ISSN 2181-6883

PEDAGOGIK MAHORAT

Ilmiy-nazariy va metodik jurnal

MAXSUS SON
(2021-yil, dekabr)

Jurnal 2001-yildan chiqa boshlagan

Buxoro – 2021

PEDAGOGIK MAHORAT

Ilmiy-nazariy va metodik jurnal
2021, maxsus son

Jurnal O‘zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi OAK Rayosatining 2016-yil 29-dekabrdagi qarori bilan **pedagogika** va **psixologiya** fanlari bo‘yicha dissertatsiya ishlari natijalari yuzasidan ilmiy maqolalar chop etilishi lozim bo‘lgan zaruruiy nashrlar ro‘yxatiga kiritilgan.

Jurnal 2001-yilda tashkil etilgan.

Jurnal O‘zbekiston matbuot va axborot agentligi Buxoro viloyat matbuot va axborot boshqarmasi tomonidan 2016-yil 22-fevral № 05-072-sonli guvohnoma bilan ro‘yxatga olingan.

Muassis: Buxoro davlat universiteti
Tahririyat manzili: O‘zbekiston Respublikasi,Buxoro shahri Muhammad Iqbol ko‘chasi, 11-uy
Elektron manzil: ped_mahorat@umail.uz

MUNDARIJA

Гулсина АТАЕВА
Старший преподаватель
Бухарского государственного университета

АНАЛИЗ ПРОГРАММ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С появлением более совершенных технологий киберпреступники также нашли больше способов проникнуть в системы многих организаций. Поскольку все больше и больше предприятий в настоящее время полагаются в своих важнейших операциях на программные продукты, важность обеспечения безопасности программного обеспечения необходимо воспринимать серьезно - сейчас, как никогда. Наличие надежной защиты, такой как программное обеспечение для ИТ-безопасности, имеет решающее значение для защиты ваших вычислительных сред и данных.

Ключевые слова: *программное обеспечение, информационная безопасность, кибербезопасность, антивирус, межсетевой экран, пароль.*

Rivojlangan texnologiylaraning paydo bo'lishi bilan kiberjinoyatchilar ko'plab tashkilotlarning tizimlariga kirishning ko'proq usullarini topdilar. Ko'proq korxonalar o'zlarining muhim operatsiyalari uchun dasturiy ta'minotga tayanar ekan, dasturiy ta'minot xavfsizligining ahamiyatiga har qachongidan ham jiddiyroq munosabatda bo'lish kerak. AT xavfsizligi dasturlari kabi kuchli himoya vositalariga ega bo'lish hisoblash muhiti va ma'lumotlaringizni himoya qilish uchun juda muhimdir.

Kalit so'zlar: *dasturiy ta'minot, axborot xavfsizligi, kiberxavfsizlik, antivirus, xavfsizlik devori, parol.*

With the advent of better technology, cybercriminals have also found more ways to infiltrate the systems of many organizations. As more and more enterprises now rely on software for their critical operations, the importance of software security must be taken seriously - now more than ever. Having strong protections, such as IT security software, is critical to protecting your computing environments and data.

Key words: *software, information security, cyber security, antivirus, firewall, password.*

Типы программного обеспечения для ИТ-безопасности. Как работает программное обеспечение для ИТ-безопасности? По сути, оно обнаруживает и, в некоторых случаях, смягчает атаки безопасности в вашей системе. Поскольку существуют различные типы атак на безопасность, существуют также различные типы продуктов безопасности, нацеленных на каждую из них. Вот некоторые из самых популярных:

Межсетевой экран. Общий термин "брандмауэр" относится к специализированным системам защиты для отдельного вычислительного устройства или компьютерной сети. Он фильтрует данные, которые поступают или покидают компьютер или сеть, блокируя или ограничивая сетевые порты от вирусов и хакеров. Он также служит барьером между надежной и ненадежной сетью, позволяя входить в сеть только трафику, определенному политикой брандмауэра. Эта утилита, служащая первой линией защиты вашего компьютера, также поставляется в еще большем количестве различных типов, таких как межсетевой экран прокси, межсетевой экран с отслеживанием состояния, межсетевой экран унифицированного управления угрозами (UTM), межсетевой экран нового поколения (NGFW) и ориентированный на угрозы NGFW.

Антивирус. Эта программная утилита предназначена для предотвращения, поиска, обнаружения и удаления вредоносного программного обеспечения или вредоносных программ, таких как вирусы, черви, вредоносное ПО и трояны. В связи с постоянным натиском новых вирусов эти программы часто обновляются, чтобы система могла проверять новые угрозы. Хотя поставщики различаются по своим предложениям, некоторые из его основных функций включают сканирование файлов и каталогов на предмет подозрительных шаблонов, планирование автоматического сканирования, сканирование определенного файла на вашем компьютере, компакт-диске или флэш-накопителе в определенный момент времени, удаление любых обнаруженных вредоносных кодов или зараженные файлы и обзор состояния вашего компьютера.

Обнаружение шпионского ПО. Шпионское ПО, также называемое вредоносным и рекламным ПО, - это программы, установленные на вашем компьютере без вашего согласия. Программное обеспечение Anti-Spyware используется для обнаружения их присутствия на вашем компьютере или в сети и предотвращения или удаления их установок. Их удаление имеет решающее значение, поскольку они «шпионят» и записывают вашу личную информацию с вашего компьютера, а также поведение компьютера, такое как ваши документы, просмотр веб-страниц и нажатия клавиш. Это может

адаптировать рекламу на вашем компьютере, изменить его конфигурацию и даже отправить ваши личные данные на другой удаленный компьютер.

Защита паролем. Одним из наиболее часто используемых методов предотвращения несанкционированного доступа к компьютеру, файлу, папке и системе является защита их паролем. Проблема наличия пароля заложена в человеческой памяти. В большинстве случаев многие люди используют легко запоминающиеся пароли, такие как дни рождения и фамилии (а во многих случаях и само слово “пароль”), что также позволяет злоумышленникам легко угадать. Кроме того, многие повторно используют один и тот же пароль на разных платформах, что подвергает риску все ваши учетные записи, даже если взломана только одна. С другой стороны, сложно запомнить уникальный пароль, который сложно угадать в каждой учетной записи. Вот где защита паролем пригодится для создания надежных паролей и их безопасного хранения.

Особенности программного обеспечения для ИТ-безопасности. Что делает программное обеспечение для ИТ-безопасности? Вот некоторые из ключевых функций программного обеспечения безопасности:

Автоматические обновления. Это гарантирует, что вы не пропустите ни одного обновления, а ваша система будет самой последней версией, способной реагировать на постоянно возникающие новые киберугрозы.

Сканирование в реальном времени. Функции динамического сканирования упрощают обнаружение и быстрое проникновение вредоносных объектов. Без этой функции вы рискуете не предотвратить повреждение вашей системы до того, как это произойдет.

Автоматическая очистка. Функция, которая избавляет себя от вирусов, даже если пользователь вручную не удаляет вирус из зоны карантина при обнаружении. Если вам не нужна возможность проверки вредоносного ПО, нет причин хранить вредоносное ПО на вашем компьютере, что делает эту функцию важной.

Множественная защита приложений. Эта функция обеспечивает защиту всех ваших приложений и сервисов, будь то электронная почта, программа обмена мгновенными сообщениями и интернет-браузеры, среди прочего.

Безопасность на уровне приложений. Это позволяет вам контролировать доступ к приложению для отдельных ролей или отдельных пользователей, чтобы гарантировать, что только нужные люди могут войти в соответствующие приложения.

Ролевое меню. При этом отображаются пункты меню, показывающие разных пользователей в соответствии с их ролями, что упрощает назначение доступа и управления.

Безопасность на уровне строк (мультитенантность). Это дает вам контроль над доступом к данным на уровне строк для одного приложения. Это означает, что вы можете разрешить нескольким пользователям доступ к одному и тому же приложению, но вы можете контролировать данные, которые им разрешено просматривать.

Единая точка входа. Сеанс или процесс аутентификации пользователя, который позволяет пользователям получать доступ к нескольким связанным приложениям до тех пор, пока они авторизованы в одном сеансе, путем входа только своего имени и пароля в одном месте.

Параметры привилегий пользователя. Это настраиваемые функции и безопасность для отдельных пользователей или ролей, к которым можно получить доступ в их профиле в любом приложении.

Источники данных для конкретных пользователей. Это позволяет вам создать единое приложение, которое, в зависимости от пользователя, получает доступ к различным источникам данных. То же самое и с безопасностью на уровне строк, но на уровне базы данных.

Аудит активности приложений. Жизненно важно для ИТ-отделов, чтобы быстро узнать, когда пользователь входил в систему и выходил из нее, а также к какому приложению он обращался. Разработчики могут регистрировать действия конечных пользователей, используя свои действия по входу/выходу.

Преимущества программного обеспечения для ИТ-безопасности. Зачем использовать программное обеспечение для ИТ-безопасности? Реальные преимущества программных решений для ИТ-безопасности напрямую связаны с последствиями их отсутствия. В какой-то момент даже самые технически подкованные пользователи могут загрузить какую-либо форму вредоносного ПО или стать жертвами онлайн-мошенничества и кражи личных данных. Интернет - небезопасное место, и, поскольку все больше и больше операций управляется решениями SaaS, необходимо уделять приоритетное внимание защите всей вашей организации [1, 34].

Предотвращение вирусов, шпионского ПО и кражи личных данных. Хакеры находят более хитрые способы создания вирусов, которые могут выдавать себя за антивирусное программное обеспечение, электронную почту от друга или веб-сайты банков-самозванцев. Как только они заразят ваш компьютер, они могут резко снизить скорость обработки, удалить важные данные и повредить ваш компьютер или сетевые системы. Кражу личных данных и шпионское ПО также можно предотвратить, используя программное обеспечение для защиты конфиденциальной личной информации, такой как пароли, финансовые данные, номера кредитных карт и номера социального страхования пользователей вашей системы. Фактически, 80% кибератак вызваны слабыми или украденными паролями, поэтому их необходимо тщательно защищать.

Защита ценной информации. Информация - один из самых ценных активов любой организации. Следовательно, его защита является жизненно важной частью вашей ИТ-инфраструктуры. Потеря важной информации из-за повреждения данных может нанести ущерб вашему бизнесу. Кроме того, MasterCard International Inc. и Visa USA требуют шифрования данных, чтобы бизнес мог работать, чтобы защитить клиентов при использовании их кредитных карт. Шифрование и ограничение доступа к конфиденциальной информации - это лишь некоторые из аспектов, которыми занимается безопасность информационных технологий.

Многие ИТ-отделы должны соблюдать юридические, страховые и отраслевые ограничения для управления данными и их передачи. Некоторые из наиболее важных правил, на которые следует обратить внимание, включают FIPS, PCI/DSS, Gramm-Leach Bliley, HIPAA и FISMA. Программное обеспечение безопасности обеспечивает шифрование, необходимое для обеспечения соответствия требованиям, когда к вашему файлу обращаются, делятся, распространяются на различных устройствах и отправляются из вашей системы или принимаются в ней.

Безопасность для клиентов. Безопасность и сохранность их конфиденциальной личной информации являются одними из основных проблем клиентов, из-за которых они не решаются делиться своей информацией и совершать транзакции в Интернете. При этом наличие решений безопасности гарантирует вашим клиентам, что их информация находится в безопасности.

Снижение затрат на разработку. Внедрение решения по обеспечению безопасности на раннем этапе позволяет избежать высоких затрат на этом пути. Хотя никогда не поздно установить программное обеспечение безопасности в вашу систему, чем раньше оно у вас будет, тем лучше. Если вы решите сделать это позже, вам нужно будет изменить больше кодов. Непреднамеренная потеря и извлечение данных также может стоить вам огромных денег и времени, если их не предотвратить.

Многослойный подход к безопасности. Одной защиты недостаточно для защиты вашей системы. Выбор программного обеспечения с многоуровневым подходом закрывает любые бреши в безопасности, чтобы выявлять потенциальные угрозы и предотвращать их дальнейшее повреждение. Изоляция и идентификация угроз должны быть покрыты всеми слоями. Сюда входят брандмауэры, сканеры вредоносных программ, инструменты шифрования локального хранилища и системы обнаружения вторжений.

Совместимость с потребностями вашей системы. Понимание вашей собственной ИТ-настройки, сетевых спецификаций, установок программного обеспечения и различных типов оборудования в вашей системе имеет решающее значение для составления короткого списка потенциальных пакетов безопасности, подходящих для вашей конкретной бизнес-среды. Примером может служить служба шифрования мультимедиа, которая необходима компаниям, использующим съемные носители для блокировки проникновения зараженных файлов в вашу сеть [2, 227].

Способность справляться с возникающими угрозами. Технологии и тактика киберпреступности постоянно развиваются. Если ваша система не может реагировать на новые угрозы, она бесполезна для вас и вашей системы. Адаптация и внедрение защиты от возникающих угроз должны быть важным фактором при выборе пакета ИТ-безопасности.

Не существует надежного программного обеспечения безопасности, которое бы полностью защитило вас от киберугроз. Выявление потенциальных проблем, с которыми вы можете столкнуться заранее, может помочь вам подготовиться и спланировать шаги по их решению до того, как они возникнут. Ниже приведены некоторые примеры, на которые следует обратить внимание:

Требуется более одного программного обеспечения. В зависимости от ваших требований вам может потребоваться установить несколько программ, чтобы удовлетворить все ваши потребности в кибербезопасности. Например, установка антивирусного программного обеспечения не защищает вас от взлома, потому что это не брандмауэр. Это можно смягчить, определив вашу ИТ-инфраструктуру, настройку организации, существующие программные системы и потенциальные киберугрозы.

Понимание вашей конкретной бизнес-среды может упростить поиск подходящего и полного решения, поскольку ваш выбор сузится.

Доступность сопряжена с риском. Доступность программных продуктов несет в себе как выгоду, так и риск. Когда в ваших системах используется программное обеспечение, любой может получить к нему доступ, указав правильные данные для входа и информацию. Следовательно, доступно программное обеспечение безопасности с доступом на основе ролей для контроля и ограничения доступа ваших сотрудников и подрядчиков. Очень важно использовать технологии сетевого мониторинга и веб-фильтрации, а также обучать ваших сотрудников [3, 332].

Далее приведены наиболее популярные программы, обеспечивающие кибербезопасность на вашем компьютере. Чтобы составить этот список лучшего программного обеспечения для ИТ-безопасности, было исследовано 246 популярных приложений, представленных в настоящее время на рынке, изучены их функции, простота использования, обслуживание клиентов, предлагаемые интеграции с другими системами, а также поддержка мобильных устройств с использованием запатентованного алгоритма оценки SmartScore TM . Этот рейтинг был разработан Луи Андре, специалистом в области B2B, специализирующимся на категории программного обеспечения для ИТ-безопасности [5].

1. Анализатор межсетевого экрана ManageEngine

Решение для анализа журналов и управления конфигурацией, которое позволяет пользователям управлять брандмауэрами, отслеживая трафик и обнаруживая аномалии. Он предоставляет пользователям информацию о сетевой активности и угрозах. С помощью ManageEngine Firewall Analyzer организации могут получать уведомления об угрозах и предотвращать злонамеренные атаки, а также поддерживать безопасность и оптимальность своих сетей.

2. Cloudflare

Ведущий на рынке глобальный сетевой сервис доставки контента и решение сетевой безопасности, ускоряющее работу веб-сайтов, приложений и других интернет-ресурсов; и защищает их от угроз безопасности и изощренных атак. Он имеет хорошо продуманную панель управления, упрощающую сложное управление ИТ-безопасностью. Он также автоматически оптимизирует ваши страницы и веб-сайт.

3. Malwarebytes

Malwarebytes - это программный пакет, который защищает устройства от вредоносных программ, программ-вымогателей, угроз и зараженных сайтов. Основные функции включают централизованную отчетность об угрозах, централизованное управление активами и функцию упреждающего автоматического сканирования. Благодаря передовым технологиям защиты от шпионского ПО, вредоносного ПО и руткитов вы можете обнаруживать и удалять угрозы в режиме реального времени.

4. Безопасность Spiceworks

Решение для мониторинга сети и ИТ-безопасности, которое помогает ИТ-специалистам и MSP проверять состояние своих серверов, устранять неполадки в сети и защищать свою сеть. Платформа также предоставляет пользователям различные инструменты, включая проверку работоспособности веб-сайта, сканер IP-адресов, тепловую карту отключения Интернета, проверку черного списка и репутацию IP.

5. Лаборатория Касперского.

Популярное решение для обеспечения безопасности конечных точек, которое защищает домохозяйства и предприятия от постоянно развивающихся киберугроз и атак. Он обеспечивает многоуровневую безопасность конечных точек и предотвращение мошенничества, позволяя вам управлять своей сетью с помощью хорошо продуманного интерфейса, который действует как центральный концентратор.

6. AVG AntiVirus

Лучшее антивирусное программное обеспечение и программа безопасности в Интернете, которая защищает предприятия от программ-вымогателей, вредоносных программ, шпионского ПО, хакеров и других киберугроз. AVG AntiVirus упрощает ИТ-безопасность благодаря интуитивно понятному интерфейсу и простым элементам управления. Функции безопасности включают в себя сканер ссылок, уничтожитель файлов, ловушку для камеры, защиту от кражи и мобильную безопасность.

7. Рынок обнаружения угроз SOC Prime

Threat Detection Marketplace - это платформа для кибер-контента на базе сообщества, содержащая действенный контент для обнаружения угроз, предназначенный для улучшения вашей аналитики

безопасности. Используя платформу MIRE ATT & CK и язык SIGMA, TDM в настоящее время имеет самый большой репозиторий, содержащий более 32 000 готовых и протестированных правил для обнаружения угроз, поиска угроз и реагирования на угрозы безопасности.

8. GlassWire

Брандмауэр и инструмент мониторинга сети для обнаружения угроз вашему компьютеру и сети. Он использует инструменты визуализации и информационные панели, чтобы пользователи могли быстро оценить состояние своих сетей и устройств. Он включает в себя монитор использования полосы пропускания и обнаружение изменения информации о приложении.

9. ManageEngine ADSelfService Plus

ManageEngine ADSelfService Plus - это безопасная веб-программа для сброса пароля конечного пользователя, предлагающая самостоятельную разблокировку и самообновление учетной записи. Предлагая интуитивно понятный интерфейс, он помогает компаниям сохранять свои данные в безопасности, используя дополнительные уровни безопасности. Это также упрощает управление паролями как для новичков, так и для экспертов.

10. Анализатор журнала событий

EventLog Analyzer - это пакет, который предоставляет наиболее экономичное программное обеспечение для управления информацией и событиями (SIEM) на рынке. Он помогает пользователям хранить и анализировать данные журналов, собранные из сетевых систем, приложений и устройств. Он имеет простой интуитивно понятный интерфейс, который упрощает анализ безопасности и работоспособности системы.

11. Облако предсказательной безопасности Carbon Black

Carbon Black Predictive Security Cloud - это комплексное программное обеспечение для обеспечения безопасности конечных точек, разработанное для предоставления ряда инновационных решений безопасности через облако.

12. Секретный сервер Thycotic

Thycotic Secret Server - это корпоративная программа для управления паролями. Это привилегированный менеджер паролей верхнего уровня для ИТ-администраторов. Быстрое развертывание. Легко использовать.

Литература

1. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие - М.: “Форум”, 2018. -118 с.
2. Запечников С.В. Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. Том 1. Угрозы, уязвимости, атаки и подходы к защите: Учебник для вузов. - М.: ГЛТ, 2019. - 536 с.
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие. - М.: “Риор”, 2018. - 400 с.
4. https://financesonline-com
5. https://1-it--management-financesonline-com
6. Атаева Г.И. Проблемы информационной безопасности: электронная подпись как один из способов защиты информации// Buxoro davlat universiteti ilmiy axboroti. 2018/4.
7. G.A. Isroilovna, L.Y. Djalolovna METHODS AND ALGORITHMS OF COMPUTER GRAPHICS - Scientific reports of Bukhara State University, 2020.4, 43-47pp
8. Тахиров Б.Н. АЛГОРИТМЫ ШИФРОВАНИЯ И ИХ СВОЙСТВА // Universum: технические науки: электрон. научн. журн. 2021. 11(92). URL: https://7universum.com/ru/tech/archive/item/12540