность, конфиденциальность и доступность информации, введенной в информационные системы организации..

Чтобы организация имела правильный подход к защите своих информационных активов, ей необходима хорошо спланированная и эффективная политика информационной безопасности. Политика может быть определена как «образ действия, принцип или процедура, которые считаются подходящими» или «страховой полис». Используя это определение, в нем говорится, что политика относится, во-первых, к действию, которое необходимо предпринять, или к процедуре, которой необходимо следовать, а во-вторых, к заявлению или заявлению, которое может быть сделано.

Поэтому, если процедура выполнена правильно, то «страховое свидетельство» должно быть целым, только тогда организация сможет достичь своих целей и задач.

Внедрение эффективной политики безопасности особенно важно в сфере управления информационной безопасностью. Мораль заключается в том, что каким бы сильным ни был технический контроль, безопасность всегда зависит от людей внутри организации. Людей часто называют самым слабым звеном в программе информационной безопасности. Однако часто упускается из виду, что если нарушение информационной безопасности или инцидент вызваны действиями неосведомленного или небрежного сотрудника, совет директоров и высшее руководство могут быть привлечены к личной ответственности за действия этого сотрудника. Поэтому нельзя пренебрегать человеческим фактором. Чтобы организация имела адекватные меры безопасности, ей нужны документированные политики, регулирующие действия ее сотрудников.

В академическом и практическом сообществе растет консенсус в отношении того, что политики информационной безопасности являются основой для распространения и применения надежных методов обеспечения безопасности в организационном контексте. Как они заявляют: По крайней мере среди профессиональных специалистов по безопасности признано, что формальные политики являются необходимым условием безопасности.

В этом разделе рассматривается важность наличия эффективной политики информационной безопасности и потенциальные проблемы реализации таких политик. Сравниваются пять подходов или методов разработки политики информационной безопасности. Результаты сравнения включены в подход «Жизненный цикл разработки политики информационной безопасности» (ISP-DLC). Целью разработки ISP-DLC является предоставление инструментов, обеспечивающих соответствие политик информационной безопасности текущим и меняющимся потребностям организации и бизнес-целям, а также их соответствие политикам. Это приводит к действительно комплексной, эффективной и устойчивой политике информационной безопасности..

Важность наличия эффективной политики информационной безопасности. Политика информационной безопасности определяет, что необходимо сделать для защиты данных организации. Наличие политик качества для решения вопросов, связанных с рисками, может расширить возможности с точки зрения повышения общей безопасности организации, а также может быть полезным с юридической точки зрения, если политики критически пересматриваются. Политика информационной безопасности должна определять полную политику защиты информации организации. Обычно он состоит из заявления о политике высокого уровня и дополнительных подробных документов о политике. Политика должна включать все меры, необходимые организации для соблюдения законодательных и нормативных требований.

Важность документов политики безопасности заключается в том, что в случае возникновения инцидента информационной безопасности, ставящего под сомнение проведение операции, она вступит в силу, то есть покажет реальную операцию.

Кроме того, даже если у компании нет обязательств по разработке и внедрению политики информационной безопасности, добровольно разработанная политика выгодна для организации по следующим причинам:

(i) Политика информационной безопасности побуждает организацию находить наилучший способ ведения бизнеса, защищая при этом ценность, подлинность, конфиденциальность и целостность своих информационных активов;

(ii) Эксперты говорят, что в эпоху, когда интернет-законодательство все еще очень запутанно, предприятия с политикой информационной безопасности могут защитить себя от ненужной головной боли.

Компании, которые признают международно признанные стандарты и имеют эффективную политику информационной безопасности в соответствии с ними, имеют явное преимущество перед компаниями, придерживающимися противоположного подхода. Компании, у которых нет политики информационной безопасности или у которых есть такая политика, но политика не реализуется эффективно, могут стать жертвами атак со стороны хакеров, взломщиков и других агентов угроз. В конечном итоге это

приводит к потере доверия клиентов и стоимости активов.

После рассмотрения того, зачем нужна политика информационной безопасности, становится ясно, что компании (особенно советы директоров) можно назвать небрежными, небрежными и безответственными, если они позволяют компании работать без эффективной политики информационной безопасности. Кроме того, из предыдущего обсуждения должно быть ясно, что важной причиной наличия такой политики является помощь директорам и высшему руководству в представлении в суде четких доказательств того, что они выполнили свои обязанности с должным вниманием и усердием. Управляя ценной информацией и защищая конфиденциальность, целостность и удобство использования своих информационных активов, организации не только выполняют свои юридические и нормативные требования,

Проблемы в реализации эффективной политики информационной безопасности. В существующей литературе особое внимание уделяется основам разработки политики информационной безопасности. Однако неясно, насколько хорошо реализованы методы, описанные в литературе. Исследования показали, что компании с такой политикой не уделяют должного внимания сопровождению и соблюдению политик. Таким образом, во многих организациях политика безопасности оказывается на полке, потому что у нее нет непрерывного жизненного цикла.

Руководствуясь проблемами, с которыми они сталкиваются при разработке политик безопасности, авторы часто обращаются к политикам других организаций, коммерчески доступным ресурсам или шаблонам, доступным в общедоступных источниках, таких как Интернет, для получения ответов на свои вопросы. Часто необходимость следовать этому подходу связана с отсутствием навыков и понимания. Однако итоговый документ не содержит адекватных рекомендаций по информационной безопасности в контексте организации, которую он должен защищать.

Разработка эффективной политики безопасности может быть трудоемкой и сложной задачей; поэтому авторы пытаются решить такие вопросы, как то, что должно быть включено в этот важный документ, чтобы гарантировать, что организации соответствуют законодательным и нормативным требованиям, и в то же время обеспечить передовой опыт в области управления

информационной безопасностью. Важно отметить, что формулирование политики — это только начало процесса. Техническое обслуживание и мониторинг соответствия более важны, чем этот начальный шаг, и обычно появляются как дополнительные проблемы в процессе. Политика должна поддерживать и улучшать бизнес-цели организации. Поэтому формирование политики информационной безопасности,

Современные методы разработки политики безопасности.Обзор существующих источников раскрывает ряд подходов или методов, которые организации могут использовать для разработки собственных политик безопасности. Эти подходы представлены в табличном формате (Таблица 1), в котором предпринимается попытка сгруппировать шаги, предложенные каждым источником, в категории, являющиеся частью аналогичного процесса. Например, этапы группы 1 обычно связаны с процессом оценки рисков, который предшествует разработке политики. Группа 2 посвящена шагам, необходимым для построения политики, например составлению политики. Группа 3 фокусируется на этапе реализации политики, а группа 4 — на мониторинге и обслуживании политики. Группа 5 выделяет ключевые роли для руководства, Группа 6 следует тому же процессу для сотрудников в целом. Обратите внимание, что нумерация шагов, предложенная конкретным источником, сохраняется, даже если шаги не перечислены последовательно в таблице из-за требования классифицировать шаги в определенной группе.

Сравнение выявляет некоторое сходство там, где авторы согласны с одними и теми же шагами, а также выявляет пробелы, когда конкретный автор не упоминает шаг, который другие считают важным. Например, в DTI (1999 г.) не упоминаются действия, необходимые в рамках группы по оценке рисков, в то время как CTRG (1998 г.) считает, что оценка рисков является ключевым шагом перед принятием каких-либо мер по выработке политики..

Таблица 4.1

Методы разработки политики информационной безопасности

Автор	Контрал данные (2000)	Вычислитьр Технологии Исследовать ч Группа КТРГ (1998)	ДТя (1999)	САНС Институт (2007)	Вудворд (2000)
Группа 1 **Этапы оценки риска**	1. Выявление возможных угроз и рисков	1. Определите, какие активы нуждаются в защите			1. Исследова ние риска
	2. Идентифика ция защищенны х активов	2. Определите уровень защиты для каждого актива			
		3. Определени е использован			
		4. Выявление существую			
		5. Выявленные угрозы научиться решать			

		6. Проведите оценку воздействия			
Группа 2 Построение полиса этапы		7. Составление политики безопасности	1. Изучите содержание политики	1. Написание политики	2. Формулировка политики
		9. Добавить раздел восстановления в политику	2. Разработка политического проекта		
Группа 3 Реализация политики этапы	3. Использование стратегии защиты активов	8. Разработка плана реализации	3. Предоставьте образцы политик	2. Публикация Политики	3. Разработка стандартов реализации политики
		10. Обучение пользователей			

Группа 4 Этапы мониторинга и обслуживания политики	4. Тестирование политики для обеспечения уверенности		4. Мониторинг и обслуживание	3. Запросить пересмотр политики	5. Обзор
Группа 5 Стадии принятия и одобрения со стороны руководства			5. Получите одобрение руководства		4. Получите сотрудничество от руководства
Группа 6 Шаги поддержки и сотрудни		11. Реагирование на инцидент			

Как видно из таблицы выше, авторы предлагают основные этапы разработки документа политики безопасности. Информация, полученная в результате анализа, представленного в таблице 1 выше, обобщается и дополняется, чтобы предложить комплексный подход к жизненному циклу разработки политики информационной безопасности, как показано на рисунке 1. Для достижения этой цели группы делятся на категории. Шаги, перечисленные в таблице 1, предприняты для организации этапов разработки предлагаемого жизненного цикла разработки политики информационной безопасности (ISP-DLC). Например, группа 1 (оценка риска) становится шагом 1 ISP-DLC. То же самое относится и к группам 2-

4, которые стали этапами 2-4 ISP-DLC. Главы 5 и 6, описывающие роль руководства и персонала в целом, считаются применимыми к каждому из этапов ISP-DLC. Каждый из шагов требует руководства со стороны руководства и поддержки со стороны сотрудников. Таким образом, захват и утверждение руководством, а также поддержка персонала описываются как горизонтальные линии, охватывающие все четыре этапа ISP-DLC. Предлагаемый жизненный цикл разработки политики информационной безопасности затем служит дорожной картой для организаций, которым следует следовать, чтобы обеспечить всеобъемлющую, эффективную и устойчивую политику информационной безопасности. Подробнее ISP-DLC будет рассмотрено позже. захват и утверждение руководством, а также поддержка персонала изображены в виде горизонтальных линий, охватывающих все четыре этапа ISP-DLC. Предлагаемый жизненный цикл разработки политики информационной безопасности затем служит дорожной картой для организаций, которым следует следовать, чтобы обеспечить всеобъемлющую, эффективную и устойчивую политику информационной безопасности. Подробнее ISP-DLC будет рассмотрено позже. захват и утверждение руководством, а также поддержка персонала изображены в виде горизонтальных линий, охватывающих все четыре этапа ISP-DLC. Предлагаемый жизненный цикл разработки политики информационной безопасности затем служит дорожной картой для организаций, которым следует следовать, чтобы обеспечить всеобъемлющую, эффективную и устойчивую политику информационной безопасности. Подробнее ISP-DLC будет рассмотрено позже. служит дорожной картой для организаций, которой следует следовать, чтобы обеспечить эффективную и устойчивую политику информационной безопасности. Подробнее ISP-DLC будет рассмотрено позже. служит дорожной картой для организаций, которой следует следовать, чтобы обеспечить эффективную и устойчивую политику информационной безопасности. Подробнее ISP-DLC будет рассмотрено позже.

Подход к жизненному циклу разработки политики кибербезопасности (CSDP).Предлагаемый ISP-DLC состоит из четырех основных этапов: оценка рисков, построение политики, реализация политики, мониторинг политики и обслуживание.

Каждую стадию можно разбить на этапы, где действия, происходящие на каждом этапе, подробно описаны, что будет кратко рассмотрено далее. Важно помнить, что разработка политики является повторяющимся и непрерывным процессом. Из-за изменений в технологии, бизнес-среде и требованиях соблюдения законодательства фаза реализации политики всегда сопровождается фазой обслуживания, которая включает эти изменения, и фазой мониторинга, которая обеспечивает операционную реализацию директив политики (т. е. соответствие политике) продолжается с .

Рисунок 4.1. Жизненный цикл разработки политики информационной безопасности

Участие и одобрение руководства показаны в верхней части диаграммы ISP-DLC и охватывают все этапы как критически важные компоненты успешного жизненного цикла разработки политики. Высшее руководство в конечном итоге несет ответственность за благополучие организации. Они обычно используют политику, чтобы определить свою поддержку и направление со стороны руководства. Если руководство не поддерживает политики безопасности, их может вообще не быть. Эта политика должна быть доведена до сведения всех сотрудников. Необходимость сотрудничества персонала включена в диаграмму ISP-DLC как горизонтальная линия, охватывающая весь жизненный

цикл разработки политики. Сотрудники должны знать, что они должны и не должны делать как отдельные лица, чтобы обеспечить надлежащий уровень безопасности. Поэтому стратегия коммуникации между менеджерами и сотрудниками необходима на протяжении всего жизненного цикла разработки политики.

Роль руководства и персонала подробно обсуждается в разделах 5.1–5.4 с выделением конкретных вопросов, относящихся к конкретным этапам, обсуждаемых в качестве подкомпонентов каждого ключевого этапа. **5.1. Шаг 1: Оценка риска**. На этапе оценки рисков определяются бизнес-активы, которые организация хочет защитить, и рассматриваются потенциальные угрозы для этих активов, задавая следующие вопросы:

- Что защищать? (например, активы)
- От чего или от кого следует защищать активы? (например, угрозы и уязвимости)
- Сколько организация готова потратить, чтобы получить адекватную защиту?
- Каковы затраты и выгоды для бизнеса?

Этап состоит из четырех подэтапов: идентификация активов, выявление уязвимостей и угроз, обобщение результатов оценки рисков и оценка возможных мер и средств контроля. Эти подэтапы следует выполнять последовательно, а результат использовать для принятия решения о том, что следует включить в политику безопасности, чтобы гарантировать снижение выявленных рисков.

Этап 1: Участие руководства и поддержка сотрудников.На основании результатов оценки риска руководство должно оценить затраты и выгоды от внедрения рекомендуемых средств контроля для снижения риска до приемлемого уровня. Если ожидаемые затраты укладываются в бюджет, можно начинать следующий этап построения политики. В противном случае стратегии снижения риска должны быть пересмотрены или заложены в бюджет, чтобы оставаться в рамках бюджета. На данном этапе жизненного цикла разработки политики вовлечение руководства является ключевым требованием, в то время как в целом персонал привлекается только с точки зрения оценки рисков..

Фаза 2: Разработка политики. На этом этапе разрабатывается политика безопасности на основе выводов и рекомендаций по снижению рисков, создаваемых угрозами и уязвимостями,

согласованных на этапе оценки рисков. На этом этапе также рассматриваются бизнес-стратегии и цели, а также юридические требования в процессе создания политики. Этап состоит из следующих подэтапов: разработка одностраничного заявления о политике и описания требований безопасности высокого уровня, проверка и утверждение заявления о политике высокого уровня, разработка подробных документов политики, проверка и утверждение подробных заявлений политики, проверка безопасности. публикация политик.

Процесс написания политики информационной безопасности включает в себя выбор соответствующих целей управления, которые должны быть достигнуты. Цель контроля определяется как формулировка желаемого результата или цели, которая должна быть достигнута путем реализации контрольных процедур в конкретном процессе. Цель управления также может рассматриваться как передовой опыт информационной безопасности, реализуемый посредством использования соответствующих средств управления безопасностью. Будет создано одностраничное заявление о политике и план требований к безопасности высокого уровня, отвечающие требованиям выбранных целей контроля. Этот план обеспечивает отправную точку для создания идеальной политики информационной безопасности, отражающей интересы организации на высшем уровне. Проект будет представлен исполнительному и высшему руководству для рассмотрения и утверждения политического заявления высокого уровня. В случае одобрения подробный проект документа о политике, основанный на политическом заявлении высокого уровня, снова будет представлен руководству на утверждение; и в случае одобрения политика безопасности готова к печати.

В дополнение к неотъемлемой роли руководства в рассмотрении и утверждении проектов политик и окончательных документов по политике безопасности, их четкая приверженность политике и ее поддержка необходимы для обеспечения того, чтобы политика была должным образом доведена до сведения сотрудников. Чтобы подготовить организацию к будущим изменениям и позволить отдельным лицам влиять на формулирование новой политики, следует инициировать план

коммуникации, который позволяет получать обратную связь от аудитории на этапе формулировки политики. Взаимодействие имеет решающее значение для перехода пользователей от подготовки к принятию обязательства и, в конечном итоге, к этапу принятия обязательства.

Кроме того, новая или обновленная политика безопасности неизбежно что-то изменит в том, как кто-то работает, а такие изменения, какими бы незначительными они ни были, требуют внимания. Влияние изменения должно быть оценено, чтобы обеспечить его успешное внедрение. Поэтому важно понимать текущую среду. Например, эти вопросы следует задать на этапе разработки политики, чтобы оценить способность сотрудников успешно поддерживать новую политику безопасности:

- Кто пострадал?
- Понимает ли окружающая среда организации важность безопасности?
- Насколько организационная среда требует внедрения компонентов новой политики и ключевых вопросов ее реализации?
- Что ожидается, когда новая политика будет реализована?

Вышеупомянутые аспекты следует учитывать на этапе реализации политики, чтобы гарантировать, что сотрудники принимают и поддерживают новые политики..

Шаг 3: Реализация политики. После завершения построения политики пришло время реализовать новый документ политики безопасности. Теперь для воплощения проекта в жизнь требуется подробный план реализации. Этот этап включает следующие подэтапы: определение требований безопасности и контроля с помощью подробных процедур и инструкций, распределение обязанностей по информационной безопасности, тестирование требований безопасности и контроля, внедрение требований безопасности и контроля, внедрение политики безопасности, постоянное обучение и повышение осведомленности.

Общение со старшими членами организации увеличивает вероятность того, что политика безопасности будет принята всей организацией, и помогает мотивировать людей на этапах принятия обязательств. Утвержденная окончательная копия политики безопасности должна быть доступна всем сотрудникам. Она должна

быть официально доведена до сведения всех пользователей, и пользователи должны подтвердить, что они прочитали и поняли политику, подписав ее и согласившись соблюдать ее. Следующим требованием будет разработка программ повышения осведомленности и обучения безопасности для новой политики. Эти программы являются очень важными шагами на этапе реализации политики,.

Шаг 4: Мониторинг и обслуживание политик. Этот этап состоит из двух основных видов деятельности, а именно. мониторинг и техническое обслуживание.

Мониторинг политики.После внедрения политики информационной безопасности организациям следует включить соответствующие механизмы мониторинга для определения повседневной деятельности организации, обеспечивающей соблюдение политики безопасности во всей организации. Должны быть выполнены следующие подэтапы: получение измеримых результатов, отражающих поведение пользователей, проведение системных аудитов и инспекций, проведение тестов на обнаружение вторжений и проникновение, анализ аудитов действий пользователей, аудит соответствия политике. Основная цель мониторинга политики — убедиться, что сотрудники соблюдают новые требования политики. Таким образом, предлагаемый ISP-DLC демонстрирует необходимость соблюдения требований политики для обеспечения согласованности политики безопасности.

Политика обслуживания.Это действие включает в себя следующие подэтапы: Анализ отчетов об инцидентах безопасности. Анализ безопасности и технологической инфраструктуры. Анализ бизнес-стратегий. Анализ тенденций и непредвиденных обстоятельств. Юридическая проверка требований, создание запроса на изменение политики и повторение жизненного цикла разработки политики.

Важно постоянно проверять инфраструктуру безопасности организации для выявления новых угроз. Это может быть связано с изменениями в технологии, используемой в других подразделениях организации. Кроме того, могут быть введены новые законы, которые должны быть включены в политику безопасности организации. Суть в том, что изменения различного характера могут привести к устареванию политик информационной безопасности.

Эти изменения должны быть включены в политики на этапе обслуживания. На этапе обслуживания необходимо повторить шаги 1–3 жизненного цикла, чтобы убедиться, что изменения политики не применяются случайно. Конечно, есть много неизвестных, и на данном этапе организации, скорее всего, столкнутся с новой угрозой, которую не рассматривали..

На этом этапе руководство должно обеспечить наличие адекватных процедур и систем, чтобы определить, понимают ли сотрудники применяемые политики и процедуры и соблюдаются ли политики и процедуры. Кроме того, руководство должно обеспечить соответствующие последствия несоблюдения требований политики безопасности. Наказания должны применяться последовательно и доводиться до сведения всех сотрудников..

Короче говоря, разработка политики безопасности выходит за рамки простого написания и реализации политики. Если организации четко не осознают различные шаги, необходимые для разработки политики безопасности, они могут в конечном итоге разработать политики, которые будут непродуманными, неполными, избыточными, не полностью поддерживаемыми пользователями, избыточными или неактуальными, и столкнутся с риском выхода. Политика безопасности имеет полный жизненный цикл, который необходимо пройти в течение своего существования. Цель этого раздела — предложить жизненный цикл разработки политики информационной безопасности, обеспечивающий всеобъемлющую и устойчивую политику информационной безопасности.

Организации не могут разработать всеобъемлющую политику безопасности одним махом, но на протяжении всего жизненного цикла разработки политики безопасности следует придерживаться хорошо спланированного непрерывного процесса. Создание политики информационной безопасности — это не разовое мероприятие, оно требует постоянной приверженности обеспечению того, чтобы политики приносили пользу. Это может быть достигнуто с помощью предлагаемого подхода к жизненному циклу. Использование комплексного жизненного цикла политики безопасности, описанного здесь, обеспечивает структуру, помогающую организациям гарантировать последовательное выполнение шагов, необходимых для разработки политики

безопасности, на протяжении всего жизненного цикла политики и соблюдение политик. Таким образом, политика сама по себе является не единственным артефактом процесса развития,

§ 4.2. Корпоративные ответы на киберпреступность

Понятие киберпреступности в корпорациях.Крупные и мелкие хакеры регулярно атакуют корпорации. Некоторые атаки настолько масштабны, что скомпрометированы миллионы клиентов. Вот почему подход корпораций к кибербезопасности так важен.

Реальность такова, что значительные ресурсы тратятся на защиту клиентов и активов, но корпорации ежедневно подвергаются атакам, краткосрочным или долгосрочным, со значительными последствиями и серьезными последствиями. Поэтому нападение на корпорацию следует рассматривать как нападение на национальное государство.

Предположительно, эта неудача не связана с неспособностью руководителей корпораций осознать существование явного риска. Однако это свидетельствует об отсутствии желания понимать риск. С практической точки зрения понимание в первом случае требует просто чтения газет, во втором — финансовых затрат, выделения ресурсов и конкретных мер, необходимых широкой общественности для предотвращения уязвимости. Все это может показаться тривиальным руководителям. Такой подход является недальновидным и обреченным на провал. Это негативно влияет на клиентов и инвесторов, обременяет правоохранительные органы, влияет на другие корпорации и общественность в целом. Наиболее тревожным и важным является то, что это подпитывает энтузиазм кибер-злоумышленников.

Некомпетентность — это неспособность предотвратить атаки, игнорировать предполагаемые уязвимости и угрозы. В таких случаях следует использовать артикуляцию. Артикуляция означает не страх, а скорее готовность признать и сказать правду, более эффективную политику информирования общественности, непосредственных заинтересованных лиц о реальных и потенциальных атаках.

Еще один эффективный подход — сотрудничество. Это означает распознавание угрозы, отражение принятия мер по минимизации угрозы, при этом не отрицая возможности нападения и уменьшения его возможных последствий. Это также создает среду, в которой клиент становится партнером в контексте

противодействия кибертерроризму, поскольку к клиенту относятся как к важному лицу.

Концепция заказчика как партнера в борьбе с кибертерроризмом создает треугольные отношения между корпорацией и покупателем/клиентом, которые более эффективны, чем правоохранительные органы, излишне минимизирующие угрозу (рис. 4.2).

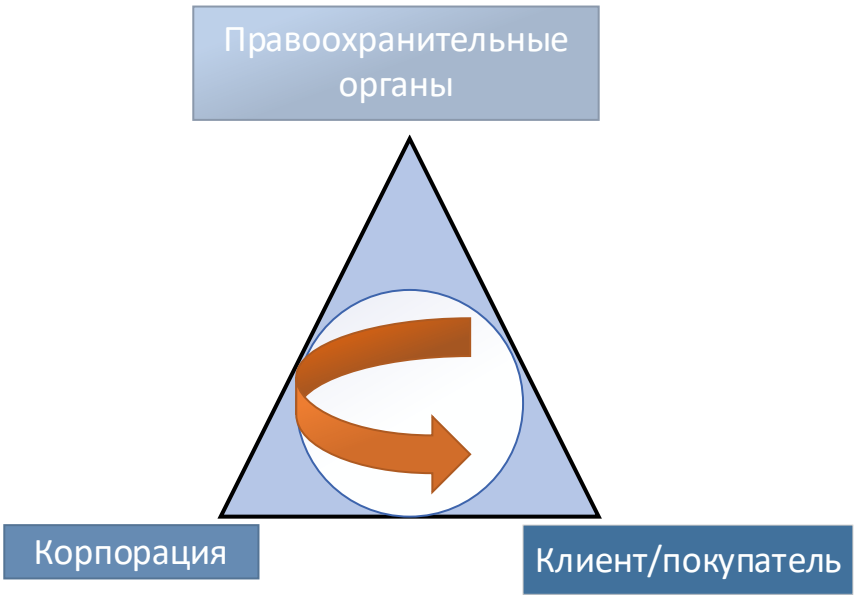


Рисунок 4.2.Треугольные отношения с корпорацией

Точно так же угроза кибератак требует от корпораций налаживания партнерских отношений с клиентами и правоохранительными органами. Правда, это сотрудничество несколько сложное, но необходимое. Потому что угрозу кибератак на корпорации нельзя отрицать. Чтобы минимизировать это, угроза требует совместных, прямых, непрерывных действий тех, кто прямо или косвенно затронут.

Тревожным и повторяющимся аспектом бесчисленных атак на малые и крупные корпорации является ценное время, которое проходит после атаки, прежде чем корпорации осознают, что произошло нарушение. Это показывает двойную слабость:

— Брандмауэры недостаточно сложны, чтобы предотвратить атаку.
— Брандмауэры недостаточно сложны, чтобы обнаруживать атаку после ее совершения.

В то время как атака остается без ответа в течение определенного периода времени, увеличивается уязвимость от одной атаки, с точки зрения модели континуума уязвимостей

незарегистрированная атака отражает постоянную уязвимость. В отличие от традиционного теракта, в его основе лежит единичная атака, отражающая трехчастную модель: планирование, выполнение, завершение (рис. 4.3).

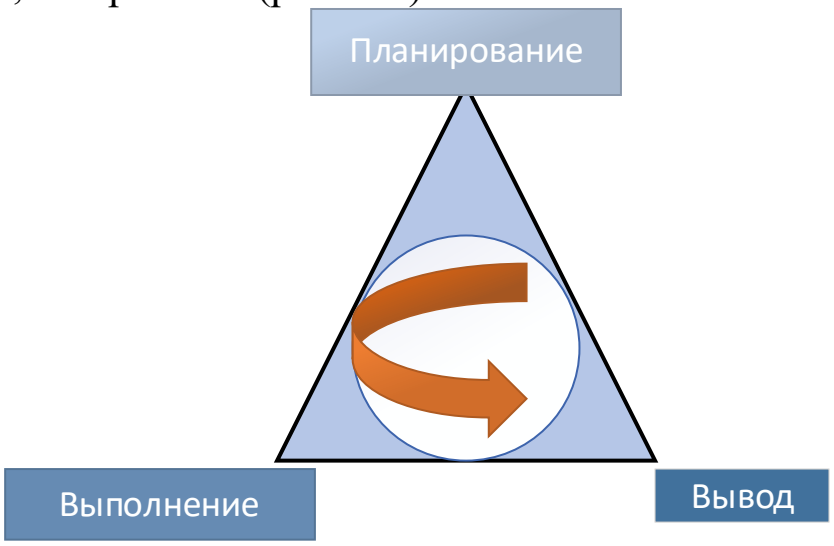


Рисунок 4.3. Трехчастная модель

Возникает вопрос, почему корпорации так не решаются признать, что нарушение произошло? Ответ прост: это негативно сказывается на финансах такой популярной корпорации, отпугивает новых клиентов, дает шанс конкурентам набрать очки и может побудить существующих клиентов заняться бизнесом в другом месте.

Еще один недостаток корпораций заключается в том, что очень немногие корпорации сразу же после взлома говорят: «Нас взломали, мы беспомощны, давайте извлечем из этого урок». Потому что это может закрыть для них многие возможности. Этот процесс очень удобен для хакеров, потому что корпорации не могут учиться друг у друга тому, как нейтрализовать угрозы.

Корпорации, отдельные лица или государства иногда недооценивают возможности потенциальных злоумышленников. Они думают, что их система лучше или эффективнее. Следствием этого является следующее:

— Постоянная слабость;
— Постоянная угроза клиентам;
— Возможна гражданско-правовая ответственность за неспособность обеспечить надлежащую защиту конфиденциальности информации о клиенте и ответственность за неуведомление о последствиях нарушения.

Наиболее важными факторами, вызывающими корпоративный крах, являются: отсутствие защиты и отсутствие осведомленности. Причины приведены ниже:

— Потенциальные клиенты не решаются начать свой бизнес после того, как обнаруживают, что не могут защитить/не общаться.

— Существующие клиенты могут начать свой бизнес в другом месте, если они решат, что не были предприняты все разумные меры для защиты их конфиденциальности.

— Широкая общественность негативно относится к корпорации в контексте противодействия кибератакам и минимизации киберрисков, но самой сильной критикой будет неправда.

Эти недостатки должны быть устранены следующим образом:

— Распознавание доступа;
— Перечень предпринятых мер по немедленному устранению доступа для защиты клиентов;
— Перечень мер, направленных на защиту клиентов в будущем;
— Общение с другими корпорациями в контексте обмена информацией;
— Применять агрессивные меры против киберпреступности.

Такой подход, с точки зрения корпорации, показывает готовность привлекать разную аудиторию, в частности, заказчиков и правоохранительные органы.

Правоохранительные органы.Нет сомнений в том, что кибератаки сложны и создают новые проблемы для правоохранительных органов. Интервью с правоохранительными органами подчеркивают, что киберпреступность принципиально отличается как от традиционных полицейских и грабителей, так и от традиционного терроризма. Для правоохранительных органов киберпреступность — это совершенно другая модель преступления, которая ставит сложные задачи. Взаимодействие с сотрудниками правоохранительных органов свидетельствует о большей готовности тесно сотрудничать с корпорациями как в инициативном, так и в реактивном порядке.

Ключевым подходом здесь является смягчение угроз и минимизация последствий фактической атаки. Треугольник кибербезопасности, корпораций и правоохранительных органов требует оперативных возможностей и будет продолжать развиваться

(рис. 4.5).

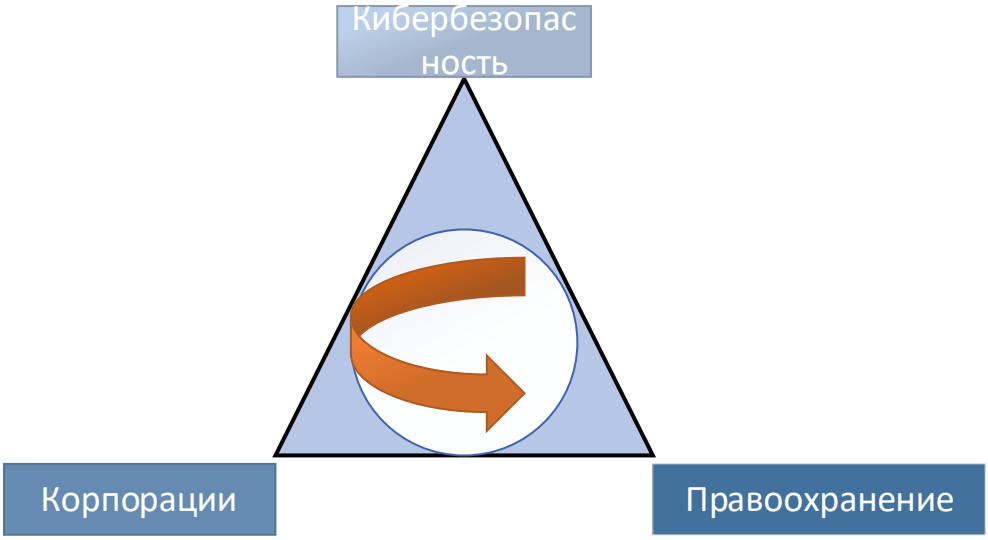


Рисунок 4.5.Треугольник кибербезопасности

Капитал.Недавние атаки показали, что корпорации может потребоваться до 243 дней, чтобы понять, распознать и обнаружить нарушение. Одна из причин этой неожиданной и часто тревожной задержки заключается в том, что предотвращение киберугроз требует значительных инвестиций. Эти инвестиции носят не только финансовый характер, но также требуют инвестиций в персонал, что требует значительных изменений в корпоративной культуре, что требует от руководства признания и четкого определения киберуязвимости.

Перед лицом киберугрозы корпорации должны признать приоритет долга перед клиентом, а не перед акционером. Эта пересмотренная модель приоритетов требует от корпоративного управления большей открытости, честности и искренности, даже если это вызывает недопонимание среди акционеров. Этот подход основан на признании того, что основной обязанностью корпорации является защита и информирование клиента, даже если эта обязанность обходится корпорации дорого.

Корпоративная безопасность Модель корпоративной безопасности может быть построена с учетом стоимости, воздействия и злонамеренных намерений хакеров (рис. 4.6).

Рисунок 4.6.Модель корпоративной кибербезопасности

Виды киберпреступлений против корпораций.Одним из примеров киберпреступлений против корпораций является фишинговая атака. При фишинговой атаке киберпреступник отправляет поддельное электронное письмо или сообщение, полученное из законного источника, например от надежного поставщика, банка или коллеги. Электронное письмо обычно содержит ссылку или вложение, при нажатии на которое на компьютер получателя устанавливается вредоносное ПО или предлагается ввести конфиденциальную информацию, такую как учетные данные для входа в систему, номера кредитных карт или личную информацию.

Как только киберпреступник получает доступ к компьютеру получателя или конфиденциальным данным, он может использовать эти данные для различных злонамеренных целей, таких как кража конфиденциальной информации, совершение финансового мошенничества или распространение вредоносного ПО на другие системы в сети организации. В дополнение к прямым финансовым и операционным потерям в результате киберпреступности организация может понести ущерб репутации, потерю доверия клиентов и юридическую ответственность.

Для предотвращения фишинговых атак организации могут применять различные меры кибербезопасности, например требовать

от сотрудников выявлять и сообщать о подозрительных электронных письмах, использовать антифишинговое программное обеспечение и брандмауэры, внедрять двухфакторную аутентификацию и улучшать программное обеспечение и системы безопасности, обучаться регулярным обновлениям. Кроме того, организации могут разрабатывать планы реагирования на инциденты, чтобы быстро обнаруживать фишинговые атаки и реагировать на них, чтобы минимизировать ущерб.

Кибератаки на корпорации дополнительно проанализированы и объяснены в таблице 1.

Таблица 4.1

Описание кибератак на корпорации

Тип киберпреступления	**Описание**
Программы-вымогатели	Тип вредоносного ПО, которое шифрует данные организации и требует оплаты в обмен на ключ дешифрования.
Фишинг	Использование мошеннической электронной почты, веб-сайтов или сообщений, чтобы обманом заставить сотрудников раскрыть конфиденциальную информацию или загрузить вредоносное ПО.
Соглашение о корпоративной электронной почте	Тип фишинговой атаки, нацеленной на сотрудников, имеющих доступ к финансовой информации или платежным системам, с целью заставить их перевести деньги на мошеннические счета.
Внутренние угрозы	Злонамеренные или небрежные действия сотрудников или подрядчиков, которые приводят к утечке данных или другим нарушениям безопасности.
Распределенные атаки типа «отказ в обслуживании» (DDoS)	Заполнение сети или сервера трафиком с целью нарушения работы организации.
Данные нарушения	Несанкционированный доступ или

	кража конфиденциальной информации, включая личную информацию (PII), финансовую информацию и интеллектуальную собственность.
Кибершпионаж	Кража конфиденциальной информации или интеллектуальной собственности с целью получения конкурентного преимущества или нарушения деятельности организации.
Внутренние угрозы	Злонамеренные или небрежные действия сотрудников или подрядчиков, которые приводят к утечке данных или другим нарушениям безопасности.

Типы киберпреступлений, с которыми сталкиваются корпорации, постоянно меняются, и организациям важно быть в курсе последних угроз и уязвимостей. Применение соответствующих мер безопасности поможет защитить их данные и операции.

Важно, чтобы организации применяли соответствующие меры безопасности для защиты своих данных и операций от киберпреступлений такого типа. Эти меры могут включать сетевую безопасность, контроль доступа, обучение сотрудников, шифрование данных и планирование реагирования на инциденты.

Корпоративные ответы на киберпреступность. Корпоративная киберпреступность становится все более актуальной проблемой для бизнеса во всем мире. Угроза кибератак серьезна, последствия варьируются от финансовых потерь до репутационного ущерба и юридической ответственности. К счастью, есть несколько контрмер, которые организации могут предпринять, чтобы снизить риск и защитить себя от киберпреступности (таблица 4.2).

Реагирование на корпоративные киберпреступления относится к стратегиям и действиям, которые организации предпринимают для предотвращения, обнаружения и реагирования на кибератаки, утечки данных и другие киберугрозы. Некоторые ключевые концепции, связанные с реагированием корпораций на киберпреступность:

— Кибербезопасность: практика защиты компьютерных систем, сетей и конфиденциальной информации от несанкционированного доступа, кражи, повреждения или уничтожения.
— Управление рисками: процесс выявления, оценки и снижения рисков, которые могут нанести ущерб активам, репутации или операциям организации.
— Реагирование на инциденты: набор процедур и протоколов, которым организации следуют, чтобы реагировать и сдерживать киберинциденты, такие как утечка данных, заражение вредоносным ПО или фишинговые атаки.
— Криминалистика: использование специализированных методов и инструментов для сбора и анализа цифровых доказательств, связанных с киберинцидентом или преступлением.
— Киберстрахование: тип страхового полиса, покрывающий финансовые убытки и обязательства, возникшие в результате кибератак или утечки данных.
— Соблюдение: процесс обеспечения соблюдения организациями соответствующих законов, правил и стандартов, касающихся кибербезопасности и конфиденциальности данных.
— Информация о киберугрозах: сбор, анализ и распространение информации о потенциальных или реальных киберугрозах, включая их источник, мотив и методы.
— Управление сторонними рисками: процесс оценки и управления рисками кибербезопасности, связанными со сторонними поставщиками, поставщиками или партнерами, имеющими доступ к системам или данным организации.
— Непрерывность бизнеса: способность организации продолжать работу во время и после разрушительного события, такого как кибератака.
— Управление: структура политик, процедур и средств контроля, которые определяют управление организацией и процессы принятия решений, связанные с кибербезопасностью.
— Обучение и осведомленность: обучайте сотрудников и заинтересованных лиц рискам кибербезопасности, передовым методам, а также организационным политикам и процедурам.

— Аналитика угроз: мониторинг и анализ киберугроз и уязвимостей для информирования об управлении рисками и стратегиях реагирования на инциденты.

Существует несколько контрмер, которые организации могут предпринять, чтобы защитить себя от корпоративной киберпреступности. Внедряя комплексную стратегию кибербезопасности, включающую обучение сотрудников, контроль доступа, сетевую безопасность, планирование реагирования на инциденты, шифрование, организации могут снизить свои риски и более эффективно реагировать на инциденты безопасности.

Таблица 4.2

Меры защиты от киберпреступлений

Контрмера	Описание
Обучение сотрудников	Обучение сотрудников передовым методам кибербезопасности может помочь им не стать жертвами мошенничества или других кибератак.
Контроль доступа	Предоставление доступа к конфиденциальной информации и системам только авторизованному персоналу помогает предотвратить несанкционированный доступ и снизить риск внутренних угроз.
Сетевая безопасность	Внедрение брандмауэров, систем обнаружения вторжений и других мер безопасности может помочь защититься от внешних угроз, таких как вредоносное ПО и DDoS-атаки.
Планирование реагирования на инциденты	Разработка плана реагирования на инциденты безопасности может помочь организациям свести к минимуму ущерб и быстрее восстановиться после атаки.
Шифрование	Шифрование конфиденциальных данных помогает защитить их от несанкционированного доступа в случае утечки данных.
Обучение технике безопасности	Обучение сотрудников выявлению киберугроз и реагированию на них может

	помочь предотвратить фишинговые атаки, компрометацию корпоративной электронной почты и другие виды киберпреступлений.
Многофакторная аутентификация	Требование от сотрудников использовать несколько форм аутентификации, таких как пароли и токены безопасности, может помочь предотвратить несанкционированный доступ к корпоративным сетям и системам.
Сегментация сети	Разделение корпоративной сети на более мелкие изолированные сегменты может помочь предотвратить распространение вредоносных программ и ограничить ущерб от кибератаки.
Планирование реагирования на инциденты	Наличие плана реагирования на кибератаки может помочь свести к минимуму последствия инцидента и обеспечить быстрое и эффективное реагирование.
Управление рисками третьих лиц	Регулярная оценка и мониторинг безопасности сторонних поставщиков и подрядчиков может помочь предотвратить атаки на цепочку поставок и другие формы киберпреступлений.

Обучение сотрудников является важнейшей мерой борьбы с киберпреступностью, поскольку сотрудники часто являются самым слабым звеном в защите кибербезопасности организации. Регулярное обучение по таким темам, как управление паролями, безопасный просмотр веб-страниц и обнаружение фишинговой электронной почты, может помочь предотвратить непреднамеренное нажатие сотрудниками вредоносных ссылок или раскрытие конфиденциальной информации.

Контроль доступа также помогает предотвратить киберпреступность, ограничивая доступ к конфиденциальной информации и системам только тем, кто в этом нуждается. Это помогает предотвратить внутренние угрозы, когда уполномоченные сотрудники или подрядчики злоупотребляют своими привилегиями в злонамеренных целях.

Меры сетевой безопасности, такие как брандмауэры и системы обнаружения вторжений, помогают предотвратить внешние угрозы, такие как вредоносное ПО и DDoS-атаки. Кроме того, разработка плана реагирования на инциденты может помочь организациям реагировать на инциденты безопасности быстрее и эффективнее.

Шифрование также может быть эффективной мерой противодействия киберпреступности, затрудняя злоумышленникам доступ к конфиденциальной информации, даже если им удастся взломать систему защиты организации. Обновление вашего программного обеспечения с помощью последних исправлений безопасности также важно, так как уязвимости и эксплойты могут быть быстро обнаружены и использованы злоумышленниками.

Важно отметить, что ни одна контрмера не является надежной, и предприятия должны использовать многоуровневый подход к кибербезопасности, который охватывает несколько областей риска. Кроме того, предприятия должны регулярно пересматривать и обновлять свои стратегии кибербезопасности для противодействия возникающим угрозам и уязвимостям.

§ 4.3. Роль отдельных лиц в предотвращении кибербезопасности

Во многих случаях сотрудники предприятий слишком легкомысленно относятся к требованиям кибербезопасности, что может иметь серьезные последствия для организаций, в которых они работают. Недавняя эпидемия программы-вымогателя WannaCry продемонстрировала, что человеческий фактор может играть важную роль в уязвимости компаний по всему миру. Спустя почти два месяца после того, как обнаруженные уязвимости были исправлены новыми патчами Microsoft, многие компании по всему миру до сих пор не обновили свои системы с учетом новых изменений. Один из стереотипов, который часто наблюдается и подтверждается в экспериментах, заключается в том, что работники, не связанные с ИТ, являются самым слабым звеном: например. сотрудники с правами локального администратора отключают защитные решения на своих компьютерах и позволяют заражению распространяться со своих компьютеров на всю корпоративную сеть. В результате безопасность сети теряется.

Рисунок 4.7.Отключение системы безопасности или получение обновлений

Когда мы ищем ответы на условный вопрос, какую роль в борьбе бизнеса с киберпреступностью играют сотрудники и отдельные лица в целом, результаты поражают. Согласно исследованиям «Лаборатории Касперского», более половины (52%) предприятий считают, что они подвержены риску изнутри. Их сотрудники подвергают риску бизнес, на котором они работают, либо намеренно, либо по собственной небрежности или невежеству.

В отчете «Лаборатории Касперского» ниже объясняется, как и почему это происходит, и что компании могут сделать, чтобы защитить себя от своих сотрудников.

В условиях сложного и растущего ландшафта киберугроз, когда 57% предприятий в настоящее время считают, что их ИТ-безопасность слаба, предприятия также понимают, что одной из самых надежных защит от кибератак являются их сотрудники. На самом деле, 52 процента компаний признают, что сотрудники являются самой большой слабостью в области ИТ-безопасности, и их неосторожные действия ставят под угрозу стратегию ИТ-безопасности бизнеса.

На приведенной ниже диаграмме показано, что компании знают, что ошибки сотрудников могут очень легко, но очень быстро повлиять на безопасность их компании. В основном это сотрудники, которые обмениваются несоответствующей информацией через

мобильные устройства (47%), физическая потеря мобильных устройств, подвергающая их компанию риску (46%), и сотрудники, использующие неправильные ИТ-ресурсы (44%).

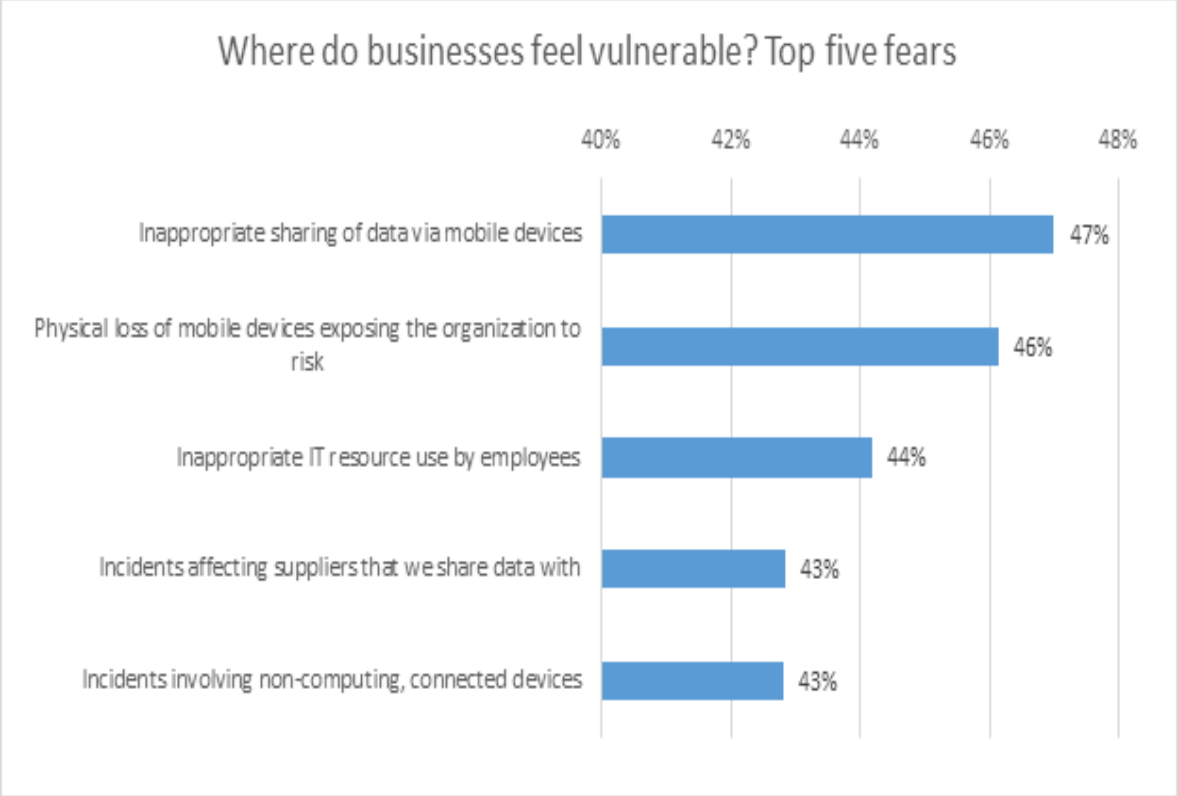


Рисунок 4.8. Последовательность рисков, влияющих на бизнес (источник: Обзор рисков ИТ-безопасности, 2017 г.)

Более пристальный взгляд на эти результаты показывает, что опасения сотрудников по поводу ненадлежащего использования ИТ значительно различаются в зависимости от размера компании, при этом малые предприятия (1-49 сотрудников являются VSB) более подвержены большему риску, чем предприятия с более чем 1000 сотрудников. Эта доля также остается большой в предприятиях среднего бизнеса (МСБ). Это может быть связано с рядом факторов, в том числе с потенциально более строгими политиками и более углубленным обучением персонала передовому опыту. Кроме того, мы часто обнаруживаем, что малые предприятия предоставляют сотрудникам неограниченный доступ высокого уровня к бизнес-ИТ-ресурсам. Но мы можем отметить это как негативный фактор с точки зрения безопасности.

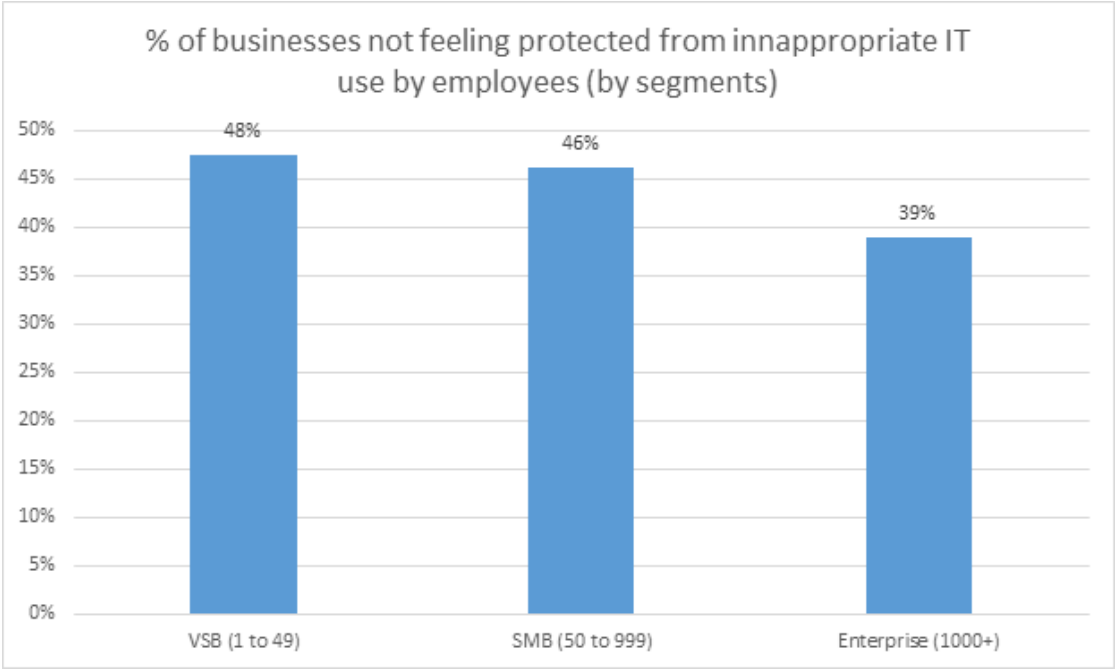


Рисунок 4.9. Уровень негативного воздействия сотрудников на малый, средний и крупный бизнес (источник: Исследование рисков ИТ-безопасности, 2017 г., глобальные данные)

Результаты исследований показывают, что у предприятий есть веские основания для беспокойства о том, что сотрудники вносят свой вклад в риски кибербезопасности. Сотрудники могут совершать ошибки, которые подвергают риску данные или системы их компании.

Небрежные или неосведомленные сотрудники, например, являются второй наиболее вероятной причиной серьезных нарушений безопасности, уступая только вредоносным программам. Кроме того, в 46 процентах инцидентов кибербезопасности за последний год небрежность или неквалифицированность сотрудников способствовали атакам на компанию.

Человеческая ошибка сотрудников — не единственный «вектор атаки», жертвами которого становятся предприятия. Тем не менее, внутренние сотрудники также создавали проблемы безопасности своими злонамеренными действиями: исследования показали, что 30 процентов инцидентов безопасности за последние 12 месяцев были связаны с тем, что сотрудники работали против своих работодателей. Среди предприятий, столкнувшихся с инцидентами кибербезопасности за последние 12 месяцев, каждый десятый (11%) из самых серьезных инцидентов был связан с небрежностью сотрудников.

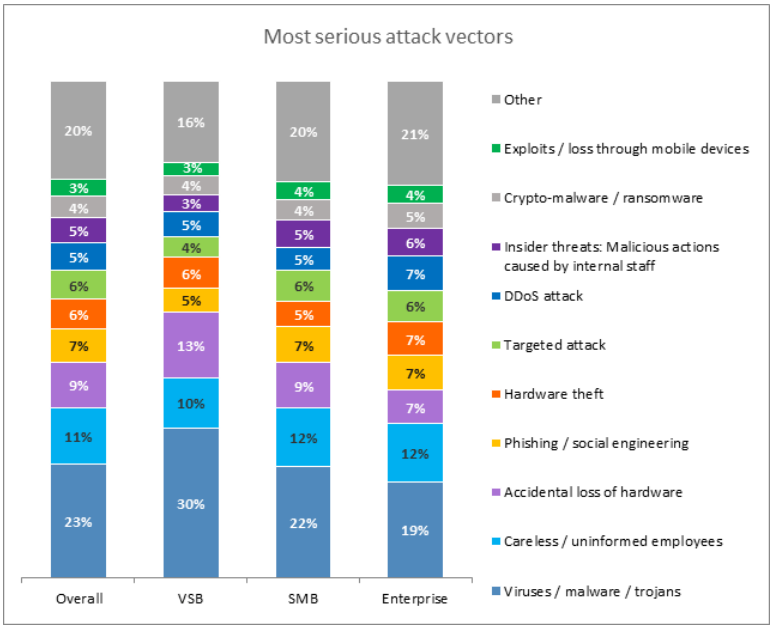


Рисунок 4.10. Опасные векторы атак в малом, среднем и крупном бизнесе (источник: Обзор рисков ИТ-безопасности, 2017 г., глобальные данные)

Халатность сотрудников и фишинг (социальная инженерия) являются ключевыми факторами распространения вредоносных программ и целевых атак.

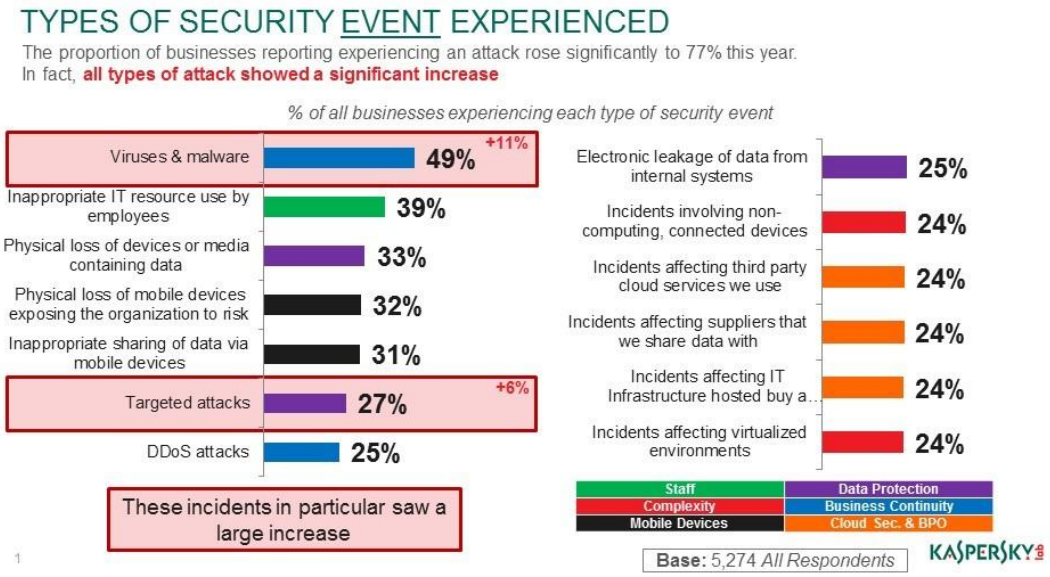


Рисунок 4.11. Тенденция роста числа атак, наблюдаемая на предприятиях (источник: Обзор рисков ИТ-безопасности, 2017 г., глобальные данные)

Сообщалось, что в 2017 году 49 процентов предприятий во всем мире подверглись атакам вирусов и вредоносных программ, что на 11 процентов больше, чем в 2016 году. Чуть более половины (53%) тех, кто столкнулся с инцидентами, связанными с вирусами и

вредоносными программами, считают, что небрежность или неосведомленность сотрудников являются основным фактором, а более трети (36%) считают, что фишинг или социальная инженерия способствовали возникновению угрозы. .

«Скрытие» или сокрытие проблемы.Когда на предприятии происходят инциденты безопасности, важно, чтобы сотрудники были готовы обнаружить нарушение или снизить риски. Однако сотрудники не всегда принимают меры, когда компания сталкивается с инцидентом безопасности. На самом деле, в 40 процентах компаний по всему миру сотрудники скрывают, когда происходит инцидент. Сокрытие инцидента может иметь драматические последствия и увеличить наносимый ущерб. Один незарегистрированный инцидент может даже привести к крупномасштабному нарушению работы всей инфраструктуры организации.

Своевременное обнаружение, а также успешное расследование и криминалистический анализ целевой атаки — ключ к решению проблемы. Полагаться исключительно на бдительность сотрудников и их способность сообщать об инцидентах уже недостаточно, поскольку риски удваиваются из-за человеческого фактора и сложности атаки. Поэтому предприятиям рекомендуется использовать специальные решения и технологии, автоматизирующие системный мониторинг и снижающие вероятность ошибки безответственности.

Для крупных компаний проблема «сокрытия» является наиболее сложной: 45% предприятий (более 1000 сотрудников) пытаются выявить сотрудников, которые скрывают инциденты кибербезопасности, по сравнению с только 29% малых предприятий (менее 49 сотрудников). .

Проблема сокрытия инцидентов должна быть доведена до сведения не только сотрудников, но и всего бизнеса, т.е. высшего руководства и HR. Если сотрудники что-то скрывают, на это должна быть причина. В некоторых случаях компании вводят строгие, но нечеткие правила и возлагают на сотрудников дополнительные обязанности, предупреждая их не делать то или иное или привлекая к ответственности, если что-то пойдет не так. Такая политика только усиливает страх и оставляет работникам только один выход — избегать любого наказания, то есть пытаться скрыть свою вину.

Ущерб от безответственных сотрудников.Помимо проблемы сокрытия инцидентов, безответственность сотрудников может серьезно повлиять на целостность данных и системы фирмы, когда речь идет об инциденте безопасности.

Например, 46% подтверждают, что эти инциденты привели к раскрытию их деловой информации или из-за неправомерных действий сотрудников. Кроме того, более четверти (28%) говорят, что потеряли конфиденциальную информацию из-за безответственности сотрудников, а 25% потеряли платежную информацию. Все это, несомненно, может иметь далеко идущие и разрушительные последствия для деловой репутации как внутри компании, так и за ее пределами.

BYOD — это вызов для бизнеса.Результаты исследований показывают, что, хотя и предприятия, и сотрудники хорошо осведомлены о тенденции использования собственных устройств (BYOD), BYOD по-прежнему является головной болью для больших и малых компаний. Тем не менее, предприятия по всему миру по-прежнему обеспокоены BYOD.

Проблемы небольших компаний, как правило, связаны с практикой BYOD сотрудников, в то время как предприятия, скорее всего, будут бороться с управлением безопасностью. Например, почти половина (48%) предприятий обеспокоены тем, что сотрудники ненадлежащим образом делятся корпоративной информацией через мобильные устройства, которые они берут с собой на работу. Это вызывает особую озабоченность у малых предприятий (57%), возможно, отчасти из-за того, что более крупные предприятия с большей вероятностью примут политику BYOD, чтобы сократить расходы и использовать мобильную рабочую силу.

С другой стороны, предприятиям сложнее управлять безопасностью на устройствах пользователей. Чуть более половины (51%) говорят, что это их беспокоит, по сравнению с двумя пятыми (42%) представителей малого бизнеса.

Одна из причин, по которой компании могут относиться к BYOD, заключается в том, что BYOD в конечном итоге зависит от обязанностей сотрудников и их способности обрабатывать бизнес-данные на своих личных устройствах. Этот процесс не всегда проходит гладко — люди теряют свои устройства, а устройства

крадут. По сути, чем больше устройство удаляется из рабочей среды, тем больше оно (и его данные) подвергается риску.

Исследования показывают, что более половины (54%) предприятий сталкиваются с утечкой данных из-за того, что сотрудники теряют устройства. Небрежность сотрудников непосредственно способствовала 48% инцидентов кибербезопасности, больше, чем кража устройств, на которую приходится треть (37%) инцидентов.

Политика ИТ-безопасности.Наличие политики ИТ-безопасности недостаточно. Политика сама по себе не может защитить бизнес от угроз. То есть политика ИТ-безопасности не всегда соблюдается сотрудниками, для которых она предназначена, либо политика безопасности не полностью покрывает все возможные риски.

Исследования «Лаборатории Касперского» показывают, что 44% компаний говорят о том, что сотрудники не в полной мере соблюдают их политики ИТ-безопасности. Еще более интересно то, что, хотя две пятых компаний признались нам, что сотрудники не соблюдают их политику безопасности, сами компании мало что делают для решения этой проблемы, и только четверть (26%) планирует следовать правилам. Эти результаты показывают, что политики ИТ-безопасности не всегда актуальны для сотрудников.

Во многих случаях политики написаны настолько сложно, что сотрудники не могут их эффективно усвоить. Вместо того, чтобы сообщать о рисках, опасностях и передовом опыте в четких и всеобъемлющих руководствах, предприятия часто раздают сотрудникам многостраничные документы, которые все подписывают, но мало кто читает и еще меньше понимает.

Но, несмотря на очевидные проблемы, компании пытаются решить проблему риска изнутри. Привлечение большего числа преданных своему делу сотрудников для помощи в обучении персонала и реализации политики безопасности является логичным ответом на проблему невнимательности персонала. И это ответ, который пытаются реализовать многие компании по всему миру.

Как мы упоминали ранее, наличия политики безопасности недостаточно. Необходимо найти надлежащий баланс между политикой и обязанностями, чтобы избежать рисков, вызванных небрежностью или неосведомленностью персонала.

Обучение сотрудников важно для повышения осведомленности сотрудников и мотивации их обращать внимание на киберугрозы и меры противодействия, даже если это не входит в их конкретные обязанности. Установка обновлений, обеспечение защиты от вредоносных программ и правильное управление личными паролями не должны быть в конце списка дел сотрудника. Меры безопасности, ориентированные на сотрудников, такие как вовлечение и обучение сотрудников, являются одними из наиболее желательных тактик, используемых предприятиями для защиты от будущих киберугроз.

«Лаборатория Касперского» утверждает, что лучший способ защитить бизнес от киберугроз — это сочетание правильных инструментов и методов. В дополнение к обучению сотрудников, защита должна включать в себя решения безопасности для групп ИТ-безопасности, которые делают корпоративную сеть более заметной и управляемой.

Большинство угроз, связанных с неосведомленностью или небрежностью сотрудников, включая спам, фишинг и программы-вымогатели, можно устранить с помощью решений для защиты конечных точек. Существуют специализированные продукты, которые могут удовлетворить конкретные потребности средних и крупных компаний с точки зрения функциональности, предварительно настроенной защиты или расширенных настроек безопасности.

Согласно цитируемым исследованиям, сотрудники могут стать векторами атаки по-разному: они могут быть небрежными, они могут быть неосведомленными или их действия могут быть злонамеренными. Тенденции мобильности означают, что небрежные или неосведомленные сотрудники могут с большей вероятностью совершать ошибки, а такие угрозы, как фишинг и социальная инженерия, а также сотрудники, которые не знают, как отличить законную деятельность от злонамеренной, могут увеличить бизнес-риск. Если они вызвали инцидент кибербезопасности (или были одним из факторов, стоящих за этим инцидентом), сотрудники могут попытаться скрыть то, что произошло, оставив некоторые нарушения нераскрытыми в течение длительного времени и еще больше подорвав бизнес.

Хотя наличие политики безопасности имеет решающее

значение, предприятия также должны понимать, что политики не могут покрывать все риски. Кроме того, сотрудники не всегда строго следуют собственной политике. Существует очевидная потребность в решениях, которые обеспечивают большую прозрачность и централизованное управление безопасностью корпоративных сетей, а также обучение, чтобы сотрудники лучше осознавали последствия своих действий. Только обучая сотрудников важности безопасной работы, компании смогут помочь снизить риск этого конкретного вектора атаки и защитить данные, которые для них наиболее важны.

Контрольные вопросы:

1. Какие основные элементы должна включать политика информационной безопасности организации?
2. Какую пользу организация может получить от добровольной разработки и внедрения политики информационной безопасности?
3. Какие существуют международные стандарты информационной безопасности и как они могут помочь организации защитить свои информационные активы?
4. Какие риски и угрозы могут возникнуть, если в организации нет политики информационной безопасности или она не соблюдается?
5. Как политика информационной безопасности может помочь организации управлять инцидентами информационной безопасности и сокращать их количество?
6. Какие основные элементы должна включать политика информационной безопасности организации?
7. Какую пользу организация может получить от добровольной разработки и внедрения политики информационной безопасности?
8. Какие существуют международные стандарты информационной безопасности и как они могут помочь организации защитить свои информационные активы?
9. Какие риски и угрозы могут возникнуть, если в организации нет политики информационной безопасности или она не следует ей?
10. Как политика информационной безопасности может помочь организации управлять инцидентами информационной безопасности и сокращать их количество?

ГЛАВА V. ПОЛИТИКА АДМИНИСТРИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ

§ 5.1. Роль правоохранительных органов в предотвращении кибербезопасности

Правоохранительные органы играют решающую роль в устранении угроз кибербезопасности, поскольку они несут ответственность за расследование киберпреступлений и уголовное преследование. Сотрудники правоохранительных органов должны обладать знаниями и навыками, необходимыми для эффективного выявления, анализа и реагирования на киберугрозы. Они должны работать с экспертами по кибербезопасности и другими заинтересованными сторонами для снижения рисков и предотвращения киберпреступлений.

Существуют различные киберугрозы и риски, с которыми люди, организации и правительства сталкиваются каждый день. Некоторые из наиболее распространенных угроз кибербезопасности включают вредоносное ПО, фишинг, программы-вымогатели, социальную инженерию, взлом и атаки типа «отказ в обслуживании» (DoS). Вредоносное ПО — это программное обеспечение, предназначенное для повреждения, отключения или получения несанкционированного доступа к компьютерным системам или сетям. Фишинг включает в себя использование поддельных электронных писем, сообщений или веб-сайтов, чтобы обманом заставить пользователей раскрыть конфиденциальную информацию или установить вредоносное ПО. Программа-вымогатель — это тип вредоносного ПО, которое шифрует файлы или блокирует доступ пользователей к их устройствам до тех пор, пока не будет выплачен выкуп. Социальная инженерия относится к манипулированию людьми с целью раскрытия конфиденциальной информации. Взлом предполагает использование уязвимостей в компьютерных системах для получения несанкционированного доступа. DoS-атаки включают переполнение сервера или сети трафиком, который приводит к сбою или сбою.

Характер киберугроз постоянно меняется, и регулярно возникают новые риски. Хакеры и киберпреступники становятся все более изощренными в своих методах, используя передовые методы, такие как искусственный интеллект (ИИ) и машинное обучение

(МО), для проведения атак. Широкое использование облачных вычислений и Интернета вещей (IoT) также расширило возможности для атак, облегчив киберпреступникам выбор целей для отдельных лиц и организаций. Распространение социальных сетей и онлайн-платформ также облегчило злоумышленникам распространение дезинформации и влияние на общественное мнение.

Киберпреступность оказывает серьезное влияние на отдельных лиц, организации и правительства. Физические лица могут столкнуться с финансовыми потерями, кражей личных данных или другими формами вреда в результате утечки их личной информации. Организации могут понести репутационный ущерб, финансовые потери или потерю интеллектуальной собственности из-за кибератак. Правительства могут потерять секретную информацию в результате угроз национальной безопасности, кибершпионажа или кибератак.

Сотрудничество между правоохранительными органами и экспертами по кибербезопасности.В сегодняшнюю цифровую эпоху правоохранительные органы сталкиваются с серьезными проблемами в борьбе с растущей угрозой киберпреступности. Традиционных методов борьбы с преступностью уже недостаточно перед лицом все более изощренной тактики киберпреступников. Таким образом, эффективная кибербезопасность требует совместных усилий правоохранительных органов и специалистов по кибербезопасности. Необходимость междисциплинарного сотрудничества между этими двумя группами невозможно переоценить.

Сотрудничество между правоохранительными органами и специалистами по кибербезопасности необходимо для обеспечения эффективного обнаружения, предотвращения и расследования киберугроз. Обе группы обладают уникальным опытом и взглядами, необходимыми для эффективного противодействия киберугрозам. Правоохранительные органы обладают юридическими полномочиями и следственными полномочиями, а специалисты по кибербезопасности обладают специальными техническими навыками и знаниями о киберугрозах. Таким образом, совместный подход помогает решать как юридические, так и технические аспекты киберпреступности.

Фирмы частного сектора, занимающиеся кибербезопасностью,

могут сыграть решающую роль в смягчении киберугроз. Эти фирмы, как правило, располагают новейшими технологиями и инструментами, что делает их хорошо оснащенными для обнаружения и предотвращения кибератак. Правоохранительные органы могут извлечь выгоду из сотрудничества с частными фирмами, занимающимися кибербезопасностью, несколькими способами, включая доступ к экспертным знаниям, обмен информацией и совместные расследования.

Обмен информацией является важнейшим компонентом кибербезопасности, и фирмы частного сектора могут предоставлять правоохранительным органам ценную информацию и оперативные данные. Делясь информацией о возникающих киберугрозах, схемах атак и новых вредоносных программах, фирмы частного сектора могут помочь правоохранительным органам лучше понять и предвидеть киберугрозы. Кроме того, фирмы частного сектора могут помочь правоохранительным органам выявить потенциальных подозреваемых и выследить киберпреступников.

Эффективная кибербезопасность требует активного подхода к обмену информацией и сбору разведданных. Правоохранительные органы должны сотрудничать с другими агентствами, фирмами частного сектора и международными партнерами для обмена информацией о возникающих киберугрозах. Такой обмен информацией помогает выявлять модели преступной деятельности и позволяет правоохранительным органам разрабатывать эффективные стратегии предотвращения кибератак и реагирования на них.

Эффективный обмен информацией также включает обмен передовым опытом и извлеченными уроками. Правоохранительные органы должны извлечь уроки из прошлых инцидентов, чтобы лучше подготовиться к будущим угрозам. Предоставление этой информации другим агентствам и специалистам по кибербезопасности поможет повысить общую кибербезопасность и обеспечить, чтобы правоохранительные органы были лучше оснащены для предотвращения кибератак и реагирования на них.

Расследование киберпреступлений и цифровая криминалистика.Расследование киберпреступлений требует специальных навыков и знаний. Правоохранительные органы должны использовать различные методы и инструменты для сбора

доказательств, отслеживания киберпреступников и подготовки дела для судебного преследования. Эти методы и инструменты включают в себя:

1. **Сетевая криминалистика:**Это включает в себя анализ сетевого трафика для выявления моделей подозрительной активности, таких как попытки несанкционированного доступа или утечки данных;
2. **Анализ вредоносных программ:**Это включает в себя анализ вредоносного кода для определения источника атаки и тактики, используемой киберпреступниками;
3. **Социальная инженерия:**Это включает в себя использование психологических методов для манипулирования людьми с целью раскрытия конфиденциальной информации или совершения действий, ставящих под угрозу их безопасность;
4. **Криптография:**Это включает в себя анализ зашифрованных данных для раскрытия секретных сообщений или преступной деятельности.

Цифровые доказательства довольно хрупкие и могут быть легко потеряны или повреждены, если с ними не обращаться должным образом. Правоохранительные органы должны уделять пристальное внимание сбору и сохранению цифровых доказательств, чтобы обеспечить их допустимость в суде. Это включает в себя установление цепочки сохранности, которая следует за обработкой доказательств с момента их сбора до момента их представления в суд.

Правоохранительные органы также должны быть осведомлены о юридических требованиях для получения цифровых доказательств. Это может включать работу с международными партнерами для получения ордера или повестки в суд или для получения доказательств из-за границы. Несоблюдение установленных законом требований может привести к тому, что доказательства будут отклонены судом.

Правовые основы кибербезопасности.Законы и положения о кибербезопасности имеют решающее значение для смягчения последствий киберугроз и атак. Они обеспечивают основу для правоохранительных органов для расследования и судебного преследования киберпреступников, обеспечивая при этом защиту отдельных лиц и организаций от киберугроз. Например, в

Соединенных Штатах законы и положения о кибербезопасности применяются на федеральном уровне и уровне штатов. Ключевые федеральные законы, регулирующие кибербезопасность, включают Закон о компьютерном мошенничестве и злоупотреблениях (CFAA), Закон о конфиденциальности электронных коммуникаций (ECPA) и Закон об обмене информацией о кибербезопасности (CISA).

CFAA запрещает несанкционированный доступ к защищенным компьютерным системам, включая сети государственных и финансовых учреждений. ECPA регулирует перехват и раскрытие электронных сообщений, включая электронную почту и телефонные разговоры. CISA поощряет обмен информацией между частными и государственными организациями для предотвращения кибератак и реагирования на них. Существуют также законы и нормативные акты на уровне штатов, которые обеспечивают дополнительные рекомендации и защиту, например, законы об уведомлении об утечке данных.

Вопросы юрисдикции возникают при расследовании кибербезопасности, поскольку кибератаки часто происходят из разных частей мира. Киберпреступники могут скрывать свою личность и местонахождение, что затрудняет их отслеживание и судебное преследование. Это представляет собой проблему для правоохранительных органов, поскольку они должны работать с международными партнерами для расследования и судебного преследования киберпреступников.

Международное сотрудничество имеет решающее значение для смягчения киберугроз, поскольку киберпреступность является глобальной проблемой, требующей скоординированного реагирования. Конвенция Совета Европы о киберпреступности, также известная как Будапештская конвенция, представляет собой международный договор, направленный на гармонизацию законов о киберпреступности и содействие международному сотрудничеству в расследовании киберпреступлений. Конвенция ратифицирована более чем 60 странами и является ведущим международным документом по борьбе с киберпреступностью.

Защита частной жизни и гражданских свобод является важным аспектом усилий по обеспечению кибербезопасности. Хотя правоохранительные органы должны расследовать киберпреступников и преследовать их в судебном порядке, они

должны делать это таким образом, чтобы не нарушать права отдельных лиц. Одним из примеров защиты конфиденциальности является использование ордеров на обыск и конфискацию электронных устройств и данных. Для выдачи ордеров требуются достаточные основания, и они подлежат судебному пересмотру, чтобы гарантировать законность и соразмерность обысков и конфискаций.

Кроме того, меры кибербезопасности должны быть направлены на защиту частной жизни и гражданских свобод людей, а не на их нарушение. Например, технологии шифрования и анонимизации могут защитить конфиденциальность людей и гарантировать, что их личная информация не будет раскрыта в случае утечки данных. Правоохранительные органы должны уравновешивать потребность в эффективных мерах кибербезопасности с защитой частной жизни людей и гражданских свобод.

Образовательные и обучающие программы необходимы для улучшения знаний и навыков сотрудников правоохранительных органов в области кибербезопасности. Эти программы обеспечивают сотрудников правоохранительных органов навыками, необходимыми для расследования киберпреступлений и предотвращения кибератак. Образовательные и обучающие программы по кибербезопасности охватывают целый ряд тем, включая сетевую безопасность, цифровую криминалистику, реагирование на инциденты и анализ угроз.

Кампании по повышению осведомленности общественности важны для продвижения передового опыта в области кибербезопасности и повышения осведомленности о киберугрозах. Эти кампании обучают отдельных лиц и организации тому, как защитить себя от кибератак, таких как фишинг и вредоносное ПО. Кампании по информированию общественности также могут способствовать использованию надежных паролей, двухфакторной аутентификации и других мер безопасности для предотвращения несанкционированного доступа к личной и конфиденциальной информации.

Сотрудничество с сообществами и предприятиями имеет решающее значение для укрепления кибербезопасности. Правоохранительные органы могут сотрудничать с предприятиями для выявления и смягчения киберугроз. Кроме того, они могут

работать с группами сообщества, чтобы повышать осведомленность о киберугрозах и продвигать передовой опыт в области кибербезопасности. Это сотрудничество поможет выявить уязвимости и усилить меры кибербезопасности для предотвращения кибератак.

Правоохранительные органы должны быть готовы быстро и эффективно реагировать на киберинциденты, независимо от того, связаны ли они с атаками на государственные учреждения или организации частного сектора. Одним из ключевых компонентов эффективного реагирования на инциденты является разработка планов и протоколов реагирования на инциденты. Эти планы и протоколы содержат рекомендации для сотрудников правоохранительных органов о том, как реагировать на различные типы киберинцидентов, в том числе о том, как идентифицировать и локализовать инцидент, как сохранить доказательства и как координировать свои действия с другими агентствами и заинтересованными сторонами.

Кибер-инциденты часто требуют участия нескольких агентств и заинтересованных сторон, включая другие правоохранительные органы, государственные учреждения, организации частного сектора и международных партнеров. Эффективное реагирование на инциденты требует тесной координации и сотрудничества между этими организациями для обеспечения предотвращения инцидентов и смягчения их последствий. Правоохранительные органы должны установить четкую связь и сотрудничество с этими организациями для обеспечения скоординированного реагирования.

Своевременная и эффективная коммуникация имеет решающее значение для эффективного реагирования на инциденты. Правоохранительные органы должны иметь возможность быстро выявлять и оценивать киберугрозы и передавать эту информацию другим агентствам и заинтересованным сторонам. Для этого требуется надежная и безопасная коммуникационная инфраструктура, а также персонал, обученный обнаруживать киберугрозы и реагировать на них.

Быстрые темпы технологических изменений являются серьезной проблемой для правоохранительных органов, которым поручено устранять угрозы кибербезопасности. Новые технологии, такие как искусственный интеллект и Интернет вещей, создают

новые уязвимости и векторы атак, которые необходимо устранять. Правоохранительные органы должны быть в курсе этих изменений и постоянно адаптировать свои стратегии и тактики, чтобы опережать киберпреступников.

Постоянно развивающийся характер киберугроз требует от правоохранительных органов постоянной адаптации своих навыков и стратегий для эффективного реагирования на возникающие угрозы. Это включает в себя непрерывное образование и обучение сотрудников правоохранительных органов, чтобы держать их в курсе последних угроз и технологий, а также развитие партнерских отношений со специалистами по кибербезопасности для приобретения их специальных знаний и навыков.

Правоохранительные органы должны уравновешивать необходимость защиты от киберугроз с необходимостью защиты частной жизни и гражданских свобод отдельных лиц и организаций. Это требует осторожного и чуткого подхода к усилиям по обеспечению кибербезопасности, учитывающего потенциальное влияние на гражданские свободы и неприкосновенность частной жизни.

В последние годы было проведено много громких расследований киберпреступлений, которые завершились успешным судебным преследованием. Эти случаи подчеркивают важность эффективного сотрудничества между правоохранительными органами и экспертами по кибербезопасности в выявлении, отслеживании и задержании киберпреступников.

Сотрудничество между правоохранительными органами и специалистами по кибербезопасности имеет решающее значение для успеха многих расследований кибербезопасности. Работая вместе, специалисты правоохранительных органов и специалистов по кибербезопасности могут объединить свои ресурсы и опыт для более эффективного выявления киберугроз и реагирования на них.

Одним из примеров успешного сотрудничества является Киберцелевая группа ФБР, которая объединяет федеральные, государственные и местные правоохранительные органы и партнеров из частного сектора для расследования киберугроз. Оперативная группа сыграла важную роль в успешном расследовании и судебном преследовании многочисленных

высокопоставленных киберпреступников.

Другим примером является партнерство Киберкомандования США с фирмами по кибербезопасности частного сектора для выявления и устранения киберуязвимостей. Результатом сотрудничества стала разработка новых инновационных технологий и стратегий для обнаружения киберугроз и реагирования на них.

§ 5.2. Политики управления данными

Политика резервного копирования и восстановления.В современном деловом мире информация — это сила. Данные — это новая нефть 21 века. Чтобы сохранить свое конкурентное преимущество, у вас должна быть надежная политика резервного копирования и восстановления для вашего оборудования и программных приложений. Политика резервного копирования и восстановления играет важную роль в предотвращении потери или повреждения данных без предупреждения.

Политика резервного копирования и восстановления— это документ, в котором указывается, как выполняется резервное копирование данных, какие шаги предпринимаются для восстановления после аварии и кто имеет доступ к резервным копиям. Этот документ помогает предотвратить потерю и повреждение ваших ценных данных. Термин «резервная копия» может быть определен как копия данных, используемая для восстановления файлов или систем в случае их потери, удаления или повреждения. Эта копия может находиться на другом устройстве или носителе для защиты от физического повреждения исходного источника. В каждом бизнесе должна быть политика резервного копирования и восстановления. Существует множество причин, по которым ваши данные могут быть потеряны или недоступны, например, стихийные бедствия, сбой оборудования или человеческий фактор.

Существует два передовых метода хранения данных: один — на локальном сервере для быстрого восстановления, а другой — в облаке, где данные сохраняются в случае сбоя. Данные резервного копирования могут включать различные наборы данных, в том числе структурированные и неструктурированные данные, созданные приложениями электронной почты или используемые различными приложениями, включая базы данных. Политика резервного

копирования данных организации и политика хранения данных обычно дополняют друг друга.

Эффективная политика резервного копирования определяет данные для резервного копирования и частоту резервного копирования, а также место хранения, в которое отправляются резервные копии данных. В рекомендациях по резервному копированию также указана частота дополнительных резервных копий, которые ИТ-отдел будет выполнять после первоначальной полной резервной копии. Политика резервного копирования организации также определяет роли членов ИТ-группы, ответственных за резервное копирование, включая администратора резервного копирования, если эта роль является частью ИТ.

Вот некоторые из целей хорошей политики резервного копирования и восстановления:

— Определите, что необходимо вашему бизнесу для защиты данных с точки зрения аппаратного и программного обеспечения. Сюда входят резервные копии серверов, резервные копии виртуальных машин, настольных систем, мобильных устройств, серверов электронной почты и т. д.

— Вам нужно решить, как часто вы будете выполнять эти резервные копии и когда они будут сделаны. Это зависит от требований вашей компании, таких как соответствие нормативным требованиям или периоды устранения нарушений.

— В случае ошибок данные должны быть последовательно восстановлены с минимальной потерей обновленных данных.

— Резервное копирование данных должно быть как можно ближе к реальному времени. Частота резервного копирования должна зависеть от типа защищаемых данных.

— Резервные копии всегда должны иметь как минимум две копии — одну локальную и одну удаленную.

Существует множество политик резервного копирования, которые можно использовать для создания успешного плана резервного копирования (Рисунок 5.1):

Рисунок 5.1.Типы резервных копий

— **Политика внешнего резервного копирования:**Цель этого типа политики резервного копирования — хранить резервные копии в месте, отличном от того, где они были созданы. Он защищает от местных стихийных бедствий, таких как пожар или наводнение.

— **Политика пассивного резервного копирования:**Цель пассивной стратегии заключается в том, чтобы кто-то другой отвечал за резервное копирование ваших данных, пока вы сосредоточены на своих основных бизнес-целях.

— **Политика активного резервного копирования:**В соответствии с этой стратегией организации несут ответственность за регулярное создание и обслуживание собственных копий.

— **Зашифрованное резервное копирование:**Если у вашей компании есть данные о клиентах или другая конфиденциальная информация, которую необходимо защитить от несанкционированного доступа, вам нужна зашифрованная резервная копия.

— **Полная резервная копия**- Полная резервная копия создает резервную копию всего сервера, которая будет использоваться в течение более длительного периода времени.

— **Дополнительный резерв**- Это только резервирует то, что изменилось с момента последнего выполнения. Инкрементальные резервные копии фиксируют все файлы, которые были добавлены или изменены с момента последней полной резервной копии.

Вот преимущества политики резервного копирования и восстановления:

— Этот тип политики обеспечивает душевное спокойствие на случай, если что-то пойдет не так с вашими данными.

— Поскольку резервные копии доступны в любое время, вы можете быстро восстановиться после любой аварии.

— Внедрение строгой политики резервного копирования и восстановления может предотвратить простои, которые могут стоить тысячи долларов в час, если работа приходится на часы пик.

— Резервная копия также защищает от случайного удаления или повреждения, и если что-то случится с одним файлом в резервной копии, обычно доступно больше копий, из которых можно легко восстановить потерянные элементы.

— Политика резервного копирования определяет процедуры, расписания и обязанности, назначенные различным ресурсам для бесперебойного выполнения резервного копирования. Это также позволяет вам контролировать, когда может происходить резервное копирование, какие инструменты/программы следует использовать, а также расположение резервных копий.

— Эта политика определяет ресурсы, ответственные за создание резервных копий, и предоставляет их контактную информацию. Он также определяет, когда и где выполнять резервное копирование.

Для обеспечения безопасности данных также предоставляются следующие рекомендации по резервному копированию (Рисунок 5.2):

Рисунок 5.2.Практики резервного копирования.

— **Автоматическое резервное копирование**- этот тип резервного копирования практически не требует вмешательства человека для резервного копирования и сохранения данных из локальной системы в резервную копию. Благодаря автоматическому резервному копированию вам никогда не придется беспокоиться о резервном копировании данных вручную. Этот процесс защищает от человеческих ошибок и повреждения файлов. Это также снижает риск полного отказа системы.

— **Шифрование данных**- это защищает от несанкционированного доступа к данным со стороны хакеров или других злоумышленников, которые могут попытаться украсть личную информацию или интеллектуальную собственность из вашей сети, которая передается через Интернет или хранится на жестком диске вашего компьютера.

— **Облачное резервное копирование**- Облачное хранилище использует мощность интернет-соединения для резервного копирования всех ваших файлов и документов, чтобы к ним можно было получить доступ из любого места, где есть интернет-соединение. Это отличный способ обеспечить бесперебойную работу вашего бизнеса даже в случае непредвиденной катастрофы.

— **Сохранить акции-** Еще одна важная задача – как долго хранится каждый запас. Не желательно сохранять каждую резервную копию. Время хранения зависит от того, как часто вы выполняете резервное копирование данных, какой метод резервного копирования используется и где хранятся резервные копии.

— **Проводите регулярные тесты-** Тестирование плана восстановления улучшает процесс восстановления в случае непредвиденных проблем. Тестирование плана помогает организации узнать, что пошло не так, и они могут улучшить процесс восстановления, убедившись, что план работает должным образом.

— **Гибридные решения для резервного копирования данных-** это последняя инновация в мире резервного копирования, популярность которой растет, поскольку организации стремятся защитить свои данные от природных и техногенных катастроф. С помощью гибридного решения для резервного копирования вы можете хранить свои данные в безопасности и удаленно, не беспокоясь об уплате огромных ежемесячных платежей, таких как услуги облачного хранилища.

Политика классификации данных.*Политика классификации данных*представляет собой комплексный план классификации хранимых данных компании в соответствии с уровнем конфиденциальности, обеспечения надлежащей работы и снижения организационных рисков. Политики классификации данных выявляют и помогают защитить важные/конфиденциальные данные с помощью структуры правил, процессов и процедур для каждого класса.

Политика классификации данных классифицирует данные вашей компании на основе риска, который они представляют для вашей организации. С помощью этой политики компания определяет, как следует классифицировать данные на основе конфиденциальности, а затем создает политику безопасности, соответствующую каждому классу. Классификация данных обычно включает три категории: конфиденциальные, внутренние и общедоступные данные. Ограничение вашей политики несколькими простыми типами позволяет легко классифицировать все данные, которые есть в вашей организации, чтобы вы могли сосредоточить ресурсы на защите самых важных данных.

Преимущества политики классификации данных:

— Политика классификации данных помогает организации понять, какие данные можно использовать, где они существуют, где они расположены, какие уровни доступа, целостности и безопасности требуются, а также соответствуют ли текущие программы обработки и обработки применимым законам и правилам.

— Это наиболее эффективная и действенная система защиты данных, поскольку она помогает классифицировать данные для защиты важных, важных и конфиденциальных данных. Если конфиденциальная информация попадает в чужие руки, организации могут быть оштрафованы за нарушение законов и нормативных актов, они могут понести финансовые потери или репутационный ущерб.

— Политики классификации данных помогают организациям соответствовать нормативным требованиям, а также лучшим отраслевым практикам и ожиданиям клиентов.

— Это также помогает организациям оптимизировать свои выделенные средства безопасности, позволяя им определять, в какие меры безопасности следует инвестировать, исходя из объема конфиденциальных данных, которые им необходимо защитить, их местоположения и ландшафта угроз.

Существует три типа классификации данных:

Конфиденциальная информация

Относитесь к конфиденциальной информации как к драгоценности компании. Если она попадет из ваших рук, эта информация может нанести серьезный финансовый ущерб организации. Конфиденциальная информация включает почти все, что дает бизнесу стратегическое преимущество. Компании часто являются административными, физическимии используйте Конфиденциальную информацию в качестве основы для создания остальных технических средств контроля.

Внутренние данные

Инсайдерская информация — это информация, которая представляет умеренный риск или вред для компании в случае ее утечки. Этот список включает конфиденциальные учетные данные и другие секреты, а также корпоративные политики и другие рекомендации.

Общая информация

Сводная информация — это любая информация, включенная (или предназначенная) на ваш корпоративный веб-сайт. Как правило, раскрытие общедоступной информации не имеет последствий, поскольку она уже является общедоступной.

Для эффективной и успешной классификации данных необходимо выполнить следующую последовательность шагов (Рисунок 5.3):

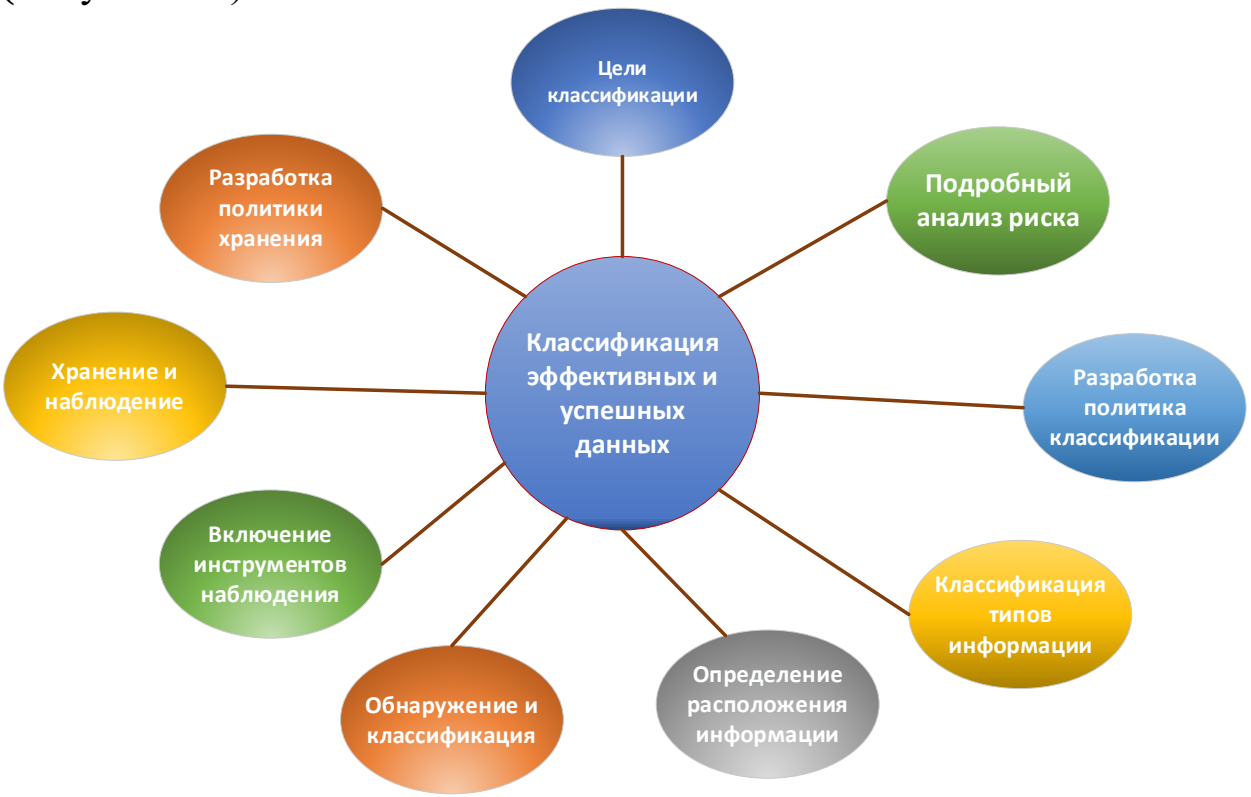


Рисунок 5.3.Последовательность классификации данных

1. Определение целей классификации;
2. Проведение анализа риска конфиденциальных данных;
   —низкий риск
   —умеренный риск
   —высокий риск
3. Разработка классификационной политики;
4. Классификация типов данных;
5. Определение местоположения данных;
6. Идентификация и классификация данных;
7. Включите устройства управления;
8. Поддерживать и контролировать политику классификации;
9. Создайте политику хранения.

Политика отмены и уничтожения данных.Политика

аннулирования и уничтожения данных — это набор процедур и руководств, описывающих, как организация должна безопасно удалять, уничтожать или избавляться от конфиденциальных данных, когда они больше не нужны. Политика должна охватывать данные, хранящиеся в физической и цифровой формах, включая бумажные записи, электронные файлы и устройства хранения, такие как жесткие диски, USB-накопители и мобильные устройства.

Целью этой политики является обеспечение надлежащего и безопасного удаления данных для защиты организации от утечек данных, несанкционированного доступа и потенциальной юридической ответственности.

Политика должна включать следующие компоненты:

1. *Объем:*Определите область действия политики, включая типы данных и устройств хранения, которые она охватывает.
2. *Обязанности:*Определите роли и обязанности персонала, участвующего в удалении и уничтожении данных.
3. *Процесс удаления данных:*Укажите процесс удаления данных, включая используемое программное и аппаратное обеспечение.
4. *Процесс удаления данных:*указать процесс физического уничтожения или утилизации устройств хранения, включая используемые методы и средства.
5. *Проверять:*Добавьте шаг проверки, чтобы убедиться, что данные были успешно удалены или уничтожены.
6. *Исключения:*Определите любые исключения из политики, такие как информация, которая должна храниться по закону в течение определенного периода времени.
7. *Обучение:*Обучите персонал, занимающийся удалением и уничтожением данных, в том числе о важности соблюдения политики.
8. *Право на участие:*Создайте систему для мониторинга соблюдения политики, включая последствия несоблюдения.

В целом, комплексная политика удаления и уничтожения данных необходима для обеспечения безопасного и надлежащего удаления конфиденциальных данных, минимизации риска утечки данных и юридической ответственности организации.

Пример дополнительной политики удаления данных:

*Цель:*Целью этой политики является защита

конфиденциальности, целостности и доступности информации, а также обеспечение безопасного и надлежащего уничтожения конфиденциальной информации, когда в ней больше нет необходимости для соблюдения законодательных и нормативных требований.

*Объем:*Эта политика распространяется на всех сотрудников, подрядчиков и сторонних поставщиков, которые имеют доступ или несут ответственность за хранение и обработку конфиденциальной информации, а также на все устройства хранения, включая, помимо прочего, жесткие диски компьютеров. жесткие диски. диски, USB-накопители, компакт-диски, DVD-диски и резервные ленты, содержащие конфиденциальную информацию.

Политика:

1. *Классификация данных:*Все данные следует классифицировать на основе чувствительности и уровня риска, связанного с потерей или разоблачением. Классификация должна определять соответствующий уровень защиты и метод утилизации.

2. *Хранилище данных:*Конфиденциальную информацию следует хранить только столько времени, сколько необходимо, и немедленно уничтожать, когда она больше не нужна.

3. *Способы уничтожения данных:*Все конфиденциальные данные должны быть уничтожены с использованием соответствующих методов для предотвращения несанкционированного доступа или восстановления. Можно использовать следующие методы:

— Физическое уничтожение. Физическое уничтожение устройств хранения — наиболее безопасный метод уничтожения данных. Это включает в себя измельчение, дегазацию или измельчение жестких дисков или других носителей информации.

— Перезапись. Перезапись — это метод уничтожения данных, который включает запись новых данных поверх существующих данных на устройстве хранения. Этот метод можно использовать для жестких дисков, USB-накопителей и других записывающих устройств хранения. Необходимо выполнить не менее трех перезаписей с использованием программного средства, одобренного организацией.

— Криптографическое стирание. Криптографическое стирание — это метод уничтожения данных, который включает

шифрование данных на устройстве хранения с использованием проверенного алгоритма шифрования, а затем уничтожение ключей шифрования. Этот метод можно использовать для жестких дисков, USB-накопителей и других устройств хранения данных, поддерживающих шифрование.

4. *Процедуры уничтожения данных:*Все сотрудники, подрядчики и сторонние поставщики должны следовать утвержденным в организации процедурам уничтожения данных при уничтожении конфиденциальной информации и устройств хранения. Процедуры должны включать рекомендации по идентификации и классификации конфиденциальных данных, определению соответствующего метода удаления и документированию процесса удаления.

5. *Проверка и документация:*Любое уничтожение данных должно быть проверено и задокументировано, чтобы гарантировать, что данные уничтожены должным образом. Документация должна включать тип уничтожаемой информации, дату уничтожения, использованный метод уничтожения и имя лица, осуществившего уничтожение.

6. *Право на участие:*На эту политику распространяются законодательные и нормативные требования, и удаление всех данных должно осуществляться в соответствии с этими требованиями.

Правоприменение: Любой сотрудник, подрядчик или сторонний поставщик, нарушающий эту политику, может быть подвергнут дисциплинарному взысканию вплоть до увольнения или увольнения.

§ 5.3 Политика использования систем

Политика использования информационных систем определяет правила допустимого использования информационных систем организации для защиты организации и ее сотрудников от злонамеренных действий. Настоящая политика распространяется на всех пользователей информационных систем в той мере, в какой это разрешено применимым законодательством.

Пользователи должны использовать информационные системы в соответствии со следующими политиками.

Рисунок 5.4. Политика использования систем

Запись и мониторинг процессов.Журналы аудита, в которых регистрируются ошибки и другие события, связанные с безопасностью, должны быть подготовлены и храниться в течение определенного периода времени, чтобы помочь в последующих аудитах и мониторинге контроля доступа. Журналы аудита включают:

(A) идентификаторы пользователей;

(B) даты и время входа и выхода, идентификатор терминала или местоположение;

(D) записи об успешных и отклоненных попытках входа в систему;

(E) записи об успешных и отклоненных попытках доступа к данным и другим ресурсам.

Некоторые журналы аудита необходимо архивировать в рамках процедур ведения записей или в соответствии с требованиями по сбору доказательств.

Должен быть установлен порядок контроля за использованием средств обработки информации и регулярно пересматриваться результаты контрольной деятельности. Такие процедуры необходимы для обеспечения того, чтобы пользователи выполняли только те действия, которые специально разрешены. Уровень мониторинга, требуемый для отдельных объектов, следует определять посредством оценки рисков. Области, которые следует

учитывать, включают:

(A) Разрешенный доступ, включая:

(i) идентификатор пользователя;

(ii) дату и время основных событий;

(iii) типы событий;

(iv) используемые файлы;

(v) используемое программное обеспечение/утилиты.

(B) Все льготные сделки, такие как:

(i) с использованием учетной записи контроллера;

(ii) запуск и остановка системы;

(iii) подключить/отключить устройство ввода-вывода.

(C) Попытки несанкционированного доступа, такие как:

(i) неудачные попытки;

(ii) нарушение процедур доступа и уведомлений для сетевых шлюзов и брандмауэров;

(iii) оповещения от собственных систем обнаружения вторжений.

(D) Системные предупреждения или неисправности, такие как:

(i) предупреждения или сообщения консоли;

(ii) исключения системного журнала;

(iii) сигналы управления сетью.

Использование персонального компьютера.Компьютеры организации предоставляются людям, которые работают в этой организации. Всем пользователям предоставляется доступ к компьютерам для выполнения рабочих задач. Вся деятельность должна соответствовать политикам и законам организации, регулирующим использование и передачу информации, и несоблюдение этих требований приведет к потере доступа и может привести к дисциплинарным взысканиям в отношении сотрудников, включая увольнение.

Политика кибербезопасности использования компьютера запрещает использование его ресурсов для:

(A) Отправка электронной почты с использованием чужого имени (подмена электронной почты).

(B) предпринимать какие-либо действия, заведомо препятствующие нормальной работе сети, ее систем, периферийных устройств и/или доступу к внешним сетям.

(C) Установка любой системы или программного обеспечения

в сети без предварительного разрешения.

(D) Устанавливать любые программные системы или аппаратные средства, которые намеренно устанавливают вирус, троянскую программу, червя или другой известный или неизвестный вредоносный механизм.

(E) Попытка изменить IP-адрес.

(F) пытаться загружать, публиковать или распространять материалы, защищенные авторским правом, без разрешения.

(G) Попытка загрузить программное обеспечение из Интернета без разрешения.

(H) Публикация личных комментариев или утверждений по ошибке.

(i) получать доступ, создавать, передавать (отправлять или получать), публиковать или загружать материалы, которые являются дискриминационными, клеветническими, непристойными, сексуальными, оскорбительными или преследующими по признаку пола, расы, религии, национального происхождения, возраста, инвалидности, медицинского статуса, сексуальная ориентация или защищены законами штата и местными законами и т. д.

Физическая охрана.Организация отвечает за документирование, реализацию, мониторинг и тестирование плана физической безопасности компьютерных и телекоммуникационных активов. Этот план физической безопасности оценивает риск потенциальных потерь из-за:

(A) физическое уничтожение или кража физических активов;

(B) потеря или уничтожение данных и программных файлов;

(C) кража данных;

(D) косвенное хищение активов;

(E) ЗАДЕРЖКА ИЛИ ВМЕШАТЕЛЬСТВО В КОМПЬЮТЕРНУЮ ОБРАБОТКУ.

План будет включать меры по снижению вероятности убытков и должен быть сосредоточен на:

(A) изменения в окружающей среде для уменьшения воздействия;

(B) меры по снижению угрозы;

(C) улучшенные процедуры контроля;

(D) раннее обнаружение;

(E) планы на случай непредвиденных обстоятельств.

Доступ к системам и мониторинг их использования.Системы должны контролироваться для обнаружения отклонений от процедур доступа и регистрировать системные события для предоставления доказательств в случае нарушений безопасности. Мониторинг системы позволяет проверить эффективность средств контроля.

Журналы аудита, документирующие ошибки и другие инциденты, связанные с безопасностью, должны быть подготовлены и поддерживаться организацией в течение установленного срока и установленных законом полномочий, чтобы помочь в будущих аудитах и мониторинге контроля доступа. Журналы аудита также должны включать:

(A) идентификаторы пользователей;

(B) даты и время входа и выхода, идентификатор терминала или местоположение;

(D) записи об успешных и отклоненных попытках входа в систему;

(E) записи об успешных и отклоненных попытках доступа к данным и другим ресурсам.

Некоторые журналы аудита могут потребоваться для архивирования в рамках ведения записей.

Должен быть установлен порядок контроля за использованием средств обработки информации и регулярно пересматриваться результаты контрольной деятельности. Такие процедуры необходимы для обеспечения того, чтобы пользователи выполняли только четко разрешенные действия. Уровень мониторинга, требуемый для отдельных объектов, следует определять посредством оценки риска. Области, подлежащие мониторингу:

(A) санкционированный доступ, в том числе:

(i) идентификатор пользователя;

(ii) дату и время основных событий;

(iii) типы событий;

(iv) используемые файлы;

(v) используемое программное обеспечение/утилиты.

(B) все льготные операции, такие как:

(i) с использованием учетной записи контроллера;

(ii) запуск и остановка системы;

(iii) подключить/отключить устройство ввода-вывода.

(C) попытки несанкционированного доступа, такие как:

(i) неудачные попытки;

(ii) нарушение процедур доступа и уведомлений для сетевых шлюзов и брандмауэров;

(iii) оповещения от собственных систем обнаружения вторжений.

(D) системные предупреждения или неисправности, такие как:

(i) предупреждения или сообщения консоли;

(ii) исключения системного журнала;

(iii) сигналы управления сетью.

Результаты деятельности по мониторингу должны регулярно пересматриваться. Частота проверок должна зависеть от риска. Факторы риска, которые следует учитывать, включают:

(A) важность программных процессов;

(B) ценность, конфиденциальность или критичность соответствующей информации;

(C) прошлый опыт доступа и неправомерного использования;

(D) степень взаимосвязанности системы.

Просмотр журнала включает в себя понимание угроз, с которыми сталкивается система, и того, как они возникают. Системные журналы часто содержат большое количество информации, большая часть которой не относится к мониторингу безопасности. Следует уделить внимание автоматическому копированию соответствующих типов сообщений во второй журнал и/или использованию соответствующих системных утилит или инструментов аудита для анализа файлов с целью определения критических событий для целей мониторинга безопасности. Следует уделить внимание распределению ролей между лицом (лицами), ответственными за просмотр журнала, и лицами, за которыми ведется наблюдение.

Особое внимание следует уделить безопасности дерева событий, так как при его изменении может появиться некорректная система безопасности. Средства контроля должны быть направлены на защиту от несанкционированных изменений и операционных проблем, в том числе:

(A) записывающее устройство отключено;

(B) вносить изменения в типы записанных сообщений;

(C) файлы журнала редактируются или удаляются, а носитель

файла журнала прекращается;

(D) файл журнала, который перезаписывает сами события.

Оперативное программное управление.Контроль должен применяться к реализации программного обеспечения в операционных системах. Для минимизации программных рисков в операционных системах следует учитывать следующие элементы управления:

(A) Обновления операционных библиотек программного обеспечения должны выполняться только назначенными источниками с соответствующего разрешения руководства.

(B) Операционные системы должны хранить только исполняемый код.

(C) Исполняемый код не должен выполняться в операционной системе до тех пор, пока не будут получены доказательства успешного тестирования и одобрения пользователем, а соответствующие исходные библиотеки приложения не будут обновлены.

(D) Должен вестись журнал аудита всех обновлений библиотек операционных программ.

(E) Предыдущие версии Программного обеспечения должны быть сохранены на случай непредвиденных обстоятельств.

Программное обеспечение, используемое в операционных системах, должно учитывать безопасность любого решения об обновлении до новой версии, то есть введение новых функций безопасности или количество и серьезность проблем безопасности, затрагивающих эту версию. Программное обеспечение должно использоваться, чтобы помочь устранить или уменьшить недостатки безопасности.

Контрольные вопросы.

1. Что такое сетевая криминалистика и какие задачи она решает? Приведите примеры сетевых доказательств и методов анализа.

2. Знаете ли вы основные типы вредоносных программ? Какие инструменты и методы используются для анализа вредоносных программ?

3. Что такое социальная инженерия и как ее используют киберпреступники? Какие способы защиты от социальной инженерии вы можете предложить? Приведите примеры успешных

или неудачных атак социальной инженерии.

4. Что такое криптография и как она связана с киберпреступностью? Какие виды шифрования вы знаете?

5. Каковы характеристики цифровых доказательств по сравнению с вещественными доказательствами?

6. Каковы юридические требования для получения цифровых доказательств?

7. Какие проблемы возникают при работе с международными партнерами по кибербезопасности?

8. Какие законы и правила регулируют кибербезопасность в вашей стране?

9. Кто несет ответственность за удаление и уничтожение данных в соответствии с Политикой?

10. Какие программные и аппаратные средства используются для стирания данных с запоминающих устройств?

11. Какие методы и средства используются для уничтожения накопителей?

13. Как проверяется успешность удаления или уничтожения данных?

14. Каковы исключения из политики в отношении информации, хранение которой требуется по закону?

15. Как сотрудников обучают удалять и уничтожать данные?

16. Как обеспечивается соблюдение политики и каковы последствия нарушения?

ГЛАВА VI. ИНФОРМАЦИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

§ 6.1. Ресурсы по технологиям безопасности

Кибербезопасность является важным вопросом как для ИТ-отделов, так и для руководителей. Безопасность должна беспокоить не только ИТ-специалистов и менеджеров, но и каждого сотрудника организации. Одним из эффективных способов разъяснить сотрудникам важность безопасности является наличие политики кибербезопасности, в которой объясняются обязанности каждого человека по защите ИТ-систем и данных. Политика кибербезопасности устанавливает стандарты поведения для таких вещей, как ограничение электронной почты, шифрование данных и использование социальных сетей. Как правило, в первом разделе политики кибербезопасности описываются общие ожидания, роли и обязанности в организации в отношении безопасности. Для крупных организаций или регулируемых отраслей политики кибербезопасности часто занимают десятки страниц. Однако для небольших организаций политика безопасности может состоять из нескольких страниц и охватывать основные методы обеспечения безопасности. Такие практики могут включать:

1. Правила использования шифрования электронной почты.
2. Шаги для удаленного доступа к рабочим приложениям.
3. Инструкции по созданию и защите паролей.
4. Условия использования социальных сетей.

Антивредоносная политика.Четко определенные и проверенные планы и процедуры принимаются и соблюдаются для обеспечения достижения целей и непрерывности бизнеса. Он обеспечивает защиту активов информационных технологий от вредоносных программ и вирусных атак. ИТ-активы защищены за счет обеспечения устойчивости к атакам вирусов и вредоносных программ. Все превентивные и защитные меры для противодействия таким атакам определены в политике защиты от вредоносных программ, которая включает следующее.

Целью этой политики является поощрение использования антивирусных и антивирусных средств. Цель состоит в том, чтобы обучить пользователей часто используемым политикам для эффективного использования средств защиты от вредоносных программ. Эта политика содержит рекомендации по обеспечению

соблюдения законодательства.

Для предотвращения проблем с вредоносными программами/вирусами используются следующие специальные методы:

1. На всех рабочих станциях, будь то сетевые или автономные, должно использоваться утвержденное антивирусное и антивредоносное программное обеспечение и конфигурация.

2. Не отключайте и не обходите антивирусные и антивирусные программы.

3. Настройки антивирусного и антивредоносного программного обеспечения не должны изменяться таким образом, чтобы это снижало эффективность программного обеспечения.

4. Не следует изменять частоту автоматического обновления антивирусных и антивредоносных программ для уменьшения частоты обновлений.

5. Каждый файловый сервер, подключенный к сети, должен использовать утвержденное антивирусное и антивредоносное программное обеспечение и настроить обнаружение и очистку вредоносных программ, которые могут заражать файловые обмены.

6. Каждый вирус или вредоносное ПО, которые не удаляются автоматически антивирусным и антивредоносным программным обеспечением, должен вызывать инцидент безопасности.

7. Организация принимает соответствующие меры для предотвращения и обнаружения внедрения вредоносного кода и несанкционированного мобильного кода.

8. Информационная система автоматически обновляет механизмы защиты от вредоносных кодов. Например, автоматические обновления антивирусных и антивредоносных программ.

9. Каждый шлюз электронной почты использует утвержденное антивирусное программное обеспечение для электронной почты и следует передовым отраслевым практикам по настройке и использованию такого программного обеспечения.

10. Следует проводить периодические оценки систем, которые, как считается, не подвержены влиянию вредоносного кода или программного обеспечения. Это необходимо для понимания и оценки развивающихся угроз вредоносных программ, чтобы подтвердить, что системам не требуется антивирусное программное

обеспечение.

Любой сотрудник, уличенный в нарушении этой политики, может быть подвергнут дисциплинарному взысканию в соответствии с кадровой политикой.

Электронная почта и сообщения.Электронная почта компании всегда была открыта. Обмен данными между двумя почтовыми серверами показан на рисунке 6.1. Пример обмена данными между двумя почтовыми серверами имеет текстовый контент, и аутентификация не требуется. Протокол позволяет вам вводить информацию в командной строке, поэтому вам даже не нужно иметь программное обеспечение почтового сервера, чтобы подделать почтовый сервер, использующий этот протокол. Хотя некоторые серверы могут потребовать от вас предоставления ключа для аутентификации или ограничения подключений к предварительно определенному IP-адресу, если какой-либо сервер в ретрансляторе электронной почты между отправителем и получателем может отправлять только текстовые сообщения, как показано на рис., если он поддерживает командную строку на основе

```
$ telnet mail.company.com 25
Trying 192.168.142.13
Connected to mail.company.com.
Escape character is '^]'.
220 mail
SMTP/smap Ready.
helo
250 Charmed, I'm sure.
mail from:spoofvictim@anothercompany.com
250 <spoofvictim@anothercompany.com>...
Sender Ok
rcpt to: unsuspecting@company.com
250 unsuspecting@company.com
OK
Data
354 Enter mail, end with "." on a line by itself
malicious message text goes here.
250 Mail
Accepted
quit
221 Closing connection
Connection closed by foreign host.
$
```

Рисунок 6.1. Пример протокола связи с почтовым сервером

Рекламодатели пользуются преимуществами открытости подключений к серверам электронной почты, поскольку они могут идентифицировать клиентов с помощью этих открытых протоколов.

Например, если сервер электронной почты компании отвечает на команды, подобные показанной на рис. 1, автоматизированная программа рекламодателя может попытаться отправить электронное письмо и, в конечном итоге, разослать его всем пользователям. При возникновении ошибок они просто прекращают попытки и переходят к следующему отгадыванию по имени. Когда рекламодатели отправляют сообщения электронной почты большому количеству потенциальных клиентов, не различая, какие потенциальные клиенты заинтересованы в их продукте, это называется спамом. На заре Интернета пользователи использовали слово «спам» для описания содержимого, которое они не хотели видеть. Термин «спам» теперь обычно относится к любому нежелательному содержимому электронной почты. Доступ к электронной почте называется фишингом и включает в себя приманку или побуждение пользователей Интернета переходить по ссылкам, ведущим на вредоносные веб-сайты. Вредоносными сайтами могут быть сайты, собирающие имена пользователей и пароли. Они могут загружать вредоносное ПО, использовать мошенничество, чтобы обманом заставить пользователей переводить деньги с их банковских счетов. Технологии обмена сообщениями основаны на протоколах между отправителем и получателем, которые редко аутентифицируются. но просто идентифицирует отправителя с помощью строки «имя пользователя», предоставляемой как часть потока сообщений. Перечисленные политики кибербезопасности для электронной почты и обмена сообщениями начинаются с общих требований к электронной почте. Политика должна решать более системные проблемы, связанные со спамом и ответственностью в целом. (таблица 6.1).

Таблица 6.1

Вопросы политики кибербезопасности, связанные с электронной почтой и обменом сообщениями

Политика	Заявление	Причины конфликта
Все организации, участвующие в электронной коммерции, должны предлагать	Эта политика требует, чтобы компании электронной коммерции	Потребители имеют право убедиться, что сообщения от поставщиков услуг и других лиц не

клиентам возможность проверки серверов электронной почты с использованием стандартных протоколов.	публиковали ключи для своих почтовых серверов в DNS.	являются мошенническими. У потребителей обычно нет программного обеспечения для проверки почтового сервера, и поэтому они должны полагаться на своих поставщиков услуг хостинга для проверки подлинности электронной почты.
Все сообщения электронной почты от имени организации или о ней должны использовать службы электронной почты, поддерживаемые организацией.	Это требование, чтобы люди использовали системы электронной почты своей организации и воздерживались от использования сайтов социальных сетей, личных мобильных телефонов и других общедоступных или частных коммуникационных услуг для ведения бизнеса организации.	Эта политика поддерживает структуру контроля управления для всех коммуникаций. Это сводит к минимуму количество людей, имеющих административный доступ к внутренним администраторам персонала. Эта политика ограничивает возможности связи для лиц, которые не могут подключиться к корпоративным службам из-за сбоев.
Уведомление о прочтении, отправленное по	Различные договорные и нормативные	Возможность использовать электронную доставку

электронной почте, должно быть доказательством доставки электронной информации.	положения требуют от организаций, направляющих уведомления, доказать, что лицо, которому было отправлено уведомление, действительно его получило.	и квитанции о прочтении в качестве подтверждения доставки снизит расходы организаций, несущих юридическую ответственность за уведомление физических лиц в различных отраслях, от банковского дела и страхования до правоохранительных органов. Текущие стандарты аутентификации цифровых записей требуют сочетания доказательств управления ключами, криптографических алгоритмов и процедур организационного контроля.
Люди должны иметь возможность внести свой адрес электронной почты в список, который запрещает маркетологам отправлять им нежелательную электронную почту.	Это эквивалент национального реестра запрета звонков для запросов по электронной почте. Этот тип списка в настоящее время используется для телефонных номеров.	Для защиты адресов электронной почты от нежелательных запросов существенно сокращается механизм применения политики «не отправлять по электронной почте». Количество спам-объявлений, полученных в настоящее время по

		электронной почте. Эта политика должна упростить обнаружение незаконного спама. Принудительное применение политик экономит пропускную способность и ресурсы хранения за счет уменьшения количества нежелательных сообщений.
Пользователи служб обмена сообщениями должны использовать только зарегистрированные доменные имена в Интернете.	Это эквивалент отдельного «белого списка» для каждого потенциального получателя электронной почты. только те, кто в списке, смогут отправить электронное письмо или сообщение получателю.	Эта политика позволяет пользователям Интернета управлять своими ресурсами и сокращать количество спам-сообщений. Это экономит как пропускную способность, так и ресурсы хранения. Поскольку не существует общепринятого метода проверки подлинности для электронной почты или обмена сообщениями, любой может обойти эту политику, указав любое имя пользователя в белом списке.
Известные	Эта политика	Отправители

отправители фишинговых сообщений электронной почты будут привлечены к ответственности, а наказания должны быть соразмерны преступлениям, совершенным в результате возможной кражи данных у получателей фишинговых сообщений.	налагает штраф за кражу личных данных на тех, кто отправляет фишинговые электронные письма.	фишинговых электронных писем составляют небольшую часть крупного организованного преступного сообщества. Это необходимое условие более крупного преднамеренного нападения на человека, и к нему следует относиться так же серьезно, как и к самому нападению. Отправитель фишинговой электронной почты, вероятно, является бизнесом, который рассылает массовые электронные письма разным клиентам. Кроме того, простая отправка электронного письма не гарантирует взаимодействия с пользователем.

Шифрование.Шифрование следует использовать для защиты конфиденциальности конфиденциальных данных. На основании оценки рисков определяется требуемый уровень защиты с учетом типа используемого алгоритма шифрования и длины используемых криптографических ключей.

Следует обратиться за советом к эксперту, чтобы определить надлежащий уровень защиты, выбрать подходящие продукты, обеспечивающие требуемую защиту, и внедрить безопасную систему управления ключами. Кроме того, следует запросить

юридическую консультацию относительно законов и нормативных актов, которые могут применяться к предполагаемому использованию организацией шифрования.

Должны быть разработаны и соблюдены процедуры использования криптографических средств защиты информации. Такие процедуры необходимы для максимизации преимуществ криптографических методов, минимизации рисков и недопущения неправильного использования.

При разработке процедур необходимо учитывать следующее:

(A) руководства по использованию средств криптографического контроля во всей организации;

(B) содержит общие принципы защиты деловой информации;

(C) подход к управлению ключами, включая методы восстановления зашифрованных данных в случае потери, компрометации или компрометации ключей;

(D) роли и обязанности, например, кто отвечает за: выполнение процедур; базовое управление;

(E) как определить соответствующий уровень криптографической защиты;

(F) стандарты, которые необходимо принять для эффективного внедрения в организации (какое решение используется для каких бизнес-процессов).

Интернет- и интранет-безопасность.Интернет можно разделить на два основных компонента: приложения, предоставляющие информацию через Интернет, и веб-серверы, представляющие собой веб-браузеры (клиенты), используемые для доступа. Веб-сервер является наиболее целевым и атакуемым узлом в сетях большинства организаций. Вот почему так важно защищать веб-серверы и сетевую инфраструктуру, которая их поддерживает.

Угрозы безопасности, характерные для веб-серверов, обычно относятся к одной из следующих категорий:

(A) Злоумышленники могут использовать программные ошибки на веб-сервере, базовой операционной системе или активном содержимом для получения несанкционированного доступа к веб-серверу. Примеры несанкционированного доступа включают доступ к файлам или папкам, не предназначенным для публичного использования, или выполнение привилегированных команд и установку программного обеспечения на веб-сервере.

(B) Атаки типа «отказ в обслуживании» направлены на веб-сервер, лишая настоящих пользователей доступа к веб-серверу во время атаки.

(C) Конфиденциальная информация на веб-сервере может быть передана неуполномоченным лицам.

(D) Незашифрованная конфиденциальная информация может быть перехвачена при передаче между веб-сервером и браузером.

(E) Информация на веб-сервере может быть изменена. Взлом веб-сайта является распространенным примером этой угрозы.

(F) Злоумышленники могут получить несанкционированный доступ к ресурсам в компьютерной сети другой организации, успешно атаковав веб-сервер.

(G) Злоумышленники могут атаковать внешние организации с скомпрометированного веб-сервера, скрывать свою истинную личность и возлагать на организацию, запустившую атаку, ответственность за ущерб.

(H) Сервер может использоваться в качестве точки распространения незаконных копий программных инструментов для атак или порнографии, что может повлечь за собой ответственность организации за ущерб.

Среду брандмауэра следует использовать для выполнения следующих общих функций:

(A) фильтрация пакетов и протоколов;

(Б) проверьте соединения;

(C) выполнять прокси или выбранные приложения;

(D) контролировать трафик, разрешенный или запрещенный брандмауэром.

Сеть.Небезопасные подключения к сетевым службам могут повлиять на всю организацию. Пользователи должны использовать только те Услуги, на использование которых они специально уполномочены. Этот контроль особенно важен для критически важных бизнес-приложений или сетевых подключений к пользователям в местах с высоким уровнем риска в общедоступных или внешних областях, которые находятся за пределами управления и контроля безопасности организации.

Процедуры использования сетей и сетевых услуг должны охватывать:

(A) сети и сетевые службы, к которым разрешен доступ;

(B) процедуры авторизации для определения того, кто имеет право доступа к тем или иным сетям и сетевым службам;

(C) средства управления и процедуры для защиты сетевых подключений и доступа к сетевым службам.

Путь от пользовательского терминала до компьютерной службы должен контролироваться. Сети предназначены для обеспечения максимальной пропускной способности для совместного использования ресурсов и гибкости маршрутизации. Эти функции также могут разрешать несанкционированный доступ к бизнес-приложениям или несанкционированный доступ к мультимедиа. Введение элементов управления, которые ограничивают маршрут между пользовательским терминалом и компьютерными службами, к которым имеет доступ его пользователь, например, создание принудительного пути, может снизить такие риски.

Для ограничения маршрута следует использовать следующие методы:

(A) выделять выделенные линии или телефонные номера;

(B) автоматически подключать порты к назначенным системам приложений или шлюзам безопасности;

(C) ограничить меню и подменю отдельными пользователями;

(D) предотвратить неограниченный сетевой роуминг;

(E) предоставлять доступ к назначенным системам приложений и шлюзам безопасности для пользователей внешней сети;

(F) шлюзы безопасности, такие как брандмауэры;

(G) ограничить доступ к сети путем создания отдельных логических доменов, таких как виртуальные частные сети, для групп пользователей внутри организации.

Внешние подключения обеспечивают несанкционированный доступ к бизнес-информации, например доступ по телефонной линии. Поэтому доступ удаленных пользователей должен быть аутентифицирован. Существуют различные типы методов аутентификации, некоторые из которых обеспечивают более высокий уровень защиты, чем другие, например, методы, основанные на использовании криптографических методов, обеспечивают надежную аутентификацию.

(A) Аутентификация удаленных пользователей должна быть достигнута с использованием одного из следующих методов:

(B) методы, основанные на криптографии;

(C) аппаратные токены;

(D) протокол возражения/ответа;

(E) проверка адреса выделенной частной линии или пользователя сети.

Сети все больше выходят за рамки традиционных организационных границ по мере того, как формируются деловые партнерства, которые могут потребовать взаимосвязи или совместного использования средств обработки информации и сетевых инструментов. Такие расширения увеличивают риск несанкционированного доступа к существующим информационным системам, использующим сеть, некоторые из которых могут потребовать защиты от других пользователей сети из-за их чувствительности или важности. В таких условиях должны быть введены средства контроля для отдельных групп информационных сервисов, пользователей и информационных систем в сетях.

Безопасность больших сетей следует контролировать, разделяя их на отдельные логические сетевые домены, такие как внутренние сетевые домены организации и внешние сетевые домены, каждый из которых защищен определенным периметром безопасности. Такой периметр должен быть реализован путем создания безопасного шлюза между двумя сетями, которые должны быть взаимосвязаны для контроля доступа и потока информации между двумя доменами. Этот шлюз должен быть настроен для фильтрации трафика между этими доменами и блокировки несанкционированного доступа в соответствии с процедурами управления доступом организации. Пример такого типа шлюза обычно называют брандмауэром. Критерии деления сетей на домены должны основываться на процедурах управления доступом и требованиях к доступу, а также

В общедоступных сетях возможности подключения пользователей должны быть ограничены в соответствии с процедурами контроля доступа.

Такие элементы управления должны быть реализованы через сетевые шлюзы, фильтрующие трафик с помощью предопределенных расписаний или правил. Применяемые ограничения должны основываться на требованиях процедур доступа и бизнес-приложений и должны поддерживаться и обновляться соответствующим образом. Примеры приложений, в

которых должны применяться ограничения:

А) электронная почта;

(В) односторонняя передача файлов;

(С) двусторонняя передача файлов;

(D) интерактивный доступ;

(Е) доступ к сети, связанный с датой или временем суток.

Общедоступные сети должны иметь элементы управления маршрутизацией, чтобы гарантировать, что компьютерные соединения и информационные потоки не нарушают процедуры управления доступом бизнес-приложений. Этот элемент управления необходим для сетей, совместно используемых сторонними (неорганизационными) пользователями.

Мобильные вычисления.Должны существовать формальные процедуры и должны быть приняты соответствующие средства контроля для защиты от рисков, связанных с мобильными компьютерами, особенно при работе в незащищенной среде. Например, такие процедуры должны включать следующие требования:

(А) физическая защита;

(В) контроль доступа;

(С) криптографические методы;

(Г) резервные копии;

(Е) защита от вирусов.

Процедуры также должны включать правила и рекомендации по подключению мобильных устройств к сетям и рекомендации по использованию этих средств в общественных местах.

Необходимо соблюдать осторожность при использовании портативных вычислительных устройств в общественных местах, конференц-залах и других незащищенных местах за пределами организации. Данные, хранящиеся и обрабатываемые этими устройствами, должны быть защищены от несанкционированного доступа или раскрытия, например, с использованием криптографических методов.

Удаленный доступ к бизнес-данным через общедоступную сеть с использованием мобильных вычислительных устройств должен осуществляться только после успешной идентификации и аутентификации, а также при наличии соответствующих механизмов контроля доступа.

Мобильные вычислительные устройства также должны быть физически защищены от кражи, особенно когда они оставлены в автомобилях и других видах транспорта, гостиничных номерах, конференц-центрах и местах встреч. Оборудование, несущее важные данные, нельзя оставлять без присмотра и по возможности использовать специальные замки для защиты оборудования.

§ 6.2. Инструменты кибербезопасности

В современном мире злоумышленники внедряют новые технологии и инструменты, которые можно использовать для кражи данных у пользователей с помощью цифровых средств, а не традиционных или старых методов кражи данных у пользователей. При этом кибер-злоумышленники пытаются проникнуть в сеть и атаковать, в то время как кибер-защитники блокируют или не позволяют злоумышленникам получить доступ к данным. Однако эти сражения не в физическом режиме, они используют различные лучшие инструменты кибербезопасности для атаки и защиты. Один и тот же инструмент можно использовать как в положительном, так и в отрицательном режиме. Все зависит от ума и цели человека, использующего инструмент. На киберрынке существует множество инструментов с открытым исходным кодом по нескольким причинам.

В кибербезопасности существует множество инструментов, основанных на конкретных областях.

Ниже приведены типы инструментов кибербезопасности.

— Информация о безопасности и средства управления инцидентами;
— Инструменты оценки уязвимости;
— Инструменты цифровой криминалистики;
— Инструменты для тестирования на проникновение;
— инструменты брандмауэра;
— инструменты IDS/IPS;
— Управление привилегированным доступом;
— Инструменты обнаружения и реагирования конечных точек;
— Сетевые средства обнаружения и реагирования;
— Инструменты безопасности электронной почты;
— Инструменты предотвращения потери данных.

К современным инструментам кибербезопасности можно отнести следующее.

NMAP, Wireshark, Metasploit, Aircrack, Hashcat, Burpsuite, Nessus Professional, Snort, Intruder, Kali Linux и другие.

1. NMAP

Рисунок 6.2. NMAP — это программный инструмент кибербезопасности.

NMAP, сокращение от Network Mapper, представляет собой инструмент с открытым исходным кодом, используемый для сканирования сетей. Этот инструмент в основном полезен для обнаружения хостов, сбора информации о сетевых устройствах, где открыта служба или порт, а также для обнаружения уязвимостей в системе безопасности, во время работы хост-устройства. NMAP поддерживает основные платформы ОС, такие как Windows, Linux и даже MAC OS. Главное преимущество этого инструмента в том, что он гибкий, легко перемещаемый, бесплатный и хорошо документированный.

Инструмент NMAP https://nmap.org/download.html можно скачать на официальном портале.

2. Wireshark

Рисунок 6.3. Wireshark — это программный инструмент для обеспечения кибербезопасности.

Wireshark — один из наиболее широко используемых в мире инструментов для анализа сетевых протоколов. Этот инструмент помогает вам захватывать, сохранять и детально анализировать каждый пакет с помощью pcap. Wireshark поддерживает Windows, Linux, Solaris, macOS и другие платформы ОС. Wireshark также является инструментом с открытым исходным кодом, похожим на tcpdump, с опцией пользовательского интерфейса. Основные возможности Wireshark заключаются в том, что он может анализировать данные из разных протоколов в режиме реального времени. Платформа также имеет функцию кодирования для

отображения пакетов, когда они соответствуют какому-либо конкретному правилу. Этот инструмент получает пакеты только из сетей, поддерживающих pcap.

Инструментhttps://www.wireshark.org/#downloadможно скачать с официального сайта.

3. Metasploit

Рисунок 6.4. Metasploit — это программный инструмент для обеспечения кибербезопасности.

Metasploit — это мощный и популярный инструмент тестирования на проникновение с открытым исходным кодом, используемый в индустрии кибербезопасности. Этот инструмент используется кибер-злоумышленниками, а также кибер-защитниками. Metasploit имеет множество встроенных модулей, которые можно использовать для эксплойтов, выполнения полезных нагрузок, служебных функций, кодирования, прослушивания, выполнения шелл-кода, Nops. Этот инструмент можно использовать для оценки безопасности, чтобы улучшить состояние безопасности компании.

Инструментhttps://www.metasploit.com/downloadможно скачать с официального сайта

4. Aircrack-ng

Рисунок 6.5. Aircrack — программа для обеспечения кибербезопасности.

Набор инструментов Aircrack-ng для управления безопасностью Wi-Fi представляет собой набор инструментов для обеспечения безопасности. Он включает в себя мониторинг, атаку, тестирование, взлом безопасности WiFi. Этот инструмент в основном используется хакерами для взлома WiFi путем взлома методов шифрования WEP, WAP, WAP2. Этот инструмент имеет функции сниффинга и внедрения пакетов. Этот инструмент

доступен для Windows, Linux, macOS, Solaris, OpenBSD, FreeBSD.

Инструмент можно скачать по этой официальной ссылкеhttps://www.aircrack-ng.org/downloads.html

5. Hashcat

Рисунок 6.6. Hashcat — это программный инструмент для обеспечения кибербезопасности.

Hashcat — всемирно используемый инструмент для взлома паролей. Этот инструмент поддерживает более 250 алгоритмов хеширования. Этот инструмент поддерживает платформы Windows, Linux и macOS. Ключевые особенности этого инструмента заключаются в том, что это очень быстрый, гибкий, универсальный инструмент с открытым исходным кодом, который помогает выполнять атаки грубой силы на несколько значений хеш-функции. Поддерживаются такие алгоритмы хэширования, как LM, MD-семейство и SHA-семейство. Hashcat можно использовать для выполнения различных кибератак, таких как атаки грубой силы, комбинаторные атаки, атаки по словарю, атаки по отпечаткам пальцев, атаки с маскировкой, гибридные атаки, атаки подстановки, атаки Toggle-Case и т. д.

Инструментhttps://hashcat.net/hashcat/Вы можете скачать его с официального сайта.

6. BurpSuite

Рисунок 6.7. BurpSuite— программный инструмент для обеспечения кибербезопасности.

BurpSuite — это унифицированная платформа из нескольких инструментов, используемых в области тестирования на проникновение. Этот инструмент был разработан Port Swigger. Существуют различные инструменты, такие как Spider, Proxy, Intruder, Repeater, Sequencer, Decoder, Extender, Scanner и т. д., которые используются для различных процессов тестирования безопасности. Этот инструмент можно использовать как на уровне проекта, так и на уровне пользователя.

Общедоступную версию этого инструмента можно загрузить с

официального сайта.https://portswigger.net/burp/communitydownload

7. NessusProfessional

Рисунок 6.8. Программный инструмент NessusProfessional для кибербезопасности

Nessus Professional — это коммерческий инструмент, используемый для оценки уязвимостей. Этот инструмент помогает найти информацию о недостатках безопасности, уязвимостях в системе безопасности, неправильной настройке систем, серверов и сетевых устройств. Этот инструмент также можно использовать для целей соответствия и аудита. Этот инструмент представляет собой расширенный инструмент, в котором все функции автоматизированы. Он в основном выполняет сканирование сети, расширенное сканирование, расширенное динамическое сканирование, сканирование вредоносных программ, сканирование мобильных устройств, тестирование веб-приложений, проверку восстановления учетных данных, обнаружение блоков и доступное сканирование уязвимостей.

8. Snort

Рисунок 6.9. Snort — это программный инструмент для обеспечения кибербезопасности.

Snort — один из лучших инструментов IPS/IDS с открытым исходным кодом. Этот инструмент использует набор правил, помогающих обнаруживать вредоносные действия и генерировать оповещения безопасности для пользователей. Snort также может быть установлен на первом уровне сети для блокировки вредоносных источников. Snort можно запускать и использовать как в личных, так и в служебных целях. Сниффер можно настроить в трех режимах: «Режим сниффера, Режим журнала пакетов, Режим системы обнаружения вторжений в сеть». Этот инструмент разработан Cisco Systems.

Инструментhttps://www.snort.org/downloadsможно скачать с официального сайта.

9. Intruder

Рисунок 6.10. Intruder — это программный инструмент кибербезопасности.

Intruder — это инструмент оценки кибербезопасности, который сканирует уязвимости в структуре компании. Этот инструмент может обнаруживать атаки на веб-приложения, такие как внедрение SQL, межсайтовый скриптинг, CSRF и т. д., приложения, настроенные с паролями по умолчанию, и т. д. Это инструмент с тремя версиями «Pro, Essential, Verified».

10. Kali Linux

Рисунок 6.11. Kali Linux — это программный инструмент для обеспечения кибербезопасности.

Kali Linux — это продвинутый инструмент для тестирования на проникновение с открытым исходным кодом. Основная цель разработки этого инструмента — действовать как кибер-злоумышленники и этичные хакеры. Kali Linux предоставляет набор из более чем 600 инструментов, включая Aircrac-ng, Autopsy, Burp Suite, Hashcat, John the ripper, Maltego, Nmap, OWASP ZAP, Sqlmap, WPScan, Nessus, Hydra, Wireshark, Nikto, Vulnhub, Metasploit. Kali-Linux — это набор инструментов Linux на основе Debian, поддерживаемый и разработанный Offensive Security.

Инструменты цифровой криминалистикиможно разделить на различные категории, включая криминалистическую экспертизу баз данных, сбор дисков и данных, анализ электронной почты, анализ файлов, просмотрщики файлов, веб-анализ, анализ мобильных устройств, судебную экспертизу сети и т. д. анализ реестра. Кроме того, многие инструменты выполняют несколько функций одновременно, и важным трендом цифровой криминалистики являются «обертки», которые объединяют сотни специализированных технологий с разными функциями в один общий набор инструментов.

Инструменты цифровой криминалистики — это аппаратное или программное обеспечение, предназначенное для восстановления цифровых доказательств кибератаки, сохранения данных или критически важных систем.

Специалисты по кибербезопасности полагаются на технологии для проведения своих расследований, и эта потребность создала большой рынок инструментов криминалистического анализа. Список основных видов цифровой криминалистики часто включает:

- инструменты для судебной экспертизы дисков,
- инструменты сетевой криминалистики,
- Инструменты судебной экспертизы беспроводных сетей,
- инструменты криминалистики базы данных,
- инструменты криминалистики вредоносного ПО,
- инструменты судебной экспертизы электронной почты,
- Инструменты судебной экспертизы на основе памяти,
- Криминалистические инструменты для мобильного телефона,
- Платформы киберкриминалистики.

Платформы криминалистики с открытым исходным кодом — это инструменты цифровой криминалистики начального уровня. Ниже приведены некоторые инструменты цифровой криминалистики с открытым исходным кодом.

1. Корпорация Paraben .

Paraben Corporation вышла на рынок кибербезопасности в 1999 году с цифровой криминалистикой,оценка рискаи представляет собой инструмент, ориентированный на решения безопасности. Сегодня, в мире с миллиардами устройств, парабены можно найти в электронной почте, компьютерах, смартфонах и других устройствах.Устройства Интернета вещей (IoT)охватывает соответствующие судебно-медицинские расследования.

2. Набор Sleuth и Autopsy.

Sleuth Kit (TSK) и вскрытиепопулярные инструменты для цифровых расследований с открытым исходным кодом. Sleuth Kit позволяет администраторам анализировать информацию о файловой системе с помощью библиотеки инструментов командной строки для проверки образов дисков. Autopsy — это платформа цифровой криминалистики, используемая для исследования общедоступных и частных компьютерных систем с графическим пользовательским интерфейсом (GUI) и возможностями TSK.

3. Инструменты Magnet криминалистики.

В 2011 году Джад Салиба, канадский полицейский, заметил, что инструменты цифровой криминалистики, используемые правоохранительными органами, недостаточны.Магнит Криминалистикаосновал компанию. Компания предлагает инструменты цифровой криминалистики государственным и частным организациям.

4. CAINE.

Компьютерная среда исследования(Caine) — это итальянский дистрибутив с открытым исходным кодом, основанный на Ubuntu и Linux, для целей цифровой криминалистики. CAINE интегрируется с существующими инструментами безопасности систем Windows, Linux и Unix.

5. Kroll — это инструмент компьютерной криминалистики.

Компьютерная криминалистика Кроллауслуги и эксперты гарантируют, что ни одно цифровое доказательство не будет упущено из виду, и помогут на любом этапе расследования или

судебного разбирательства, независимо от количества или местоположения источников данных.

6. Sanssift.

SIFT Рабочая станцияпредставляет собой набор бесплатных и открытых инструментов реагирования на инциденты и криминалистических инструментов для проведения цифровой криминалистики. Предлагая бесплатные решения с открытым исходным кодом, SIFT Workstation предлагает множество вариантов использования, включая виртуальную машину (ВМ), локальную установку в Ubuntu или установку в Windows через подсистему Linux.

7. Exterro.

Он был из Портленда, штат Орегон.ЭкстерроЗапущенное в 2004 году программное обеспечение на основе рабочего процесса иуправление, риск и соблюдениеспециализируется на решениях. В то время как все наши варианты по своей сути поддерживают потребности организаций в соблюдении требований, Exterro особенно ценен тем, что помогает внутренним юридическим группам оптимизировать процессы соответствия и управлять рисками.

8. X-Ways.

Судебная экспертиза X-Waysрабочая среда для компьютерных криминалистов. Ресурсоемкий, но известный своей скоростью, он основан на шестнадцатеричном и дисковом редакторе WinHex и предлагает дополнительные программы для записи дисков и данных, клонирования, создания образов и другие инструменты.

9. Cellebrite.

Начато в 1999 годуЦеллебритспециализируется на криминалистике мобильных устройств для правоохранительных органов и предприятий, которым необходимо собирать, просматривать, анализировать или управлять данными устройств. Платформа Digital Intelligence Investigation Platform помогает интегрировать жизненный цикл расследования и сохранять цифровые доказательства.

10. ProDiscover.

ProDiscover был запущен в 2001 году, чтобы помочь государственным и частным организациям раскрывать цифровые преступления. По состоянию на 2021 год индийский провайдер работает более чем в 70 странах с более чем 400 клиентами, включая NIST, NASA и Wells Fargo.ProDiscover Forensicsэто криминалистический инструмент для сбора, хранения, фильтрации и анализа улик.

11. Wireshark.

Впервые он был разработан в 1998 году.Wiresharkвыполняет судебную экспертизу и анализ сетевых пакетов, а также выполняет сетевое тестирование и устранение неполадок. Это включает в себя проверку сотен протоколов в трехпанельном браузере пакетов, охватывающем структуры данных.

Тест на проникновение(также называемое пентестингом) — это метод кибербезопасности, используемый организациями для выявления, тестирования и устранения слабых мест в своих средствах управления безопасностью.

Инструменты тестирования на проникновение используются как часть тестирования на проникновение для автоматизации

определенных задач, повышения эффективности тестирования и выявления проблем, которые трудно обнаружить с помощью одних только ручных методов анализа. После оценки угроз и уязвимостей специалисты по тестированию на проникновение предоставляют отчет, который помогает организации устранить выявленные риски для улучшения своей системы киберзащиты.

Инструменты пентестинга необходимы для тестирования безопасности в современных крупномасштабных ИТ-средах. Они позволяют обнаруживать активы в сложных гибридных средах и помогают тестировщикам оценивать системы по критериям безопасности и требованиям соответствия.

Набор для тестирования на проникновение должен включать множество инструментов. Существует несколько инструментов для тестирования на проникновение:

— **Сканеры портов-** определяет открытые порты в системе. Это помогает тестировщикам идентифицировать операционную систему и приложения, работающие в сети, к которой они пытаются получить доступ. Сканирование портов используется в разведке и может дать идеи для потенциальных векторов атак.

— **Сканеры уязвимостей-** ищет известные уязвимости в серверах, операционных системах и приложениях, а также неправильные конфигурации, которые можно использовать при тестировании. Отчеты, предоставляемые сканерами уязвимостей, помогают специалистам по тестированию на проникновение выбрать уязвимость, которую можно использовать, которая дает им первоначальный доступ к системе.

— **Сетевой сниффер-** отслеживает информацию о сетевом трафике, включая его источник, пункт назначения, устройства, взаимодействующие в сети, используемые протоколы и порты. Это может быть полезно для проверки того, зашифрованы данные или нет, а также для определения путей связи, которые можно использовать во время тестирования на проникновение.

— **Веб-прокси-** позволяет пентестерам перехватывать и изменять трафик между своим браузером и веб-серверами организации. Это позволяет обнаруживать скрытые поля

формы и другие функции HTML, которые могут способствовать атакам, таким как межсайтовый скриптинг (XSS) или подделка межсайтовых запросов (CSRF).

— **Взлом пароля**- хеширование паролей является распространенной целью злоумышленников как средство повышения привилегий в целевой системе или сети. Инструменты для взлома паролей позволяют специалистам по тестированию на проникновение определять, использует ли организация слабые пароли, подвергающие сотрудников риску.

Инструменты для специалистов по тестированию на проникновение:

— **Kali Linux**— это операционная система, которая облегчает тестирование на проникновение, тестирование безопасности и связанные с ними действия. Это дистрибутив Linux на основе Debian, предоставляемый с открытым исходным кодом и поддерживаемый Offensive Security.

— **Armitage** - графический инструмент для управления сетевыми атаками.

— **Nmap**- сканер портов.

— **Wireshark**- анализатор пакетов.

— **Metasploit** - система тестирования на проникновение с тысячами модулей эксплуатации.

— **Jon Ripper** - взломщик паролей.

— **sqlmap**- автоматизированная инъекция SQL и импорт базы данных.

— **Aircrack-ng**- пакет программ для тестирования доступа к беспроводной локальной сети.

— **OWASP ZAP** — сканер безопасности веб-приложений.

— **Burp suite** - проверить безопасность программы.

§ 6.3. Обучение по кибербезопасности для сотрудников

Обеспечение кибербезопасности сегодня остается одной из основных задач каждого государства в рамках общей системы обеспечения информационной безопасности. Обучение кибербезопасности обучает удаленных сотрудников тому, как использовать устройства, когда они находятся за пределами

корпоративной инфраструктуры.

Причина обучения сотрудников знаниям и навыкам кибербезопасности проста: если сотрудники не знают, как выявлять угрозы безопасности, они не смогут их устранить. Например, исследование кибербезопасности 2019 года показало, что безопасность электронной почты и обучение сотрудников были определены как главные проблемы, с которыми сталкиваются специалисты по кибербезопасности. Это подтверждает тот факт, что более 30% сотрудников, опрошенных Wombat Security Technologies, не знают, что такое фишинг или вредоносное ПО.

Короче говоря, 90-95% инцидентов кибербезопасности вызваны человеческими ошибками. Кроме того, только 38% международных организаций заявили, что готовы противостоять изощренным кибератакам. Еще 54% компаний сообщили об одной или нескольких атаках за последние 12 месяцев, и это число растет с каждым месяцем.

Излюбленной тактикой киберпреступников сегодня является социальная инженерия, психологическое манипулирование жертвами с целью убедить их добровольно или невольно передать личную информацию. На долю фишинга приходится 95% кибератак, поэтому важно читать и узнавать о фишинге.

Вредоносное ПО для кибербезопасности также представляет постоянную угрозу. Это включает в себя загрузку приложений или программ, предназначенных для джейлбрейка устройств или предоставления хакерам доступа к сети.

В связи с широким использованием ИТ в бизнес-процессах, внедрением цифровых технологий и использованием сети Интернет требуется обучение сотрудников навыкам кибербезопасности.

Интернет вещей (IoT). Сотрудники подключают личные устройства к корпоративным сетям или даже используют их для служебной работы. Подключение личных устройств к другим машинам и сетям увеличивает уязвимость. Мобильные устройства представляют серьезную угрозу для внутренней кибербезопасности организации, поскольку многие из них недостаточно защищены. С атаками IoT можно бороться, управляя и, возможно, сводя к минимуму практику использования собственных устройств на рабочем месте и обеспечивая строгое соблюдение политик безопасности среди сотрудников.

Обучение персонала кибербезопасности

Сотрудники, обладающие знаниями и навыками в области кибербезопасности, являются первой и главной линией защиты от киберпреступности. Любой сотрудник, имеющий доступ к рабочему компьютеру или мобильному устройству, должен пройти обучение по кибербезопасности. Потому что почти каждый сотрудник может стать мишенью киберпреступника. Личные телефоны могут хранить данные, которые можно использовать для доступа к корпоративным сетям, или, если личная информация сотрудника украдена, ее можно использовать для доступа к информационным системам компании, что позволяет осуществлять киберпреступную деятельность.

Сотрудникам необходимы базовые знания о различных формах угроз, чтобы обнаруживать и предотвращать нарушения. Киберугрозы включают спам, фишинг, вредоносное ПО и сетевые атаки, а также социальную инженерию.

При обучении сотрудников необходимо предоставить информацию о видах вредоносного ПО, уровне вредоносности, способах защиты от них и разъяснить их практическими инструкциями. В то же время должны быть предоставлены подробности о социальной инженерии. Потому что социальные инженеры маскируются под фальшивые, но надежные онлайн-личности и заманивают их нужной им информацией.

Сегодня пароли используются повсеместно в информационной системе. Эта тактика, разработанная как инструмент безопасности, привела к тому, что многие люди стали устанавливать общие повторяющиеся пароли, которые легко запомнить и, следовательно, легко угадать. Обучение кибербезопасности должно помочь учащимся понять важность паролей и обеспечить понимание политик создания паролей и доверенных программ, которые могут их хранить.

Электронная почта сотрудников и привычки в социальных сетях могут подвергнуть компанию вредоносному ПО, которое атакует корпоративные приложения и учетные записи социальных сетей, похищая данные и деньги. Вот почему так важно, чтобы обучение включало правила и рекомендации по использованию электронной почты, Интернета и социальных сетей.

У каждой компании есть своя политика защиты данных, но не все сотрудники компании могут знать об этой политике. Он должен

предоставлять знания и навыки в области информационной безопасности для новых сотрудников и объяснять юридические и практические обязательства по защите. Регулярное обучение необходимо для того, чтобы все сотрудники помнили правила и умели их применять.

Методы обучения кибербезопасности.

Никогда не соглашайтесь на готовые учебные модули или онлайн-курсы. Должны быть привлечены специалисты по кибербезопасности, которые работают непосредственно с предприятием. Тренинг, проводимый профессионалами, позволит вам разработать полную стратегию безопасности, адаптированную к потребностям новых правил кибербезопасности, конфиденциальности данных и сотрудников. Учебные занятия по кибербезопасности следует проводить часто, предоставляя возможность практиковать безопасное поведение между занятиями.

Осведомленность о кибербезопасности и информирование пользователей о фишинговых атаках достигается с помощью одного или нескольких методов доставки. Существует несколько типов обучения кибербезопасности и методов повышения осведомленности.

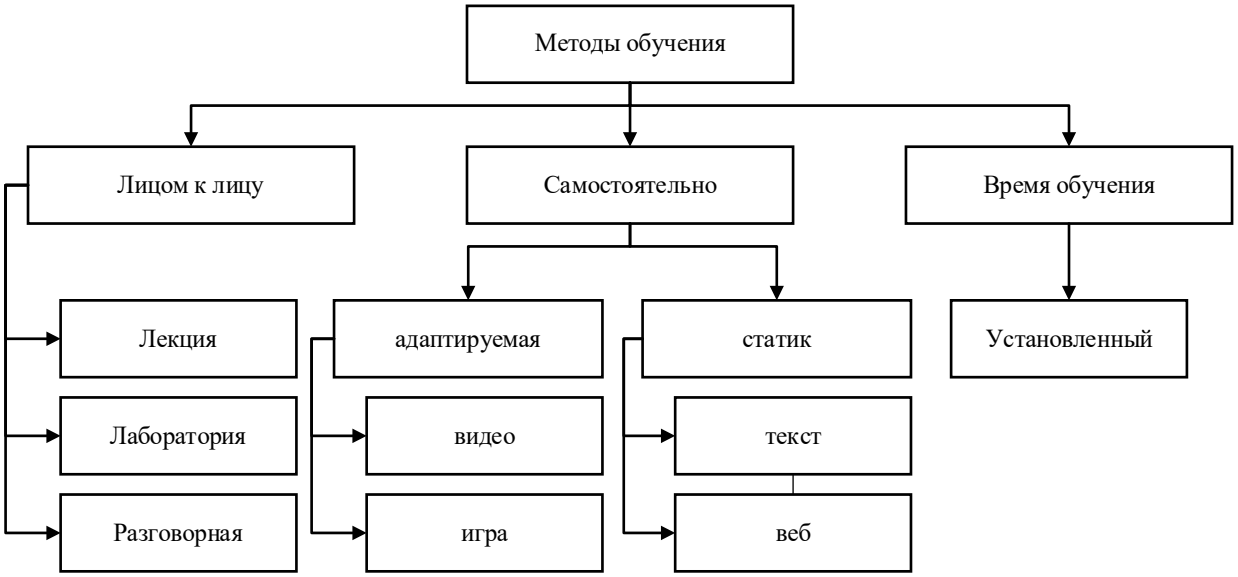


Рисунок 6.5.Классификация методов обучения кибербезопасности

На рис. 6.5 показана предлагаемая классификация методов обучения осведомленности о кибербезопасности. По сути, методы доставки делятся на три основных класса: очный класс, самоуправляемый класс и встроенный класс. Класс самоуправляемых методов доставки делится на гибкие и статические

категории.

Повышение осведомленности об угрозах онлайн-безопасности должно начинаться с первого дня работы новых сотрудников. Это помогает включить политики и правила защиты данных, правила использования Интернета в справочнике сотрудников.

Типы обучения кибербезопасности

Инвестиции в кибербезопасность имеют решающее значение для всех предприятий, и сотрудники должны воспользоваться соответствующей программой обучения.

Ваша подготовка по кибербезопасности должна быть обновлена для борьбы с новыми угрозами, создаваемыми киберпреступниками. Это включает в себя просмотр учебных материалов и обновление контента на постоянной основе.

Доступны различные методы обучения, включая моделирование атак, осведомленность о распространенных и редких атаках и подробные отчеты.

Следующий список программ обучения поможет сотрудникам пройти обучение по кибербезопасности. Кибербезопасность — это постоянная проблема, требующая частых ежеквартальных обновлений, чтобы ваша команда была готова к новым атакам.

1. Обучение по вопросам кибербезопасности

Основная форма обучения кибербезопасности направлена на повышение осведомленности сотрудников о потенциальных угрозах.

Его можно включить в процесс адаптации новых сотрудников, а также распространить среди членов команды.

При обработке данных клиентов существуют юридические обязательства, и защита этих данных является важной частью работы каждого сотрудника.

1. Ознакомительный тренинг включает в себя:

1) Обучение безопасности электронной почты
2) Обучение безопасности в Интернете
3) Обучение процедурам обмена информацией
4) Базовое инженерное образование против общества

Обычные преступления в области кибербезопасности, такие как социальная инженерия, фишинг и интернет-угрозы, могут показаться очевидными, но их важно освещать. Сотрудники должны знать, как обнаружить потенциальную угрозу и кого предупредить в

вашей организации.

Существует множество бесплатных онлайн-курсов обучения, которые помогут вашим сотрудникам быстро разобраться в последних проблемах кибербезопасности. Курсы доступны от известных организаций, а также государственных учреждений.

2. Специализированные программы кибербезопасности

Есть более продвинутые программы для ИТ-специалистов и аналитиков по безопасности.

Эти программы помогают сотрудникам получить более глубокое представление о кибербезопасности и дают им навыки, необходимые для создания собственной защиты.

Это обучение должно быть связано с:

1) Самая лучшая десятка OWASP

2)CWE/SANS ТОП 25 самых опасных программных ошибок

3) Обучение DevOps безопасным операциям для облака и доставки.

4) обучение CSA

5) Обучение работе с сетью

6) Обучение взлому Whitehat и тестированию на проникновение

7) Обучение безопасности операционной системы (ОС) для системных администраторов

Учебные курсы — это наиболее полный способ развития профессиональных навыков в области кибербезопасности, поскольку они включают в себя оценку уязвимостей, безопасность данных и тестирование на проникновение. Эти программы предназначены для обучения основам информатики, и студенты могут получить практический опыт противодействия кибератакам.

Давайте взглянем на передовые программные решения для обучения команд кибербезопасности.

1. Cofense PhishMe.Cofense PhishMe знакомит пользователей с реальной тактикой фишинга посредством обширных исследований, информации об угрозах и расширенных ресурсов защиты от фишинга.

Cofense предлагает ряд облачных решений для защиты компаний от кибератак путем вымогательства, компрометации корпоративной электронной почты и фишинга.

Cofense PhishMe — это решение для обучения безопасности и одна из самых популярных платформ в своем роде. Это инструмент для обучения сотрудников и моделирования фишинга, направленный на повышение устойчивости организации к атакам социальной инженерии.

Cofense PhishMe имитирует активные фишинговые угрозы, чтобы создать осмысленное поведение пользователей. Платформа предлагает предприятиям реалистичные симуляции, настроенные для определенных типов атак социальной инженерии разной степени сложности. В дополнение к обучению Cofense также обеспечивает защиту от фишинга для сети электронной почты.

Cofense Playbooks позволяет вам настроить полную 12-месячную программу, которая включает в себя сценарии моделирования, мультимедиа и образовательный контент.

Cofense проверяет каждый фрагмент контента в симуляторе, чтобы убедиться, что он соответствует запросам аудитории — контент представлен на 36 языках, включая русский.

2. **Тренинг по вопросам корпоративной безопасности Knowbe4.**Обучение по вопросам корпоративной безопасности

KnowBe4 предлагает комплексный подход к обучению, который включает в себя базовые пробные тесты атак, интерактивное обучение и непрерывное моделирование различных шаблонов атак.

Перед началом обучения KnowBe4 предоставляет базовые тесты для оценки количества пользователей в вашей компании, уязвимых к фишингу (атакам через телефонную связь, например,

обман конфиденциальной информации владельца платежной карты под разными предлогами), смишингу (фишинг).

Компания предлагает самую большую в мире библиотеку учебных материалов по безопасности, включая интерактивные модули, видео, игры и информационные бюллетени.

Платформа KnowBe4 объединяет все функции в одном графическом интерфейсе. Учебные кампании запускают и имитируют атаки за считанные минуты, а команды проходят обучение с помощью полностью автоматизированных фишинговых, вишинговых и смишинговых атак, включающих тысячи шаблонов. Эти шаблоны полностью настраиваются и содержат более 4000 реалистичных фишинговых писем, которые со временем будут развернуты.

Во время обучения KnowBe4 отправляет отчеты о сильных и слабых сторонах компании. Доступны общие и подробные статистические данные и графики, которые можно легко включить в управленческие отчеты. Они дают представление о производительности безопасности всей организации.

Контрольные вопросы.

1. Каковы обязанности по кибербезопасности каждого человека в организации?
2. Каковы правила использования шифрования электронной почты в политике кибербезопасности?
3. Каковы рекомендации по созданию и защите паролей?
4. Какие правила следует соблюдать при использовании социальных сетей?
5. Что такое политика защиты от вредоносных программ и какова ее цель?
6. Какие меры по предотвращению и защите от атак вирусов и вредоносных программ указаны в политике защиты от вредоносных программ?
7. Что такое веб-сервер и как он связан с приложениями, предоставляющими информацию через Интернет?
8. Какие угрозы безопасности могут возникнуть на веб-сервере и как их можно классифицировать?
9. Каковы последствия несанкционированного доступа к веб-серверу для организации?
10. Что такое атаки типа «отказ в обслуживании» и как они

могут повлиять на веб-сервер и его пользователей?

11. Какие меры следует принять для защиты конфиденциальной информации на веб-сервере от передачи или перехвата посторонними лицами?

12. Как злоумышленники могут использовать веб-сервер для доступа или атаки на ресурсы других организаций?

13. Какие проблемы могут возникнуть, если веб-сервер используется для распространения нелегального контента или программного обеспечения?

14. Что такое брандмауэр и какие функции он выполняет для защиты веб-сервера и сетевой инфраструктуры?

СПИСОК АББРЕВИАТУР :

ISO - International Organization for Standardization
NIST - National Institute of Standards and Technology
IO – Input/Output
LAN - Local area network
CTI - Cyberthreat Intelligence
NCSC - National Cyber Security Centre
CSOC - Cybersecurity Operations Center
CISP - Cyber Security Information Sharing Partnership
SIEM – Security information and event management
CVE - Common Vulnerabilities and Exposures
APT - Advanced Packaging Tool
MISP - Malware Information Sharing Platform
SMT - Simultaneous Multithreading
FIS - foreign intelligence services
OCG - Organized crime groups
CMDB - configuration management database
OSINT - Open source intelligence
GPMS - Global PDI Management System
ARPANET - Advanced Research Projects Agency Network
IETF - Internet Engineering Task Force
IANA - Internet Assigned Numbers Authority
ICANN - Internet Corporation for Assigned Names and Numbers
GLBA - Grahm-Leach-Bliley Act
HIPAA - Health Insurance Portability and Accountability Act
DCF - discounted cash flow
ИМСиТ – Институт Мировых стандартов и технологий
АНБ – Агенство национальной безопасности
DBIR - Data Breach Investigation Report
МСЭ – Международный союз электросвязи
ЕОпБиС–Европейская организация по безопасности и сотрудничеству
СУИБ – Системы управления информационной безопасностью

CTRG - Computer Technology Research Group
ЖЦСПК – Жизненный цикл создания политики кибербезопасности
DDOS - Distributed Denial of Service
BYOD - Bring Your Own Device
AI - artificial intelligence
ML - machine learning
IOT - internet of things
DNS - Domain Name System
GUI - graphical user interface

ТОЛКОВЫЙ СЛОВАРЬ ТЕРМИНОВ

Конфиденциальность - под этими правилами понимается способность ограничивать распространение системных данных разрешенным использованием, обеспечивая “чтение” информации только законными пользователями.

Целостность (целостность) относится к способности сохранять подлинность, достоверность и источник записанной и сообщаемой информации, то есть защищать информацию от несанкционированного изменения или “записи”.

Удобство использования - обеспечение точности и достоверности информации, подразумевающее своевременное предоставление функциональности, возможность использования информации, информации и системы, т. е. защита от несанкционированного “исполнения”.

Слово **"политика"** применяется к различным ситуациям, связанным с кибербезопасностью. Он используется для обозначения законов и постановлений, касающихся распространения информации, целей частного предприятия по защите информации, методов компьютерных операций для управления технологиями и переменных конфигурации в электронных устройствах.

Сканеры портов - обнаруживает открытые порты в системе. Это помогает тестировщикам идентифицировать операционные системы и приложения, работающие в сети, к которой они пытаются получить доступ. Сканеры портов используются в разведке и могут дать представление о потенциальных векторах атаки.

Сканеры уязвимостей - ищет известные уязвимости в серверах, операционных системах и приложениях, а также неправильные конфигурации, которые можно использовать при тестировании. Отчеты, предоставляемые сканерами уязвимостей, помогают тестерам на проникновение выбрать используемую уязвимость, которая дает им первоначальный доступ к системе.

Сетевой сниффер - отслеживает информацию о сетевом трафике, включая его источник, адрес, устройства, обменивающиеся данными

в сети, используемые протоколы и порты. Это может быть полезно для проверки того, зашифрованы ли данные, и для определения возможных путей связи, которые можно использовать во время тестирования на проникновение.

Веб-прокси позволяет тестерам на проникновение перехватывать и изменять трафик между их браузером и веб-серверами организации. Это позволяет обнаруживать скрытые поля формы и другие функции HTML, которые могут активировать атаки, такие как межсайтовые скрипты (XSS) или межсайтовые подделки запросов (CSRF).

Взлом пароля - хеширование паролей является общей целью для злоумышленников как средство повышения привилегий в целевой системе или сети. Инструменты взлома паролей позволяют тестерам на проникновение определять, используют ли они слабые пароли, которые представляют опасность для сотрудников организации.

Kali Linux - это операционная система, которая упрощает тестирование на проникновение, проверку безопасности и сопутствующие действия. Это дистрибутив Linux на основе Debian, представленный как открытый исходный код и поддерживаемый Offensive Security.

Использованная литература:

1. Cyber security policy guidebook. Jennifer L. Bayuk. Jason Healey. Paul Rohmeyer, et.c. Willey publisher.2018-y. 288 p. ISBN 978-1-118-02780-6.
2. Cybersecurity Curricula 2017 – Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8) (Crosscutting concepts).
3. Ғаниев С.К., Каримов М.М., Ташев К.А., "Ахборот хавфсизлиги", "Фан ва технологиялар" нашриёти, Тошкент 2016.
4. Abend, V., et al. (2008). Cybersecurity for the banking and finance sector.
5. ISO/IEC 27000 Information technology. Security techniques. Information security management systems. Overview and vocabulary.
6. Шангин В.Ф., «Комплексная защита информации в корпоративных системах», Учебное пособие. М.: ИД. «ФОРУМ» - ИНФРА М. 2019, 591с.
7. Mark Stamp. Information security. Principles and Practice. Second edition. A John Wiley& Sons, Inc., publication. Printed in the United States of America. 2011y. 584p
8. CISSP Official Study Guide (Mike Chapple, James Michael Stewart, Darril Gibson) (2018, Sybex).
9. Mark Ciampa. Security+.Guide to Network Security Fundamentals. Fifth Edition. Printed in the United States of America Print Number: 01 Print Year: 2014
10. Tim Boyles. CCNA Security Study Guide. Copyright © 2010 by Wiley Publishing, Inc., Indianapolis, Indiana. Published simultaneously in Canada ISBN: 978-0-470-52767-2.
11. Joseph Migga Kizza. Computer Network Security and Cyber Ethics. Fourth edition. McFarland & Company, Inc., Publishers Jefferson, North Carolina © 2014.
12. ANSI and ISA (2010). The financial management of cyber risk. An Implementation Framework for CFOs, American National

Standards Institute (ANSI) and the Internet Security Alliance (ISA).In Wiley Handbook of Science and Technology for Homeland Security, ed. J. G. Voeller. Hoboken, NJ: John Wiley & Sons, Inc.

13. Bayuk, J. (2010). Enterprise Security for the Executive: Setting the Tone at the Top. Santa Barbara, CA: Praeger.

14. Hubbard, D. W. (2009). The Failure of Risk Management. Hoboken, NJ: John Wiley & Sons, Inc., p. 6.

15. Markoff, J. (2012). Researchers find a flaw in a widely used online encryption method. The New York Times, February 15.

16. NCSC / Cabinet Office. *Minimum Cyber Security Standard.* London : publishing.service.gov.uk, 2018. Version 0.1.

17. MITRE. MITRE Cyber Attack Lifecycle. *MITRE.* [Online] attack.mitre.org/resources/enterpriseintroduction.

18. Gartner. Market Guide for Security Threat Intelligence Products and Services. *Gartner.* [Online] https://www.gartner.com/doc.3765965/market-guide-security-threat-intelligence.

19. FireEye. Threat Intelligence Use Case Series. *FireEye.* [Online]

https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/intel/sb-incident-responderprofile.pdf

20. Recorded Future. Threat Intelligence Use Cases. *Recorded Future.* [Online]

https://www.recordedfuture.com/threat-intelligence-use-cases.

21. OASIS. Introduction to STIX. *OASIS Open Github.* [Online] https://oasis-open.github.io/ctidocumentation/stix/intro.

22. Lockheed Martin. The Cyber Kill Chain. *Lockheed Martin.* [Online] [Cited: 27 09 2018.] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

23. BAE Systems. *Intelligence Led Threat Mitigation.* s.l. : BAE Systems, 2017.

24. Caltagirone, Sergio, Pendergast, Andrew and Betz, Christopher. *The Diamond Model Of Intrusion Analysis.* s.l. : Active Response, 2013.

O‘QUV ADABIYOTINING NASHR RUXSATNOMASI

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining 2023-yil 29-avgustdagi 895-22-sonli buyrug‘iga asosan

N.S.Yuldasheva, O.N.Mavlonov, D.J.Sodiqova,

(muallif familiyasi, ismi-sharifi)

R.SH.Meliqoziyev, M.A.Shakarov

5330300-“Axborot xavfsizligi (sohalar bo‘yicha)”

(ta’lim yo‘nalishi(mutaxassisligi))

ning talabalari (o‘quvchilari) uchun tavsiya etilgan

Политика кибербезопасности

(O‘quv adabiyotlar nomi va turi: darslik, o‘quv qo‘llanma)

O‘quv qo‘llanma ga

O‘zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan litsenziya berilgan nashriyotlarda nashr qilishga ruxsat beriladi

Rektor _____ **B.Sh. Maxkamov**

(imzo)

M.O‘

Ro‘yxatga olish raqami
№ 2023-087

Н.С.ЮЛДАШЕВА, О.Н. МАВЛОНОВ, Р.Ш. МЕЛИҚЎЗИЕВ
Д.Ж. СОДИҚОВА, М. А. ШАКАРОВ

ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ

Bosishga ruxsat etildi. 29.09.2023 y.
Qog`oz bichimi 60x84 1/16.
Times New Roman garniturasida terildi.
Ofset uslubida oq qog`ozda chop etildi.
Nashriyot hisob tabog`i 18,25, Adadi 100. Buyurtma № 21-02
Bahosi kelishuv asosida

«ZUXRA BARAKA BIZNES» MChJ
bosmaxonasida chop etildi.
Manzil: Toshkent shahar Chilonzor tumani,
Bunyodkor shoh ko‘chasi 27 A–uy.