DOI https://doi.org/10.15407/usim.2019.01.068
УДК 004.9:004.75

Ю.М. ЛИСЕЦКИЙ, д-р технических наук, генеральный директор,
ДП «ЭС ЭНД ТИ УКРАИНА»,
Киев, 03680, просп. Академика Палладина, 44, Украина,
Iurii.Lysetskyi@snt.ua

КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Рассмотрены основные требования к системам информационной безопасности, описаны особенности, достоинства и недостатки, входящих в ее состав компонент. Проведен анализ наиболее распространённых информационных угроз и средств организации атак. Предложен вариант построения комплексной эшелонированной защиты корпоративной информационной системы и ее архитектура, обеспечивающая стабильную, управляемую и безопасную работу организации.

Ключевые слова: *корпоративная информационная система, информационная безопасность, компоненты, архитектура, сетевая сегментация, демилитаризованная зона, межсетевой экран, аутентификация, криптозащита, DDoS-атака, кибератака.*

Введение

При построении корпоративной информационной системы (КИС) любой современной организации она должна отвечать таким основным требованиям, как: бесперебойность работы всех служб организации; надежное хранение массивов данных и возможность их распределенной обработки; высокий уровень информационной безопасности; непрерывность в работе приложений; эффективное управление всей системой и ее ресурсами; резервирование основных элементов системы (оборудования и каналов).

Особого внимания, безусловно, заслуживают вопросы информационной безопасности, ставшие особенно актуальными в последнее время, так как КИС и особенно данные, хранящиеся в этих системах, постепенно превратились в объекты стратегического интереса [1, 2]. Это порождает бесконечный процесс поиска средств и путей для несанкционированного доступа к этим данным [3].

Для обеспечения комплексной информационной безопасности КИС необходимо построение надежной архитектуры корпоративной системы информационной безопасности.

Компоненты корпоративной системы информационной безопасности

Информация в электронном виде, к которой имеет доступ корпоративная система, должна обладать следующими свойствами:

- конфиденциальностью — доступ заранее определен и ограничен;
- целостностью — гарантируется неизменность оригинального содержания;
- аутентичностью — однозначно определять лицо (юридическое или физическое), несущее ответственность за содержание;
- достижимостью — обеспечение санкционированного доступа в определенном режиме работы (права только на чтение, права на ко-

пирование и печать фрагментов, права на отправку по электронной почте и др.).

Эти свойства и должна гарантировать корпоративная система информационной безопасности. При этом, как результат, обеспечивается защита информации от большого количества разнообразных угроз, непрерывность процессов электронной обработки информации, минимизируются нарушения жизнедеятельности корпорации.

Ранее считалось, что наличие межсетевого экрана решает почти 90 процентов проблем, связанных с возможными атаками на КИС. Однако в настоящее время, наряду с ростом ценности содержимого КИС, растет и спрос на атакующие технологии.

Сегодня арсенал средств и способов получения или уничтожения информации в КИС огромен. Кроме классических средств, позволяющих легко диагностировать удаленную систему и выявление слабых мест, появились различные варианты скрытых вредоносных программ, проникающих через почтовые системы и *Web*-сессии, маскируемых в изображениях, и др.

Поэтому современная корпоративная система информационной безопасности должна включать в себя компоненты, выполняющие различные функции и дополняющие друг друга:

- сетевая сегментация;
- межсетевые экраны;
- система аутентификации;
- криптозащита;
- система определения вторжения и реакции;
- система безопасности серверов и рабочих станций;
- антивирусная система и детального контроля контента.

Сетевая сегментация. Основа системы безопасности КИС — тщательное планирование сетевой сегментации [4]. Необходимо четко определить как зоны, требующие стандартных политик безопасности, так и специфических. Особое внимание требуется при определении правил для этих зон.

Несмотря на различные требования, все правила политики безопасности КИС должны быть единым комплексом, исключающим слабые места на стыках зон и межзонных обменах.

В большинстве случаев КИС должна иметь как минимум одну демилитаризованную зону (ДМЗ) локальной сети. Сегмент ДМЗ располагается между внешней сетью (*Internet*, *extranet*) и внутренней сетью корпорации и состоит из систем, предоставляющих такие открытые ресурсы, как информационные серверы общего доступа, почтовые серверы, серверы доменных имен и т.п. Эта зона должна быть защищена межсетевым экраном от внешней сети и контролироваться средствами определения вторжений.

Причем реакция на вторжение должна заключаться не только в тревожном оповещении, но и в экстренных мерах по пресечению доступа. Мониторинг наиболее критических систем (непосредственно влияющих на работоспособность КИС) должен осуществляться в масштабе реального времени и анализироваться средствами безопасности уровня серверов и рабочих станций.

Исходя из сложности приложений, используемых в КИС, возможно создание нескольких ДМЗ для обеспечения различного уровня доступа к ресурсам. При этом множественность ДМЗ контролируется межсетевыми экранами с использованием технологий аутентификации. Для разграничения сетевого трафика целесообразно применение сетевых коммутаторов в качестве активного сетевого оборудования.

Межсетевые экраны. Межсетевой экран рассматривается как основное средство защиты от угрозы несанкционированного (неавторизованного) доступа из внешних систем к наиболее важным информационным ресурсам КИС [5]. Он включает в себя компоненты аппаратного и программного обеспечения, реализующие политику безопасности управления сетевым трафиком между двумя и более сегментами сети, и должен реализовывать следующие виды контроля:

- разрешенные сервисы — количество сервисов, разрешенных для прохождения через межсетевой экран, должно быть минимально

необходимым для реализации функционирования определенных приложений;

▪ ограничение коммуникационных потоков — межсетевой экран должен контролировать и ограничивать направление коммуникационных потоков взаимодействующих сетевых сегментов;

▪ контроль доступа — количество систем, разрешенных для использования соответствующих сервисов, должно быть ограничено так же, как и число пользователей;

▪ контроль сообщений — для сокрытия топологии защищаемых информационных компонент межсетевой экран не должен возвращать контрольные сообщения сетевых протоколов (*host unreachable*, *port unavailable* и т.д.).

Аутентификация. Важной характеристикой защищенности КИС является уровень доверительных отношений между всеми объектами системы — пользователями, приложениями, подсистемами и т.д. Это обеспечивается системой аутентификации, обладающей необходимыми функциональными средствами проверки и предоставления конкретных прав и полномочий. Выбор определенной технологии аутентификации зависит от классификации информации, типа прикладных систем, сервисов, сетевой топологии корпорации и осуществляется на этапе планирования системы безопасности, в противном случае очень сложно гарантировать целостность выполнения политики безопасности.

Для гарантированности аутентичности возникающего информационного трафика корпорация может расширять механизм аутентификации, обеспечивая прохождение обратных транзакций к определенному запрашивающему объекту. В качестве примера можно привести системы электронной почты, контролирующие легальность сервера, запрашивающего соединение; подключение к приложениям через специальные клиенты, обеспечивающие доступ только в случае подтверждения взаимных запросов.

Криптозащита. Криптозащита является основной компонентой при обеспечении конфиденциальности электронной информации, конкретных документов и данных [6-9]. Она также используется для закрытия данных в процессе их передачи и деталей самой сессии.

Для достижения большей безопасности необходима реализация криптозащиты данных в процессах хранения и использования на стороне получателя. Например, использование специальных аппаратных ключей, содержащих в памяти цифровой сертификат пользователя, и позволяют шифровать не только трафик, но и данные, хранящиеся на локальных дисках.

Системы определения вторжения

Адаптивные системы определения вторжения представляют собой относительно новый элемент в системах защиты. Их главная цель – слежение в реальном масштабе времени за последовательными событиями как на сетевом уровне, так и на уровне приложений. Анализ событий позволяет предсказать атаки или попытки вторжения, основанные на выполнении разрешенных операций (например, через обращение к серверу доменных имен). Это дополняющие средства к межсетевым экранам, которые обычно также умеют модернизировать политику безопасности в зависимости от типа атаки. Причем, при обнаружении опасных действий осуществляется не только тревожное оповещение, но и динамически изменяются соответствующие правила для межсетевого экрана с целью их пресечения. Системы определения вторжения делятся на сетевые (исследованию подвергаются тип и содержание сетевых пакетов) и системы уровня приложений (исследованию подвергаются результаты аудита работы серверов приложений и рабочих станций). Обнаружение неавторизованного доступа (или попытки) к корпоративным ресурсам, как и их использование, определяется специальными методиками поиска:

▪ известных сигнатур атак;

▪ неадекватного поведения (на основе последовательности определенной активности пользователя или приложения).

Сетевые системы определения вторжения обычно устанавливаются в каждой зоне или

сегментах внутренней сети, контролируемых межсетевым экраном. Система должна быть сконфигурирована на работу с несколькими сетевыми контроллерами: один (или несколько) для анализа трафика, другой — для осуществления связи с консолью управления сетевой системой определения вторжения. Интерфейсы, определяющие связь систем определения вторжения с консолью, обычно выделены в отдельный сегмент локальной сети, контролируемой межсетевым экраном. Это дает ряд преимуществ:

- межсетевой экран ограничивает доступ к сегменту систем обнаружения вторжения;
- повышается производительность системы в вопросе анализа отчетов процессов обнаружения вторжения;
- исключается влияние информационного трафика (отчетов систем обнаружения вторжения) на полезный трафик.

Связь систем определения вторжения с консолью обязательно подвергается криптозащите и строгой аутентификации, системное время синхронизируется.

Системы обнаружения вторжения уровня приложений предназначены для установки на тех компонентах, которые являются информационным ресурсом и имеют классификацию критичных в нотации разработанной политики безопасности. Для правильного функционирования на исследуемых компонентах необходимо в полном объеме выполнять процессы аудита и регистрации событий.

Безопасность серверов и рабочих станций. Это самый критичный аспект в системе корпоративной информационной безопасности [10, 11]. Основным принципом поддержания безопасности серверов и рабочих станций является их правильная конфигурация с обязательной инсталляцией актуальных обновлений и изменений программного обеспечения. Однако появляются новые технологии, направленные на укрепление серверов приложений — системы, позволяющие на уровне ядра операционной системы распределить полномочия по управлению каждым приложением. В этом случае даже раскрытие пароля системного администратора не позволит получить доступ к данным или файлам конфигурации приложения, как и остановить процессы, связанные с ним. Эта же система не позволит администратору остановить работу операционной системы без согласия пользователя, ответственного за работу приложения.

Применение подобных технологий очень актуально, например, для провайдеров, предоставляющих услуги хостинга. Владельцы приложений получают возможность эксклюзивно управлять содержимым и работой приложений, но не имеют доступа к управлению ресурсами операционной системы сервера. Администраторы серверов имеют возможность полного управления работой операционной системы, но не могут влиять на работу приложений и иметь доступ к не принадлежащим им данным.

Антивирусная система и детального контроля контента. Проблема анализа контента в настоящее время приобрела дополнительную актуальность, что, прежде всего, связано с ростом интенсивности использования почтовых пересылок с прикрепленными документами. Это, с одной стороны, повышает опасность получения вирусов и вредоносных приложений, с другой — этот канал может использоваться для передачи конфиденциальной информации (как умышленно, так и случайно). Чтобы контролировать эти ситуации, современные антивирусные программы корпоративного уровня имеют специальные программные интерфейсы для стыковки с межсетевыми экранами. В этом случае весь контент-трафик проходит через антивирусный сервер, который осуществляет тщательную проверку, причем не только с целью поиска сигнатур известных вирусов, но и сигнатур, заданных администратором (например, наличие слов «конфиденциально» в тексте документов).

Требования к корпоративной системе информационной безопасности и ее архитектура

Для организации комплексной безопасности к системам защиты КИС предъявляются следующие требования [2]:

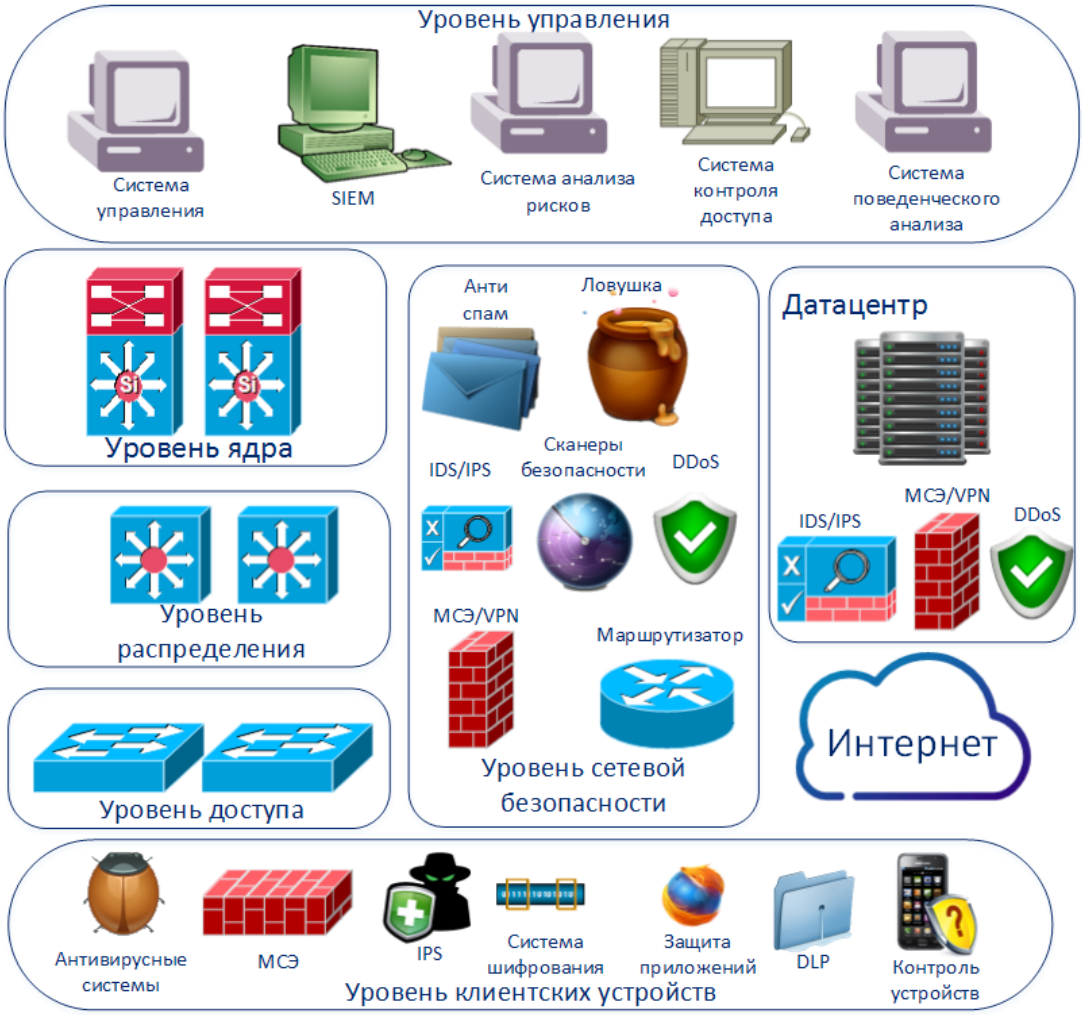

Рис. Архитектура корпоративной системы информационной безопасности

▪ обеспечение гранулированного детерминированного доступа к ресурсам корпоративной сети на основе анализа информации о *IP*-адресах, портах, используемых устройствах, типах приложений, данных геолокации;

▪ антивирусная защита передаваемой по сети информации, антиспам-защита почтовых систем;

▪ предотвращение комплексных атак и атак нулевого дня, атак типа отказ в обслуживании;

▪ предотвращение утечки критически важных данных и защита их целостности;

▪ защита от уязвимостей и угроз корпоративных порталов, *Web*-приложений, используемых для доступа к базам данных, браузеров и т.п.;

▪ централизованное согласованное управление средствами защиты;

▪ предоставление инструмента анализа рисков безопасности и ретроспективного анализа [12, 13].

Современная защищенная КИС требует внедрения целого комплекса программно-аппаратных средств. Традиционно основным инструментом являются межсетевые экраны, осуществляющие фильтрацию пакетов в соответствии с заданными правилами, динамическую трансляцию *IP*-адресов и терминацию *VPN*-соединений [5]. Кроме традиционной роли по аутентификации, авторизации и отчетности *AAA*

(*Authentication*, *Authorization*, *Accounting*) действий пользователей, в современных сетях осуществляется контроль над соблюдением политик безопасности, включая не только доступ к информационным системам, но и контроль за соответствием пользовательского устройства этим политикам (анализ версионности установленных программных продуктов, установленных обновлений, проверку актуальности антивирусной базы, контроль за целостностью файловой системы и т.д.)

Возрастающая роль *Web*-приложений в бизнес-процессах привела к появлению специализированных межсетевых экранов, направленных на контроль и защиту соответствующих приложений *WAF* (*Web-Application Firewall*). Обработка *Web*-пакетов основана на корреляции зависимостей поведения приложений и протоколов, анализа *XML/SOAP* потока и выявлении атак на уровне *Web*-трафика.

Еще одна возможность защиты — размещение ловушек (*Honeypot*). Это ресурс, специально созданный для привлечения несанкционированных действий. Проактивная система собирает информацию о действиях взломщиков и их методах, а также инструментах, используемых для атаки. Несмотря на прогресс информационных технологий, устройства периметра сети имеют физические ограничения мощности аппаратных средств и пропускной способности каналов связи. Поэтому работа КИС может быть парализована с помощью *DDoS* (*Distributed Denial of Service*) атак, направленных на отказ в обслуживании [14].

DDoS-атака представляет собой поток ложных запросов на базе различных протоколов, основной целью которого является блокировка ресурсов или сервисов КИС. Наиболее уязвимы базы данных и программные средства для доступа к ним [15]. Поэтому для защиты применяются специализированные программные продукты, обеспечивающие разграничение полномочий, логирование проводимых действий с механизмами автоматической отчетности и обладающие минимальным влиянием на производительность баз данных. В последнее время *DDoS*-атаки используют также в качестве основного инструмента реализации кибератак.

Второе по опасности место хранения корпоративной информации — это рабочий компьютер. Кроме мест хранения и интерфейса *Web*-доступа, очень важно защитить приложения, использующие критически важные данные. Чаще всего данные передаются и обрабатываются с помощью браузеров, которые уязвимы для атак типа шпион в браузере. Защититься от атак данного типа помогают программы, контролирующие интерфейс прикладного программирования (*Application Programming Interface*) браузера и выполняющие блокировку клавиатурных шпионов.

Описанный комплекс средств позволяет построить эшелонированную защиту КИС и тем самым обеспечить стабильную, управляемую и безопасную работу организации. Архитектура корпоративной системы информационной безопасности представлена на рисунке.

Заключение

В статье рассмотрены основные требования к системам информационной безопасности, описаны особенности, достоинства и недостатки, входящих в ее состав компонент.

Проведен анализ наиболее распространённых информационных угроз и средств организации атак. Комплексное использование описанных компонент, входящих в состав корпоративной системы информационной безопасности, позволяет защититься от большинства известных видов атак, а разработка эффективной и надежной архитектуры построения корпоративной системы информационной безопасности — одна из важных и актуальных задач.

REFERENCES

1. Koneev, I.R., 2003. *Enterprise Information Security.* Saint-Petersburg: BHV-Petersburg, 752 p. (In Russian).
2. Lysetskyi, Yu.M., 2016. «Some Aspects of Complex Security of Corporate Networks». Proceedings of the 5th International Scientific and Practical Conference on Informational Management Systems and Technologies, Odessa, pp. 145–148. (In Ukrainian).

3. Gerasimenko, V.A., 1994. *Protection of Information in Automatic Data Procession Systems.* Book 1. Moscow: EnergyAtomIzdat, 400 p. (In Russian).
4. Melyuk, A.A., Pazizin, S.V., Pogozhin, N.S., 2001. *Introduction to Protection of Information in Automated Systems.* Moscow: Goryachaya Liniya – Telecom, 48 p. (In Russian).
5. Ogltry, T., 2001. *Practical Application of Firewalls.* Moscow: DMD Press, 400 p. (In Russian).
6. Babenko L.K., Ischukova E.A., 2006. *Modern Algorithms of Block Cyphering and Methods of their Analysis.* Moscow: Gelios ARV, 376 p. (In Russian).
7. Tchmora, A.L., 2002.*Modern Applied Cryptography*. *2nd edition.* Moscow: Gelios ARV, 256 p. (In Russian).
8. Schneier, B., 2002. *Applied Cryptography*. Moscow: Triumph. 816 p. (In Russian).
9. Ferguson, N., Schneier, B., 2005. *Applied Cryptography*. Moscow: Williams, 424 p. (In Russian).
10. Anin, B.Y., 2000. *Protection of Computer Information.* Saint-Petersburg: BHV- Saint-Petersburg, 384 p. (In Russian).
11. Sokolov, A.V., Stepanyuk, A.V., 2002. *Manual on Protection from Computer Terrorism.* Saint-Petersburg: BHV-Saint-Petersburg, Arlit, 496 p. (In Russian).
12. Litvinov, V.V., Kazimir, V.V., Rindich, E.V., 2009. *Modern State of Information Protection in IP-Telephony*. Mathematical Machines and Systems, 2, pp.76-84 (In Ukrainian).
13. Korneev, V.V., Gareev, A.F., Vasyuti, S.V., Ie, 2001. *Databases. Intellectual Procession.* Moscow: Knowledge, 496 p. (In Russian).
14. Lysetskyi, Yu.M., 2014. «Information Security: Protection from DDoS-Attacks». Proceedings of the 16th International Conference «System Analysis and Information Technologies SAIT, Kiev, 405–406 pp. (In Ukrainian).
15. Simon, A., 1999. *Databases Strategic Technologies.* Moscow: Finance and Statistics, 484 p. (In Russian).

Received 22.02.2018

Yu.M. Lisetskyi, Dr. of Eng. Sci., General Director, DP «S&T UKRAINE»,
Prosp. Akad. Palladina, 03680, Kiev, Ukraine 44,
Iurii.Lysetskyi@snt.ua

COMPLEX SECURITY OF THE CORPORATE INFORMATION SYSTEMS

Introduction. Implementation of a corporate information system (CIS) for any modern organization requires special attention to be paid to the issue of information security. This issue has recently grown extremely important as more and more CIS and data they store become the object of strategic interest. This brought about the endless search for tools and ways of unauthorized data access. To ensure complex information security of the CIS there is to be built a reliable architecture of the corporate system of the information security.

Components of the Corporate System of Information Security. Electronic information accessed by the corporate system is to possess the following qualities: confidentiality, authenticity, integrity, accessibility. They are to be provided by the corporate system of the information security, thus, it is to contain the complementary components with different functions: network segmentation, firewalls, authentication system, cryptoprotection, intrusion detection and reaction system, server and workstation security system, anti-virus system, detailed content control system.

Requirements to the Corporate System of Information Security and its Architecture. To provide complex security there exist the following requirements to the CIS protection systems: granular determined access to corporate networks resources based on the analysis of IP-addresses, ports, devices, applications and geolocation data; anti-virus protection of the network information; anti-spam protection of the mailing systems; advanced and "zero day" threats prevention; DDoS-protection; leakage prevention and integrity protection of the critical information; protection from threats and vulnerabilities of corporate portals, Web-applications used to access databases, browsers etc.; centralized and coherent management of protection tools; provision of security risks analysis and retrospective analysis tool.

Conclusion. This way the modern CIS requires implementation of the whole complex of hardware and software devices for its protection. Complex usage of the described components of the corporate system of the information security enables protection from the most known types of attacks. It is also shown that development of effective and reliable architecture of the corporate system of information security is an important and urgent task.

Keywords*: corporate informative system, informative safety, components, architecture, network segmentation, demilitarized zone, firewall, authentification, cryptoprotection, DDoS-attack, cyber attack.*

Ю.М. Лисецкий, д-р технічних наук, генеральний директор,
ДП «ЭС ЭНД ТИ УКРАИНА», просп. Академіка Палладіна, 03680, Київ, Україна 44,
Iurii.Lysetskyi@snt.ua

КОМПЛЕКСНА ІНФОРМАЦІЙНА БЕЗПЕКА КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Вступ. При побудові корпоративної інформаційної системи (КІС) будь-якої сучасної організації особливої уваги заслуговують питання інформаційної безпеки, що стали особливо актуальними останнім часом, так як КІС і особливо дані, що зберігаються в цих системах, поступово перетворилися в об'єкти стратегічного інтересу, що породжує «нескінченний» процес пошуку засобів і шляхів для несанкціонованого доступу до цих даних. Для забезпечення комплексної інформаційної безпеки КІС необхідна побудова надійної архітектури корпоративної системи інформаційної безпеки.

Компоненти корпоративної системи інформаційної безпеки. Інформація в електронному вигляді, до якої має доступ корпоративна система, повинна мати такі властивості: конфіденційність; цілісність; автентичність; досяжність. Ці властивості і повинна забезпечувати корпоративна система інформаційної безпеки. Тому сучасна корпоративна система інформаційної безпеки повинна включати в себе компоненти, які виконують різні функції і доповнюють один одного: мережеву сегментацію; міжмережеві екрани; систему аутентифікації; криптозахист; систему визначення вторгнення і реакцію; систему безпеки серверів і робочих станцій; антивірусну систему і систему детального контролю контенту.

Вимоги до корпоративної системи інформаційної безпеки та її архітектура. Для організації комплексної безпеки до систем захисту КІС ставляться такі вимоги: забезпечення гранульованого детермінованого доступу до ресурсів корпоративної мережі на основі аналізу інформації про IP-адреси, порти, використовувані пристрої, типи додатків, даних геолокації; антивірусний захист інформації, що передається по мережі інформації, антиспам-захист поштових систем; запобігання комплексних атак і атак «нульового дня», атак типу «відмова в обслуговуванні»; запобігання витоку критично важливих даних і захист їх цілісності; захист від вразливостей і загроз корпоративних порталів, *Web*-додатків, що використовуються для доступу до баз даних, браузерів тощо; централізоване узгоджене управління засобами захисту; надання інструментів аналізу ризиків безпеки і ретроспективного аналізу.

Висновок. Таким чином, сучасна КІС для свого захисту вимагає впровадження цілого комплексу програмно-апаратних засобів. Комплексне використання описаних компонент, що входять до складу корпоративної системи інформаційної безпеки, дозволяє захиститися від більшості відомих видів атак, а розробка ефективної і надійної архітектури побудови корпоративної системи інформаційної безпеки є одним з важливих і актуальних завдань.

***Ключові слова**: корпоративна інформаційна система, інформаційна безпека, компоненти, архітектура, мережева сегментація, демілітаризована зона, міжмережевий екран, аутентифікація, криптозахист, DDoS- атака, кібератака.*