Столыпинский вестник

Научная статья

Original article

УДК 005

ТРЕБОВАНИЯ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ

CYBERSECURITY REQUIREMENTS FOR MANAGEMENT INFORMATION SYSTEMS

Голубятников Артем Олегович, Студент кафедры защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург artemgolubyatnikov@mail.ru

Golubyatnikov Artyom Olegovich, Student of the Department of Secure Communication Systems, St. Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruevich, St. Petersburg artemgolubyatnikov@mail.ru

Аннотация: Кибербезопасность является одним из наиболее важных элементов безопасности в развитых странах. Тем более, что существует общая тенденция к кибербезопасности во всех аспектах жизни, я обнаружил, что идея кибербезопасности основана на защите критически важных объектов: информационной инфраструктуры страны. Информационные системы, включая системы управления электронным правительством, находятся в ведении ключевых государственных ведомств. Как и в случае с экономическими, научными, торговыми и другими системами , угрозы — это угрозы национальной безопасности страны. Таким образом, мы обнаружили, что многие страны готовят институты, способные интегрировать кибербезопасность в защиту,

развитие и информационную безопасность. Эта концепция стала самой важной заботой развитых стран, которые обеспечили все научные возможности и системы для ее достижения. Электронная информационная сеть стала неотъемлемой частью повседневной жизни во всех местах. Помимо личного использования, цифровая информация используется, обрабатывается, хранится и передается. По мере увеличения и распространения этой информации мы обнаружили, что ее защита становится более важной и оказывает эффективное влияние на национальную безопасность и технический прогресс.

Abstract: Cybersecurity is therefore one of the most important elements of security in developed countries. Especially since there is an overall trend towards cybersecurity in all aspects of life, I have found that the idea of cybersecurity is based on protecting critical facilities: The nation's information infrastructure. Information systems, including e-government management systems, are managed by key state agencies. As with economic, scientific, commercial, and other systems, threats are threats to a nation's national security. We have therefore found that many countries are preparing institutions capable of integrating cybersecurity into protection, development, and information security. This concept has become the most important concern of developed countries, which have secured all scientific possibilities and systems to achieve it. The electronic information network has become an integral part of today's daily lives in all places. In addition to personal uses, digital information is used, processed, stored, and shared. As this information increases and spreads, we have found that its protection has become more vital and has an effective impact on national security and technical progress

Ключевые слова: Кибербезопасность , Безопасность , Информационные системы

Keywords: Cybersecurity, Security, Information Systems

1. Введение

Вопрос информационной безопасности и защиты считается одним из важнейших вопросов эпохи — эпохи четвертой промышленной революции, — когда успех любого учреждения во многом зависит от информации, которой он

обладает [1] . Но большая часть информации, систем и инфраструктуры, связанной с сетями, время от времени подвергается опасности [2]. Поскольку он сталкивается с различными типами утечек информации, а также подвергается преступной деятельности (хакерам), которая нарушает работу его служб и уничтожает его собственность. Хакерские атаки варьируются от одной стороны к другой, от одного места к другому и время от времени. Это достигается за счет постоянного использования возобновляемых, сложных хакерских инструментов и механизмов. Это подтверждает важность кибербезопасности для поддержания безопасности Родины и ее граждан [3].

Окончание «холодной войны» привело к появлению множества вызовов и угроз, свидетелями которых международное сообщество ранее не сталкивалось [4]. Эти вызовы и угрозы известны как транснациональные угрозы, поскольку они не признают границ, национального суверенитета или идеи национального государства, что привело к сдвигам в сфере безопасности и стратегических исследованиях, а также на уровне политической практики [4] .] .

В этом контексте многие арабские страны стремились всесторонне развивать свою родину, свою безопасность, свою экономику, благосостояние своих граждан и достойный уровень жизни [5] . Возобновляемые глобальные системы информационных технологий (ИТ) и системы операционных технологий готовятся к работе с данными искусственного интеллекта и преобразованиями четвертой промышленной революции в соответствии с ростом возможностей компьютерной обработки и возможностей массового хранения и передачи данных [1] .

Эта трансформация требует потока информации, ее безопасности и интеграции ее систем, а также сохранения и усиления кибербезопасности арабских стран в целях защиты жизненно важных интересов стран, их национальной безопасности, критической инфраструктуры, приоритетных секторов, услуг, и государственная деятельность [1] . Поэтому был издан королевский указ о создании организации под названием «Национальное управление кибербезопасности» в некоторых странах, например, в Саудовской Аравии. Эта организация является органом, занимающимся вопросами кибербезопасности, и

считается эталоном для государства по двум причинам [2]. Первая цель — защитить свою национальную безопасность, жизненно важные интересы и чувствительную инфраструктуру. Вторая цель заключается в предоставлении безопасных технических услуг и методов защиты для защиты данных и систем связи от кибератак, а также для поддержания конфиденциальности и целостности информации [1].

- Национальное управление кибербезопасности:

Помимо появления угроз и киберпреступности, они представляют собой серьезную проблему для национальной и международной безопасности, особенно с учетом многочисленных последствий, вытекающих из развития информационной революции и наступления цифровой эпохи в 21 ^{веке}. Многие исследователи считают киберпространство пятой ареной войны после Земли, моря, воздуха и космоса [2].

Это создало необходимость обеспечения безопасности в этой цифровой среде. Кибербезопасность в значительной степени материализовалась с ее появлением в качестве нового измерения в повестке дня исследований в области безопасности, которое привлекло внимание многих исследователей в этой области. Исследования в области кибербезопасности стали одной из последних инноваций в мировом технологическом и цифровом развитии, и мы не можем позволить себе упускать их из виду [3]. Итак, эти технические исследования в области цифровых вычислений стали целью для многих ведущих ученых всего мира, но это цифровое развитие, которое мы наблюдаем, имеет потенциал для стабилизации. Есть еще один темный аспект атак и взломов, который может к этому привести [1].

Отсюда необходимость понять, что такое кибербезопасность, и тщательно изучить ее в различных аспектах как новую переменную в международных отношениях.

2. Проблема поиска

Несмотря на огромные положительные результаты, достигнутые информационными технологиями, растущая информационная революция повлекла за собой множество серьезных негативных последствий в результате

неправильного использования информационных технологий. Среди этих новых влияний — феномен цифровой преступности, опасность которой продолжает возрастать и порождать новые виды преступности, такие как трансконтинентальная преступность. Его опасность и достоинство больше не ограничиваются некоторыми странами и создают ряд юридических проблем для органов по предупреждению преступности.

В последнее время термин «кибербезопасность» стал популярным, и многие специалисты по информационной безопасности услышали о том, что такое кибербезопасность, является ли информационная безопасность частью кибербезопасности, в чем между ними разница и о многих других возникающих вопросах. К кому применяется этот термин и от каких угроз защищает кибербезопасность? Зависят ли они исключительно от институтов или от институтов и отдельных лиц, и как они выйдут из войны четвертого поколения, от которой нужно будет защищаться.

Киберпространство имеет три измерения. Первое измерение — экономическое, которое делит интернет-экономику на две основные области: первая — это индустрия ИКТ, которая включает разработку аппаратного обеспечения, производство программного обеспечения и другие услуги. Второй — в области электронной коммерции, открыв бесплатный онлайн-рынок. Второе измерение – информационная безопасность. Многие страны выделяют значительную часть своего бюджета на противодействие кибератакам, а также на обновление и развитие своих систем безопасности. Третье измерение — это измерение безопасности, лучшим примером которого является Центр интеграции информации о киберугрозах (CTIIC) в Соединенных Штатах Америки. Этот центр координирует работу различных других агентств безопасности США, таких как ФБР, ЦРУ и Агентство национальной безопасности.

В свете изложенного проблематика исследования определяется в попытке ответить на следующий вопрос:

Каковы требования для достижения кибербезопасности в информационных системах управления в арабских странах, стремящихся к этому?

3. Цель исследования

Исследование направлено на:

Знать требования для достижения кибербезопасности в информационных системах управления в некоторых арабских странах.

Важность исследования:

Важность исследований заключается в самих исследованиях, поскольку образовательные исследования в области кибербезопасности по-прежнему ограничены, а террористические атаки продолжаются и могут усилиться по мере технологического развития и революции знаний. Также кажется важным искать рекомендации и предложения, которые поддерживают кибербезопасность информационных систем управления арабских стран.

Искать термин:

Кибербезопасность: «Все процедуры, меры, методы и инструменты, используемые для защиты безопасности сетей, программного обеспечения и информации от атак, потери или незаконного доступа, а также для защиты устройств и данных».

4. Теоретическая основа и предыдущие исследования

Предыдущие исследования:

Арабский институт планирования (2019 г.) Исследование рисков и экономических последствий кибератак: пример стран Персидского залива.

В этом исследовании была предпринята попытка подчеркнуть важность электронных рисков и их экономические последствия, способы управления ими и международные модели инцидентов. Затем он решил и оценил ситуации стран Персидского залива в качестве модели или тематического исследования, направленного на повышение интереса к инвестициям в кибербезопасность и устранение пробелов в экономическом планировании для устранения этих рисков. Другие страны Персидского залива лидируют по некоторым типам кибератак на экономическую деятельность, например, по количеству

вредоносного ПО в электронной почте и количеству спама. Убытки от кибератак в странах Персидского залива также превышают средний мировой уровень. Хотя эффективность стран Персидского залива в противодействии кибератакам улучшилась, в Руководстве Организации Объединенных Наций по глобальной кибербезопасности указывается, что существует множество правовых, технических, организационных, учебных и совместных пробелов, которые необходимо заполнить путем улучшения эффективности, завершения и анализа текущей ситуации в странах Персидского залива. это уважение. Одного увеличения расходов недостаточно для устранения угроз и обеспечения кибербезопасности в странах Персидского залива. Осведомленность, управление и процессы необходимо улучшить, поскольку этот регион является одним из самых передовых регионов мира в быстром внедрении современных технологий.

Исследование Шетти (2019 г.) по оценке политики информационной безопасности и конфиденциальности в образовательных учреждениях Саудовской Аравии с применением в Университете Касима.

Исследование выявило необходимость в программах повышения осведомленности персонала, поощрении исследований в области кибербезопасности, а также важность интеграции и оценки данных в образовательных учреждениях.

Исследование (2020) Эль Хисси

В исследовании была предпринята попытка предложить структуру управления кибербезопасностью в государственных университетах Марокко. Он пришел к выводу, что использование кибербезопасности в академических учреждениях принесет множество административных, материальных и академических преимуществ.

Исследование Аль-Отаиби (2017 г.) о роли кибербезопасности в повышении безопасности человека:

Проблема исследования заключалась в том, чтобы ответить на вопрос президента: какова роль кибербезопасности в повышении безопасности человека?

Исследовательское сообщество состоит из специалистов по кибербезопасности филиала Saudi Aramco в регионе Эр-Рияд (400 случайно выбранных человек). В исследовании использовалась аналитико-описательная учебная программа.

Одним из наиболее важных выводов исследования является:

• Технические процедуры защиты киберпространства компании в значительной степени доступны, поскольку система блокируется, если не используется в течение определенного периода времени.

• Технические процедуры компании по защите киберпространства в значительной степени доступны с использованием биометрических данных (отпечатков пальцев глаз, отпечатков пальцев и звуковых отпечатков пальцев) для санкционированного прохода.

Исследователь рекомендовал использовать научные и практические средства обеспечения кибербезопасности для государственных и частных учреждений и компаний. Он также рекомендовал продолжить изучение связи между кибербезопасностью и безопасностью человека.

Исследование Бакри (2017)

Об информационной безопасности в суданских университетских библиотеках. Целью этого было выявить риски, связанные с отсутствием защиты информации, и способы ее защиты для университетских библиотек. В исследовании использовалась учебная программа по истории, просмотр опубликованной литературы и инструмент наблюдения за университетскими библиотеками Судана.

Исследование (Рехман, 2016 г.)

Что касается реалий систем управления кибербезопасностью в высших учебных заведениях и университетах Пакистана, было рекомендовано внедрить систему управления рисками и разработать политику безопасности для устранения этих рисков.

Предыдущие исследования в области кибербезопасности кажутся ограниченными, но научные исследования и теоретическая литература также подчеркивают необходимость изучения кибербезопасности во многих и

меняющихся формах. Нынешнее исследование также движется в том же направлении, чтобы продвигать идею и культуру кибербезопасности, особенно в университетской сфере, где она почти полностью ограничена.

5. Кибербезопасность

Концепция кибербезопасности:

Значение слова кибер

Киберпространство — это связь между Интернетом и компьютерами, а это означает современные технологии. Речь идет о компьютерных сетях, Интернете и различных приложениях, таких как WhatsApp, Facebook и сотнях других приложений.

Информационная безопасность:

Кибербезопасность направлена на защиту вещей с помощью ИТ, таких как аппаратное и программное обеспечение, которое называется информационными и коммуникационными технологиями (ИКТ).

Кибербезопасность означает принятие необходимых мер для защиты киберпространства от кибератак с помощью различных технологических средств. Целью является систематическое и административное предотвращение несанкционированного доступа, незаконного использования и систематического злоупотребления электронной информацией. Это делается для обеспечения непрерывности доступных систем и информации в них, а также для защиты конфиденциальности и конфиденциальности путем соблюдения необходимых мер и процедур для защиты данных.

Терминология кибербезопасности:

В основе кибербезопасности лежит множество концепций. Он определяется как «набор защитных решений перед лицом кибератаки и ее последствий, включая реализацию необходимых контрмер».

Это то, что Нейттаанмаки Пекка и Лето Артти изложили в своей книге «Анализ, технологии и автоматизация кибербезопасности», описывая кибербезопасность как «защиту от пиратских атак и их последствий, включая реализацию необходимых контрмер», которая определяется как серия действий. быть взятым.

Эдвард Аморосо определил Эдвард как способ снизить риск атак на программное обеспечение, компьютеры или сети, включая инструменты, используемые для борьбы с пиратством, обнаружения и остановки вирусов, а также обеспечения зашифрованной связи.

В Отчете МСЭ о направлениях реформирования связи на 2010–2011 годы Сообщество кибербезопасности «использует ряд задач, таких как составление инструментов обеспечения безопасности, политики, решений, руководящих указаний, методов кризисного управления, образования, практики, передового опыта и технологий, которые можно использовать для защитить киберпространство, корпоративные активы и пользователей». Министерство обороны США дает четкое определение термина «кибербезопасность». То есть «все нормативные решения, необходимые для защиты информации во всех ее физических и электронных формах от различных преступлений и атак шпионских программ».

Европейская декларация также показала, что кибербезопасность — это способность информационных систем противостоять попыткам проникнуть в их стены.

Обратите внимание, что кибербезопасность — это глубокая концепция информационной безопасности. Кибербезопасность связана с безопасностью всего, чего нет в Интернете, а информационная безопасность не такая. Это связано с безопасностью «бумажной» информации, тогда как кибербезопасность не такая [5].

Понятия, связанные с кибербезопасностью:

Существует множество концепций, связанных с кибербезопасностью, в первую очередь:

Киберпространство: Французское агентство по безопасности медиасистем (ANSSI) определило его как «коммуникационное пространство, демонстрируемое посредством глобальной связи методов сбора цифровой информации», очень сложную интерактивную среду, включающую физические и нефизические элементы, состоящую из ряда цифровых устройств, сетевых

систем, программного обеспечения и пользователей, которые были важными операторами или пользователями».

Угрозы кибербезопасности и их последствия:

Существует множество типов угроз кибербезопасности, с которыми страны по всему миру столкнулись и атаковали свои сектора, такие как фишинг, вредоносное ПО, программы-вымогатели, шпионское ПО, трояны, распределенный отказ в обслуживании (DDoS), Emotet, «Человек посередине» и SQL-инъекция.

Угрозы кибербезопасности становятся все более серьезными. Таким образом, эти угрозы могут привести к отключениям электроэнергии, сбоям в работе военной техники и утечкам секретной информации. Они могут привести к краже бесценной и частной информации, включая медицинские записи. Они могут вывести из строя системы, обездвижить телефонные и компьютерные сети и предотвратить доступ к данным. Не будет преувеличением предположить, что киберопасности могут повлиять на то, как устроена жизнь в том виде, в каком мы ее знаем в настоящее время.

Чтобы защитить персональные данные от этих угроз, необходимо учитывать множество потенциальных ролей:

• Создайте резервную копию данных.

• Поддерживайте актуальность программного и аппаратного обеспечения.

• Выбирайте надежные пароли.

• Включите двухфакторную аутентификацию.

• Используйте оригинальность в вопросах и ответах на восстановление учетной записи.

• Избегайте важных транзакций через общедоступную сеть Wi-Fi.

• Будьте осторожны при разглашении личной информации в Интернете.

• Установите антивирусную программу и выполняйте регулярные проверки на вирусы.

• Используйте социальные сети с умом.

6. Итак, требования к приложению

Многие финансовые и коммерческие учреждения создают специализированные организационные подразделения для управления информацией и безопасности либо через одно организационное подразделение для управления и защиты информации, либо через два отдельных подразделения управления информацией, одно из которых занимается управлением информационной безопасностью. Подразделение управления информацией (IMU) включает процессы для источников данных, информации и процессов, а также их связь с целями. Подразделение управления информационной безопасностью включает в себя операции по защите информации, наблюдение и защиту компьютерного оборудования, а также реагирование на события безопасности. В состав этого подразделения входит специальный центр, называемый Операционным центром кибербезопасности [4].

Для реализации этой структуры каждому учреждению необходимо будет определить лиц, ответственных за проведение этих процессов и мероприятий. Поскольку шкала COBIT 5 в первую очередь касается этих операций и событий, таблица распределения ответственности RACI руководствуется этим масштабом этих процессов и действий внутри различных организационных подразделений. Это сделано для того, чтобы дисциплины, необходимые для кибербезопасности, могли определяться Таблицей распределения должностей в области кибербезопасности NIST.

Для улучшения управления информационной безопасностью учреждений необходимо сделать следующее:

1) Развитие эффективного управления информацией в каждой организации через новое организационное подразделение для:

• Строить и управлять структурой цепочек целей от институциональных целей до организационных подразделений.

• Строить и управлять структурой операций в этих учреждениях, их отношениями друг с другом и их взаимосвязью со структурой целей.

• Построение и управление структурой данных и информации предприятия, их взаимоотношениями друг с другом, а также местами создания, использования, передачи, хранения и уничтожения.

2) Развитие управления информационной безопасностью путем сосредоточения работы в новом центральном подразделении на:

• Построение и управление структурой полномочий доступа и обработки данных в соответствии с таблицами классификации информации.

• Создавать и управлять структурой и полномочиями пользователей данных.

• Последующие действия по внедрению и изменению политик, связанных с безопасностью и защитой информации, таких как политика безопасности и защиты информации и связанные с ней политики, совместно с соответствующими органами.

• Изучение и оценка рисков информационной безопасности совместно с соответствующими организациями.

• Обеспечить соответствие деятельности учреждения международным и национальным законам и законодательству в отношении обработки информации.

• Выполнение требований советов директоров относительно их требований к безопасности и защите информации на предприятии, а также разработка и обновление стратегии и политики безопасности и защиты информации соответственно.

3) Повысить эффективность управления кибербезопасностью через отдельное организационное подразделение для:

• Выполнить необходимые технические процедуры для защиты компьютерной инфраструктуры в соответствии с требованиями и политиками безопасности.

• Постоянный мониторинг и мониторинг безопасности компьютерной инфраструктуры через Центр управления безопасностью.

• Обеспечить эффективность систем и процедур обнаружения событий безопасности в компьютерной инфраструктуре.

• Реагировать на события безопасности и внедрять необходимые процедуры для борьбы с ними и минимизировать их влияние в рамках планов обеспечения непрерывности бизнеса.

• Работать со всеми соответствующими органами для восстановления компьютерной инфраструктуры в обычном режиме.

7. Заключение

Таким образом, кибербезопасность является одним из наиболее важных элементов безопасности в развитых странах. Тем более, что существует общая тенденция к кибербезопасности во всех аспектах жизни, я обнаружил, что идея кибербезопасности основана на защите критически важных объектов, таких как информационная инфраструктура страны. Информационные системы, включая системы управления электронным правительством, находятся в ведении ключевых государственных ведомств. Как и в случае с экономическими, научными, коммерческими и другими системами, угрозы — это угрозы национальной безопасности страны. Таким образом, мы обнаружили, что многие страны готовят институты, способные интегрировать кибербезопасность в защиту, развитие и информационную безопасность. Эта концепция стала самой важной заботой развитых стран, которые обеспечили все научные возможности и системы для ее достижения.

Электронная информационная сеть стала неотъемлемой частью повседневной жизни во всех местах. Помимо личного использования, цифровая информация используется, обрабатывается, хранится и передается. По мере увеличения и распространения этой информации мы обнаружили, что ее защита становится более важной и оказывает эффективное влияние на национальную безопасность и технический прогресс.

Литература

1. Красов А. и соавт. Использование методов математического прогнозирования для оценки нагрузки на вычислительные мощности сети IoT // 4-я Международная конференция по будущим сетям и распределенным системам (ICFNDS). – 2020. – С. 1-6.

2. Гельфанд А. М. и др. ИНТЕРНЕТ ВЕЩЕЙ (IoT): УГРОЗЫ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ДЕТЕКТИРОВАНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ //Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. СРАВНЕНИЕ МЕТОДОВ ОБУЧЕНИЯ СВЁРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.

Literature

1. Krasov A. et al. Using mathematical forecasting methods to assess the load on the computing power of the IoT network // 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. INTERNET OF THINGS (IoT): THREATS TO SECURITY AND PRIVACY //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. A study of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. ANALYSIS OF MACHINE LEARNING METHODS FOR DETECTING ANOMALIES IN NETWORK TRAFFIC //Digitalization of education: theoretical and applied research of modern science. - 2021. – pp. 33-37.

5. Kosov N. A., Timofeev R. S. COMPARISON OF TRAINING METHODS FOR CONVOLUTIONAL NEURAL NETWORKS //Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.

Для цитирования: Голубятников А.О. ТРЕБОВАНИЯ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ// Научный сетевой журнал «Столыпинский вестник» №2\2024