НАУЧНЫЙ ФОРУМ
nauchforum.ru

ISSN 2618-9402

LVIII Студенческая международная заочная научно-практическая конференция

ТЕХНИЧЕСКИЕ И МАТЕМАТИЧЕСКИЕ НАУКИ. СТУДЕНЧЕСКИЙ НАУЧНЫЙ ФОРУМ

№2(58)

г. МОСКВА, 2023

ТЕХНИЧЕСКИЕ И МАТЕМАТИЧЕСКИЕ НАУКИ. СТУДЕНЧЕСКИЙ НАУЧНЫЙ ФОРУМ

Электронный сборник статей по материалам LVIII студенческой международной научно-практической конференции

№ 2 (58)
Февраль 2023 г.

Издается с февраля 2018 года

Москва
2023

УДК 62+51
ББК 30+22.1
Т38

Т38 Технические и математические науки. Студенческий научный форум. Электронный сборник статей по материалам LVIII студенческой международной научно-практической конференции. – Москва: Изд. «МЦНО». – 2023. – № 2 (58) / [Электронный ресурс] – Режим доступа. – URL: https://nauchforum.ru/archive/SNF_tech/2(58).pdf

Электронный сборник статей LVIII студенческой международной научно-практической конференции «Технические и математические науки. Студенческий научный форум» отражает результаты научных исследований, проведенных представителями различных школ и направлений современной науки.

Данное издание будет полезно магистрам, студентам, исследователям и всем интересующимся актуальным состоянием и тенденциями развития современной науки.

ISSN 2618-9402

ББК 30+22.1

Оглавление

Секция 1. Технические науки **4**

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ В ЭНЕРГЕТИКЕ 4
Дарьяновский Алексей Алексеевич
Соколов Олег Аркадьевич

ПРОТОКОЛЫ СЕТЕВОЙ БЕЗОПАСНОСТИ 9
Кузьменко Григорий Сергеевич
Гиш Татьяна Александровна
Пелешенко Виктор Сергеевич
Андрусенко Юлия Алексеевна

ОЦЕНКА ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИИ ФЕДЕРАЛЬНОГО ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В УСЛОВИЯХ ПЕРЕХОДА НА ОТЕЧЕСТВЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ 17
Орлова Елена Валерьевна
Сизов Валерий Александрович

СЕКЦИЯ 1.

ТЕХНИЧЕСКИЕ НАУКИ

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ В ЭНЕРГЕТИКЕ

Дарьяновский Алексей Алексеевич
студент,
Санкт-Петербургский государственный университет
гражданской авиации
имени Главного маршала авиации А.А. Новикова,
РФ, г. Санкт-Петербург

Соколов Олег Аркадьевич
научный руководитель, канд. техн. наук,
доцент кафедры №13
Системы автоматизированного управления,
Санкт-Петербургский государственный университет
гражданской авиации
имени Главного маршала авиации А.А. Новикова,
РФ, г. Санкт-Петербург

Введение

В наше время из-за роста энергетических систем, с которыми работает человек, происходят трудности в восприятии информации, и из-за этого возникает большая необходимость повысить эффективность процесса обработки входящей и исходящей информации при управлении техническим и экономическим процессами.

Нужность в усовершенствовании и оптимизации технологических процессах в технике и экономике необходима для снижения работы персонала на производство и управление. Именно вся совокупность тех. средств совместимо с электронными вычислительными машинами (ЭВМ) повышает эффективность. ЭВМ выступает, как качественная средство, которое запоминает, накапливает и быстро перерабатывает информацию. Но абсолютно все функции ЭВМ могут

функционировать только при тех математических программах, который задаёт человек.

В общем и целом, Автоматизированные системы управления (АСУ) – это та система, которая получает и обрабатывает информацию. Помимо этого, АСУ использует различные автоматические и автоматизированные устройства, но не смотря на это, все основные управленческие функции выполняет человек. Слово “Автоматизированная” подразумевает собой обязательное присутствие людей при основных функциях. Эту систему часто называют эргатической, либо человеко-машинная система. Они очень повышают эффективность в управлении, которая зависит с экономической эффективностью, так как это управление имеют две части: технические и экономические.

Отраслевые Автоматизированные системы управления:

Отраслевая Автоматизированная система управления (далее ОСАУ) – это определенный ряд административных и математико-экономических средств и методов, средства связи и вычислительных техник, которые определенным органам могут позволить применить определенные оптимальные руководство данной отрасли.

Отраслевые АСУ могут характеризовать огромное число информационных источников и их распределение (географическое).

Также у Отраслевых АСУ присутствуют задачи:

1. Оптимизировать текущие предстоящие планы развития определенного предприятия промышленности;

2. Повысить темпы развития отдельной отрасли в определенной промышленности;

3. Совершенствовать составы промышленных объектов, комплексов и тд.

Все эти задачи решаются благодаря осуществлению традиционными процедурами обработки данных, которые заключаются в выводе в видах неких машинных программ. В отраслевых АСУ большая часть информации присутствует в ЭВМ (в их памяти), и они участвуют в процессах плановых и экономических расчетах.

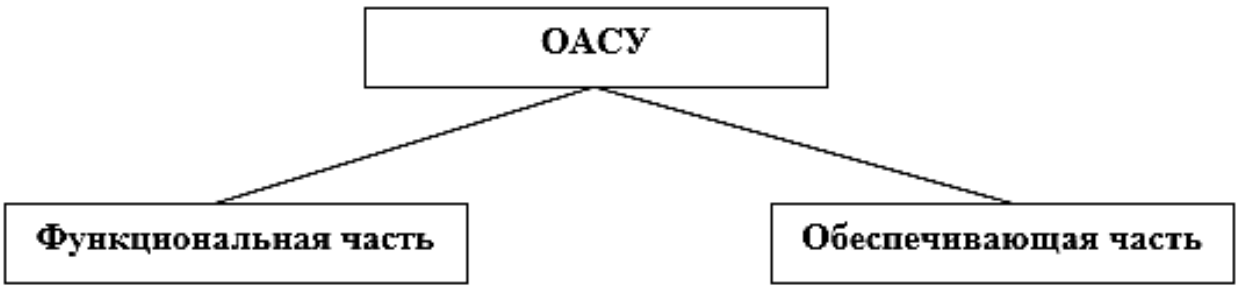

Рисунок 1. Составляющие части отраслевых автоматизированных систем управления

Отраслевая Автоматизированная система управления имеет две части:

1. Функциональная;

2. Обеспечивающая:

Функциональная часть – она имеет организационные и комплексы экономических методов, которые в целом могут обеспечить и решить задачи оперативных и перспективных планирований, а также их учет и анализ экономических-технических покахателей.

Обеспечивающая часть – она имеет информационные, технические и другие определенные виды обеспечения, которые в свою очередь могут быть характерны практически для любой автоматизированной системы информации, которая имеет организационный тип.

АСУ в электрических частях электростанции:

В данное время присутствует очень большое развитие атомной энергетике, создано очень много мощных ГЭС (гидравлических электростанций), ТЭС (тепловых электростанций) и АЭС (атомных электростанций). Такие дальние сооружения для электропередач очень высокого напряжения могут сильно осложнить задачи для диспетчерского пункта управления, как для отдельных территорий, так и для управления энергосистемы всей страны.

Для упрощения задач основных направлений совершенствований технологических и экономических процессов существует автоматизированные системы управления технологическими процессами (АСУ ТП) энергоблоков, автоматизированные системы диспетчерского управления (АСДУ), широкие использования

ВТ (вычислительной техники) и создание тех автоматизированных систем управление, которые взаимодействуют с режимами нормальной и аварийной эксплуатации на базе определенных микро-ЭВМ.

Вся информация о режимах и работе определенного энергоблока выдается благодаря расчетам техническим-экономическим показателям (ТЭП). Но тэп рассчитывают из показателей, которые были сняты с прошлого времени из-за чего становятся бесполезными в определенно сложных ситуациях, к примеру, когда в процессе очень быстро меняются определенные нужные для работы параметры.

Для того, чтобы обеспечить более стабильную работу энергоблоков или иных важных объектов, нужно выбирать оптимальные условия управления противоаварийной автоматики и системами, которые регулируются автоматически. Практически все аварийные ситуации, при их появлении, часто приводят к энерго колебаниям, то есть происходит дисбаланс мощности в энергосистеме.

На 1ом этапе: Всегда возникают наимощнейшие колебания параметров режима, в последствии чего происходит нарушение их динамической устойчивости. В среднем этот процесс длится от 5 до 10 секунд.

На 2ом этапе: Медленно изменяется частота, в процессе изменения которой происходит перераспределение потоков мощности, в следствии чего через 30 секунд – 5 минут происходит нарушение статической устойчивости после аварийных режимов.

Чтобы решить эти задачи управления с сохранением устойчивости этих после аварийных режимов, имеются моделирование аварийных ситуаций, моделирование переходных процессов и разработка методов решений проблем после аварийных процессов. Чтобы выбрать правильное управляющие воздействие, которое обеспечивает правильную работу энергосистем, необходим определенный анализ режимов, которые установились в моделировании после аварийного режима, для чего и применяется микро-ЭВМ и микропроцессы. Их достоинства заключаются в том, что они очень надежны, не очень дорогие, просты в обслуживании большой объем памяти и большая производительность.

Заключение

Исходя из совокупности всех факторов и учитывая все эти условия, которые сложились в данной ситуации, можно сделать вывод, что АСУ в энергетике является одним из важнейших действий в автоматизации многих систем, которое позволяет надежно, а что самое главное, практически безопасно работать, обеспечивать электроэнергию, при этом затраты на их обслуживание сведено к минимуму, что позволяет использовать их с очень высокой эффективностью.

Список литературы:

1. Гидроэлектростанции» – В.И. Брызгалов, Л.А. Гордон, Красноярск, 2002г
2. «Электрическая часть электростанций и подстанций» (Справочные материалы для курсового и дипломного проектирования). – 3-е изд., перераб. и доп. М.: Энергия, 1978.
3. http://foraenergy.ru, URL: http://foraenergy.ru/1–8-1-avtomatizirovannye-sistemy-upravleniya-asu-dolzhny-obespechivat-reshenie-zadach
4. http://engineeringsystems.ru, URL
5. http://engineeringsystems.ru/gidroelektrostancii/asu-v-energetike.p

ПРОТОКОЛЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

Кузьменко Григорий Сергеевич
студент,
Северо-Кавказский федеральный университет,
РФ, г. Ставрополь

Гиш Татьяна Александровна
научный руководитель, доцент кафедры
информационной безопасности автоматизированных систем,
Северо-Кавказский федеральный университет,
РФ, г. Ставрополь

Пелешенко Виктор Сергеевич
научный руководитель, доцент кафедры
информационной безопасности автоматизированных систем,
Северо-Кавказский федеральный университет,
РФ, г. Ставрополь

Андрусенко Юлия Алексеевна
научный руководитель, преподаватель кафедры
информационной безопасности автоматизированных систем,
Северо-Кавказский федеральный университет,
РФ, г. Ставрополь

1. Механизмы безопасности на сетевых уровнях

Безопасность на *прикладном* уровне − меры безопасности, используемые на этом уровне, зависят от конкретного приложения. Для различных типов приложений потребуются отдельные меры безопасности. Для обеспечения безопасности прикладного уровня приложения необходимо модифицировать. Примером протокола безопасности прикладного уровня является **SSH** – это протокол разрешающий реализовывать удаленное управление ОС и туннелирование TCP-соединений. Основной недостаток состоит в том, что на прикладном уровне в общем случае невозможно предотвратить несанкционированное событие, т.к. контролируется сам факт того, что событие произошло, поэтому на подобное событие лишь можно отреагировать (максимально оперативно), с целью минимизаций последствий.

Безопасность на *транспортном* уровне − меры безопасности на этом уровне могут использоваться для защиты данных в одном сеансе связи между двумя хостами. Наиболее распространенными протоколами являются **TLS** и **SSL.** Безопасность на *сетевом* уровне − меры безопасности на этом уровне могут использоваться во всех приложениях. В некоторых средах протокол безопасности сетевого уровня (**IPSec**) обеспечивает гораздо лучшее решение, чем элементы управления транспортного или прикладного уровня, из-за трудностей добавления элементов управления в отдельные приложения. Однако протоколы безопасности на этом уровне обеспечивают меньшую гибкость связи, которая может потребоваться некоторым приложениям.

1.1. Протоколы защиты прикладного уровня

SSh – это протокол разрешающий реализовывать удаленное управление ОС и туннелирование TCP-соединений. Протокол похож на работу Telnet, но в отличии от них, шифрует все, даже пароли. Протокол работает с разными алгоритмами шифрования. *SSH*-соединение может создаваться разными способами:

- реализация socks-прокси для приложений, которые не умеют работать с ssh-туннелями
- VPN-туннели также могут использовать протокол ssh

Обычно протокол работает с 22 портом. Также протокол использует алгоритмы электронно-цифровой подписи для реализации аутентификации. Также протокол подразумевает сжатия данных, но используется редко и по запросу клиента.

Безопасная реализация SSH:

- запрещение подключение с пустым паролем
- выбор нестандартного порта для ssh-сервера
- использовать длинные ключи более 1024 бит

1.2. Протоколы защиты транспортного уровня

Протоколы **SSL** и **TLS**

Сразу нужно отметить, что это один и тот же протокол. Сначала был *SSL*, но его взломали, он был доработан и выпущен как *TLS*. Конфиденциальность реализуется *шифрованием* данных с реализацией симметричных сессионных ключей. Сессионные ключи также *шифруются*, только на основе открытых ключей взятых из сертификатов абонентов. Протокол *SSL* предполагает следующие шали при установке соединения:

1. аутентификация сторон
2. согласование криптоалгоритмов для реализации
3. создание общего секретного мастер-ключа
4. генерация сеансовых ключей на основе мастер-ключа

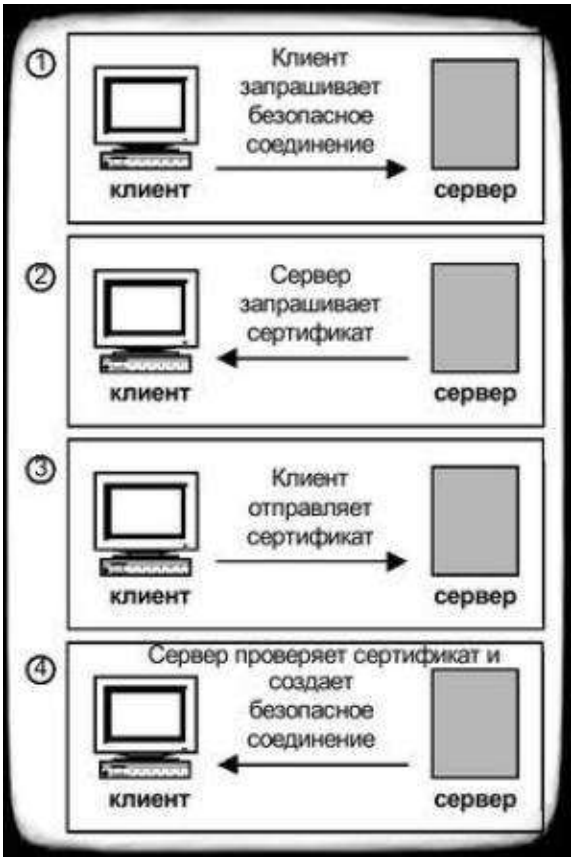

Рисунок 1. Процесс аутентификации клиента сервером с помощью протокола SSL

Следует отметить, что *TLS* и *SSL* работают только с одним протоколом сетевого уровня – IP.

Протокол **SOCKS**

Протокол *SOCKS* реализует алгоритмы работы клиент/серверных связей на транспортном уровне уровне через сервер-посредник или прокси-сервер. Такой алгоритм уже разрешает создавать функцию трансляции сетевых IP-адресов NAT. Замена у исходящих пакетов внутренних IP-адресов отправителей разрешает скрыть топологию сети от 3 лиц, тем самым усложняя задачу несанкционированного доступа.

С помощью этого протокола межсетевые экраны и VPN могут реализовывать безопасное соединение между разными сетями. Относительно спецификации протокола *SOCKS* разделяют SOCKS-сервер, который ставят на шлюзы сети, и SOCKS-клиент, который ставят на конечные узлы.

Схема создания соединения по протоколу SOCKS v5 описана следующими шагами:

1. Запрос клиента перехватывает SOCKS-клиент на компьютере
2. После соединения с SOCKS-сервером, SOCKS-клиент отправляет все идентификаторы всех методов аутентификации, которые он может поддержать
3. SOCKS-сервер выбирает один метод. Если сервер не поддерживает ни один метод, соединение разрывается
4. Происходит процесс аутентификации
5. После успешной аутентификации SOCKS-клиент отправляет SOCKS-серверу IP или ВТЫ нужного узла в сети.
6. Далее сервер выступает в роли ретранслятора между узлом сети и клиентом

Ограничения защиты на транспортном уровне

- Используется в ПО на основе TCP
- Заголовки TCP / IP в открытом виде.
- Подходит для прямой связи между клиентом и сервером. Не обслуживает защищенные приложения, использующие цепочку серверов
- SSL не обуславливает отказ от авторства, поскольку аутентификация клиента не является обязательной.

- При необходимости, аутентификация пользователя должна быть выполнена выше SSL.

Применение безопасности транспортного уровня имеет множество преимуществ, однако протокол безопасности, разработанный на этих уровнях, может использоваться только с протоколом TCP. Они не обеспечивают безопасность связи, реализованной с использованием UDP.

1.3. Протоколы защиты прикладного уровня

протокол **IPSec**

Главная задача протокола *IPSec* это реализация безопасности передачи информации по сетям IP.

Доступность – протокол не реализует, это входит в задачу протоколов транспортного уровня TCP. Реализуемая защиты на сетевом уровне делает такую защиту невидимой для приложений. Протокол работает на основе криптографических технологий:

- обмен ключами с помощью алгоритма Диффи-Хеллмана
- криптография открытых ключей для подлинности двух сторон, что бы избежать атак типа «человек по середине»
- блочное шифрование
- алгоритмы аутентификации на основе хеширования

IPSec позволяет защитить сеть от множества сетевых атак, откидывая чужие пакеты до того, как они дойдут к уровню IP на узле. На узел могут войти те пакеты, которые приходят от аутентифицированных пользователей.

1.4. Протоколы защиты канального уровня

Обеспечение безопасности беспроводных сетей – достаточно сложная задача. Затруднения вызваны невозможностью физически изолировать злоумышленников от сети или отследить их местоположение.

Канальный уровень в сетях Ethernet очень подвержен нескольким атакам. Наиболее распространенные атаки –

- ARP спуфинг- Подмена ARP может позволить злоумышленнику выдать себя за легитимного хоста, а затем перехватить кадры данных в сети, изменить или остановить их.
- MAC Flooding- При атаке с использованием MAC-адреса злоумышленник заполняет коммутатор MAC-адресами, используя поддельные пакеты ARP, до тех пор, пока таблица CAM не заполнится.
- Порт Кража - Атака кражи портов использует эту способность коммутаторов. Атакующий заполняет коммутатор поддельными кадрами ARP с MAC-адресом целевого хоста в качестве адреса источника.

Безопасность так же сильна, как и самое слабое звено. Когда дело доходит до сетей, уровень 2 может быть очень слабым звеном. Общая черта этих протоколов видна в реализации организации защищенного многопротокольного удаленного доступа к ресурсам сети через открытую сеть. Для передачи конфиденциальной информации из одной точки в другую сначала используется протокол PPP, а затем уже протоколы шифрования.

Протокол **PPTP**

Протокол *PPTP* определяет реализацию крипто-защищенного туннеля на канальном уровне OSI. *PPTP* отлично работает с протоколами IP, IPX или NETBEUI.

Протокол **L2TP и L2f**

Протокол *L2TP* основан на протоколе *L2F*, который был создан компанией Cisco Systems, как альтернатива протоколу *PPTP*. Протокол *L2TP* был создан как протокол защищенного туннелирования PPP-трафика через сети с произвольной средой. Этот протокол не привязан к протоколу IP, а поэтому может работать в сетях ATM (сети с асинхронным режимом транспортировки) или же в сетях с ретрансляцией кадров. Архитектура протокола видна на рисунке.

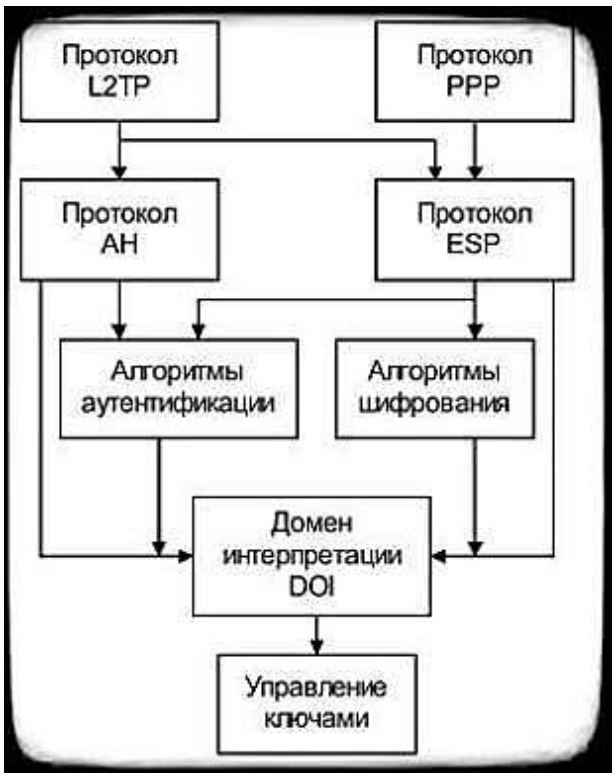

Рисунок 2. Архитектура протокола L2TP

Соединение реализуется в 3 этапа:

1. этап: производится соединение с сервером удаленного доступа локальной сети. Пользователь создает PPP-соединение с провайдером ISP. Концентратор доступа LAC устанавливает соединение, и создает канал PPP. Также концентратор выполняет аутентификацию пользователя и конечного узла. На основе имени клиента, провайдер ISP решает, нужно ли ему туннель на основе L2TP, если нужно – создается туннель.

2. этап: сервер LSN локальной сети реализует аутентификацию пользователя. Для этого может быть использован любой протокол аутентификации клиента.

3. этап: при успешной аутентификации, создается защищенный туннель между концентратором доступа LAC и сервером LNS локальной сети.

Протокол L2TP работает поверх любого транспорта с коммуникацией пакетов. Также L2TP не определяет конкретные методы криптозащиты.

Заключение

В данной статье были рассмотрены основные протоколы защиты информации в сети. Из всего вышеописанного можно сделать вывод, что для любой цели можно подобрать протокол защиты так, чтобы информация сохраняла конфиденциальность, целостность и доступность

Список литературы:

1. Протоколы сетевой безопасности ssh, ssl, tls, smtp, l2f, ipsec, l2tp, pptp, socks. // ЗИ URL: http://infoprotect.net/protect_network/protokolyi-ssh-ssl-smtp-ipsec-l2tp-pptp-socks (дата обращения 22.05.2022).
2. Сетевая безопасность // Tutorialspoint URL: https://translated.turbopages.org/proxy_u/en-ru.ru.6344e6e8-62947df0-5d6cd101-74722d776562/https/www.tutorialspoint.com/network_security/network_security_quick_guide.htm (дата обращения 22.05.2022).
3. TCP/IP – сетевая модель передачи данных // Википедия URL: https://ru.wikipedia.org/wiki/TCP/IP (дата обращения 22.05.2022).

ОЦЕНКА ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИИ ФЕДЕРАЛЬНОГО ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В УСЛОВИЯХ ПЕРЕХОДА НА ОТЕЧЕСТВЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Орлова Елена Валерьевна
студент,
Российский экономический университет им. Г.В. Плеханова,
РФ, г. Москва

Сизов Валерий Александрович
научный руководитель,
Российский экономический университет им. Г.В. Плеханова,
РФ, г. Москва

В условиях жестких санкционных ограничений существующая проблема импортозамещения в программной сфере стоит достаточно остро, так как в первую очередь существенные риски от использования зарубежного программного обеспечения грозят органам власти и управления.

Именно такая угроза - угроза несанкционированного доступа нависла над решающими стратегические задачи органами государственного и местного управления.

Следовательно, можно смело сказать, что проблема импортозамещения в программной сфере – это дело национальной безопасности и соблюдения государственной тайны.

Поэтому в настоящее время вопрос быстрого перехода отечественного управления, включая государственные органы и их учреждения на отечественное программное обеспечение должен быть разрешен как можно быстрее.

Данные факт также связан с принятием на государственном уровне ряда программных документов, включая Стратегию национальной безопасности Российской Федерации до 2030 г , Доктрину информационной безопасности Российской Федерации , Распоряжение Правительства Российской Федерации от 26 июля 2016 г. №1588 , ведомственные нормативные акты: Приказ Минкомсвязи России 20.09.2018 №486 , Приказ Министерства цифрового развития, связи и

массовых коммуникаций РФ от 4 июля 2018 г. № 335 , Приказ Минкомсвязи России от 08.05.2019 № 184 и др.

Однако, учитывая малую конкурентоспособность отечественного программного обеспечения, развитие которого долгое время не поощрялось, встает вопрос как сделать это не только быстро, но и безопасно, ведь риски существуют.

На фоне вышесказанного встает вопрос о критериях оценки эффективности обеспечения информационной безопасности, о гарантиях решения задачи не только выполнения определенного программного алгоритма, но и контроля качества его выполнения.

Рассмотрим алгоритм применения метода нечеткой логики при оценке обеспечения эффективности информационной безопасности с использованием программной среды MATLAB.

Правила нечеткой логики позволяют моделировать систему в случае невозможности применения традиционных методов, а также вместо точных математических вычислений более эффективно использовать качественные оценки состояния объекта информационной безопасности, в нашем случае Учреждения федерального органа исполнительной власти.

Вводные параметры диагностики состояния системы информационной безопасности Учреждения преобразуются с помощью программной среды MATLAB в нечеткие выходные, с использованием алгоритма нечеткого логического вывода Мамдани.

Предлагается определять состояние входных диагностических параметров состояния системы информационной безопасности (входных переменных) с помощью лингвистической переменной, принимающей два нечетких значения - хорошо и плохо.

Таким образом, нечеткая база знаний будет иметь вид:

Правило 1: если параметры xp есть «хорошо», то Y есть «высокий уровень»;

Правило 2: если параметры x1 есть «хорошо», параметр x2 есть «плохо», то Y есть «средний уровень»;

Правило 3: если параметр x1 есть «плохо» и параметр x2 есть «плохо», то Y есть «низкий уровень».

Для оценки эффективности использования нечеткой логики для диагностики технического состояния объектов при двух значениях выходной переменной используются критерии качества бинарной классификации: F-мера и критерий ***AUC.***

Таким образом, при определении ряда индикаторов системы информационной безопасности и мониторинге их состояния с помощью метода нечеткой логики программной среды MATLAB можно создать алгоритм оценки эффективности обеспечения информационной безопасности в учреждении федерального органа исполнительной власти.

Укажем, что метод нечеткой логики отнюдь не призван заменить традиционные методы диагностики системы информационной безопасности, а может удачно дополнить их, безусловно повысит точность традиционных методов.

Список литературы:

1. Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации».
2. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".
3. Распоряжение Правительства Российской Федерации от 26 июля 2016 г. №1588 Об утверждении плана перехода органов исполнительной власти и государственных внебюджетных фондов на использование отечественного программного обеспечения //Собрание законодательства Российской Федерации, 2016, №31, ст. 5068.
4. Приказ Минкомсвязи России 20.09.2018 №486 «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения».
5. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 4 июля 2018 г. № 335 «Об утверждении методических рекомендаций по переходу органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления муниципальных образований Российской Федерации на использование отечественного офисного программного обеспечения, в том числе ранее закупленного офисного программного обеспечения».

6. Приказ Минкомсвязи России от 08.05.2019 N 184 (ред. от 15.09.2021) Об утверждении методических рекомендаций по переходу предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, органам исполнительной власти субъектов Российской Федерации, органам местного самоуправления и государственным внебюджетным фондам, на преимущественное использование отечественного программного обеспечения, в том числе офисного программного обеспечения>
7. Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. 2015. №8 (224). URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-organov-ispolnitelnoy-vlasti-na-sovremennom-etape (дата обращения: 14.11.2022).
8. Дерябина О.С. Совершенствование системы информационной безопасности в органах государственной власти РФ / О.С. Дерябина. // Молодой ученый. – 2020. – № 5 (295). – С. 8-11. – URL: https://moluch.ru/archive/295/67041/ (дата обращения: 14.11.2022).

ДЛЯ ЗАМЕТОК

ТЕХНИЧЕСКИЕ И МАТЕМАТИЧЕСКИЕ НАУКИ. СТУДЕНЧЕСКИЙ НАУЧНЫЙ ФОРУМ

Электронный сборник статей по материалам LVIII студенческой международной научно-практической конференции

№ 2 (58)
Февраль 2023 г.

В авторской редакции

Издательство «МЦНО»
123098, г. Москва, ул. Маршала Василевского, дом 5, корпус 1, к. 74
E-mail: mail@nauchforum.ru

16+