УДК 004.056.57

# ЗАЩИТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

**Дмитриев Александр Александрович**

Алтайский государственный университет, г. Барнаул
e-mail: dmitriev@asu.ru

# PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE OF AN EDUCATIONAL ORGANIZATION

**Dmitriev Alexander A.**

Altai State University, Barnaul

*Аннотация:* В статье предложены технические и программные средства для защиты образовательной организации от актуальных угроз информационной безопасности. Показано, что выбор средств защиты информации и их эффективное применение зависит от специфики деятельности организации, архитектуры сети передачи данных и используемых информационных сервисов. Для защиты сети организации от внешних атак предложено использовать межсетевой экран с расширенными функциями контентной фильтрации и встроенным потоковым антивирусом. Такое применение оборудования позволило блокировать вредоносные программы на периметре локальной сети до достижения рабочих станций сотрудников. Обеспечение защиты от эксплуатации уязвимостей в программном обеспечении компьютеров и серверов проводилось путем расширенного мониторинга работы сетевых устройств и внедрения антивирусных систем. Результаты работы могут быть использованы для защиты объектов критической информационной инфраструктуры образовательных учреждений.

*Ключевые слова:* объекты критической информационной инфраструктуры, образовательная организация, средства защиты информации.

*Abstract:* The article proposes technical and software tools to protect an educational organization from current threats to information security. It is shown that the effective use of information security tools depends on the architecture of the data transmission network and the information services used. To protect the organization's network from external attacks, it is proposed to use a firewall with advanced content filtering functions and a built-in streaming antivirus. This use of equipment made it possible to block malware on the perimeter of the local network before reaching employee workstations. Ensuring protection from the exploitation of vulnerabilities in the software of computers and servers was carried out through advanced monitoring of the operation of network devices and the implementation of antivirus protection. The results of the work can be used to protect critical information infrastructure facilities of educational institutions.

*Keywords:* critical information infrastructure facilities, educational organization, information security tools.

*Для цитирования: Дмитриев А.А. Защита критической информационной инфраструктуры образовательной организации // Проблемы правовой и технической защиты информации. 2024. № 12. С.20-24.*

*For citation: Dmitriev A.A. Protection of critical information infrastructure of an educational organization // Legal and Technical Problems of Information Security. 2024. No. 12. P.20-24.*

*Введение.* Научная и учебная деятельность высших учебных заведений повсеместно сопряжена с использованием информационных технологий. Для образовательного процесса создается разнообразный цифровой учебный контент, который используется обучающимися и преподавателями [1-2]. Выполнение научных исследований требует хранения обрабатываемых данных, а для решения производственных задач в организации используются информационные сервисы по обработке персональных данных. Обычно оборудование, на котором установлены информационные системы и базы данных, подключено к локальной вычислительной сети организации [3]. С помощью сетевого доступа обеспечивается работа пользователей и сотрудников с хранимой цифровой информацией.

В виду того, что современные крупные образовательные учреждения зачастую занимаются передовыми научными исследованиями и разработками, то базы данных с хранимой информацией, информационные сервисы и вычислительная сеть организации определяются, как объекты критической информационной инфраструктуры (КИИ). Согласно Федеральному закону "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ образовательная организация определяет комплекс технических мер по защите объектов КИИ. Однако реализация комплекса технических мер является сложной задачей в виду особенностей построения компьютерных сетей образовательных организаций, задействованного разнотипного сетевого, компьютерного оборудования и информационных сервисов, используемых в конкретной организации. В настоящей работе предложены технические меры обеспечения комплексной защиты сетевой и информационной инфраструктуры образовательной организации.

*Подходы к обеспечению защиты.* В работе рассмотрена вычислительная сеть высшего учебного заведения, показанная на рисунке 1. Компьютерная сеть, построенная по представленной топологии с перечисленными сетевым оборудованием и устройствами пользователей, является распространенным решением при создании сетей учебных организаций.

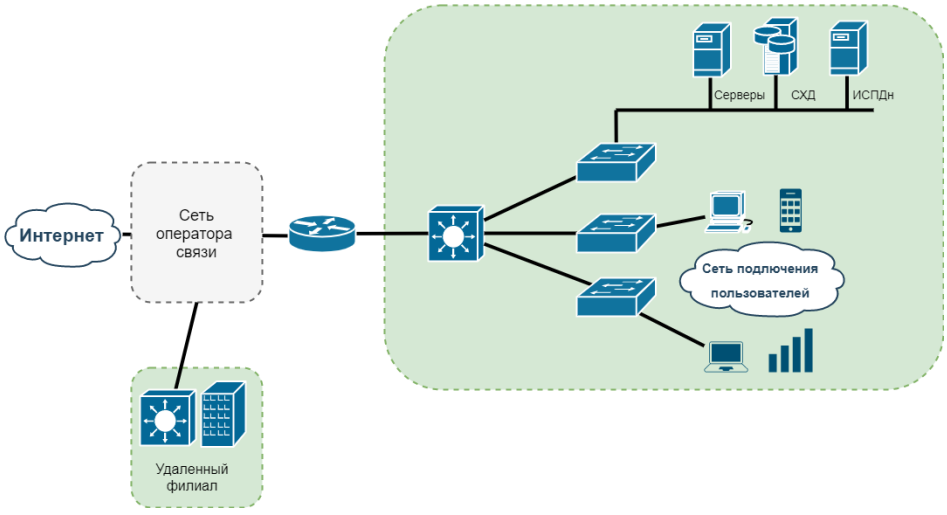


Рисунок 1. Рассматриваемая в работе локальная сеть образовательной организации

Локальная сеть построена по сетевой архитектуре с выделенным центральным маршрутизатором, с помощью которого образовательная организация подключается к сети Интернет. Через маршрутизатор проходит весь сетевой трафик, создаваемый при подключении внешних и внутренних пользователей к информационным сервисам и при работе пользователей в сети Интернет [4]. Внутренняя часть локальной сети разделена на отдельные сегменты с помощью технологии виртуальных локальных сетей. Выделена отдельная подсеть для работы сотрудников и студентов. Для подключения беспроводных устройств создана сеть Wi-Fi. Основные вычислительные сервера, на которых установлены системы управления базами данных и информационные сервисы, а также сетевые устройства хранения данных подключены в отдельную подсеть [5]. Через сеть внешнего оператора связи осуществляется сетевой обмен данными с филиалами организации, находящихся в других городах.

Текущий контроль сетевого трафика, передаваемого из организации в сеть Интернет и внутри локальной сети, реализуется средствами фильтрационных списков доступа, настроенных на маршрутизаторе. В качестве основной операционной системы компьютеров пользователей используется ОС Windows. Защита компьютеров сотрудников от действия вредоносных программ осуществляется с помощью обновления операционной системы, рабочих программ и установки антивирусного программного обеспечения.

Уязвимыми точками сетевой инфраструктуры при такой архитектуре, используемом оборудовании и программном обеспечении становятся сервера, предоставляющие информационные сервисы, например, официальный сайт организации, образовательные ресурсы, и системы обработки данных [3-4]. При проведении атак злоумышленником задействуется вредоносное программное обеспечение для взлома сервера и похищения необходимой информации. Другим подходом является проведение специальных распределенных атак на отказ в обслуживании DDOS, приводящих к потере работоспособности отдельных сетевых устройств или всей сети в целом [6-7].

Для обеспечения защиты сетевой и информационной инфраструктуры учебной организации используемые в ней методы обеспечения безопасности были дополнены за счет внедрения новых программных и аппаратных средств защиты информации. В качестве центрального маршрутизирующего устройства, обеспечивающего контролируемый доступ в сеть Интернет и фильтрацию сетевого трафика, установлен межсетевой экран Usergate E1000 [8]. Для безопасного подключения удаленных филиалов к основной сети использовано оборудование для создания защищенных каналов связи ПАК ViPNet Coordinator HW100 [9]. Усиление защиты компьютеров на рабочих местах сотрудников реализовано через переход на отечественные операционные системы на базе Astra Linux. На компьютерах сети установлено антивирусное программное обеспечение компании Kaspersky. Проведена дополнительная конфигурация коммутаторов в локальной сети для включения функций, препятствующих подключению в локальную сеть сторонних устройств пользователей. С целью контроля событий на сетевом оборудовании и анализа сетевого трафика установлено программное обеспечение для мониторинга Zabbix.

*Обсуждение.* Применение перечисленных в работе средств защиты информации позволило затруднить проведение атак на сетевую инфраструктуру образовательной организации. Установка в качестве граничного маршрутизатора сети межсетевого экрана Usergate E1000 обеспечило прохождение сетевого трафика через данное устройство. Такая установка оборудования позволила задействовать расширенные функции межсетевого экрана по фильтрации сетевого трафика [4]. Для ограничения доступа к сомнительному содержимому сайтов была включена опция

контентной фильтрации на межсетевом экране. Защита от вредоносного программного обеспечения на периметре локальной сети проводилась с помощью встроенного потокового антивируса межсетевого экрана. Подготовленные на межсетевом экране списки ip-адресов устройств, состоящих в ботнет-сетях, использовались для блокирования подключения с этих устройств к информационным и образовательным сервисам организации, что приводило к эффективному смягчению распределенных атак на отказ в обслуживание, осуществляемых из сети Интернет.

На основе оборудования ПАК ViPNet Coordinator HW100 обеспечена конфиденциальность передаваемой по сети Интернет информации между сетевыми устройствами филиалов и основной сетью образовательного учреждения [9]. Между ViPNet координаторами, которые были установлены в сетях филиала и головной организации, был создан виртуальный шифрованный канал связи. Такой способ соединения локальных сетей обеспечил безопасный доступ сотрудников филиала к информационным сервисам и системам обработки данных, находящимся в основной сети, только по защищенному соединению. Достоинством такого подхода является использования отечественных криптографических систем для обеспечения конфиденциальности и целостности данных, передаваемых через сеть Интернет.

Улучшение защиты рабочих компьютеров сотрудников осуществлено с помощью установки в качестве основной операционной системы Astra Linux и антивирусного программного обеспечения от компании Kaspersky. В организации внедрено использование технологии Port Security для предотвращения подключения к сети организации сторонних устройств пользователей. Применение этой технологии позволило закрепить персональный компьютер сотрудника за конкретным портом коммутатора сети и блокировать передачу данных в локальную сеть при включении неизвестного устройства.

*Заключение.* Описанный в работе комплекс мер по защите критической информационной инфраструктуры образовательного учреждения был представлен в рамках дискуссии международного «круглого стола» БРИКС «Цифровое общество: тенденции, возможности, риски» в Алтайском государственном университете. При обсуждении участниками дискуссии была подчеркнута важность обеспечения информационной безопасности организаций образования на территориях межгосударственного объединения. Отмечено, что описанные в статье технические и программные средства по защите информации могут использоваться для обеспечения информационной безопасности сетевой инфраструктуры образовательных учреждений. Для успешного реагирования на новые атаки злоумышленников при дискуссии было предложено дополнительное внедрение новых технологий для защиты объектов критической информационной инфраструктуры, основанных на применении искусственного интеллекта.

## Библиографический список

*1. Проталинский, О.М. Информационная безопасность вуза / О.М. Проталинский, И.М. Ажмухамедов // Вестник АГТУ. – 2009. – №1. – С. 18-24.*

*2. Ромашкова, О.Н. Анализ угроз и рисков информационной безопасности в вузе / О.Н. Ромашкова, А.И. Каптерев // Вестник МГПУ. – 2023. – №1(63). – С. 37-47.*

*3. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474 с.*

*4. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: ИНФРА-М, 2011. – 416 с.*

*5. Конахович, Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф.*

*Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов. – К.:"МК-Пресс", 2005. – 288 с.*

*6. Mahajan D. DDoS Attack Prevention and Mitigation Techniques - A Review // International Journal of Computer Applications. – 2013. – Vol. 67, Iss. 19. – Pp. 21–24.*

*7. Garber L. Denial-of-Service Attacks Rip the Internet // IEEE Computer. – 2000. – Vol. 33, Iss. 4. – Pp. 12–17.*

*8. Дмитриев, А.А. Метод фильтрации трафика на основе анализа сетевых взаимодействий устройств / А.А. Дмитриев, Д.А. Дмитриев // Проблемы правовой и технической защиты информации. – 2023. – №11. – С. 16-20*

*9. Чайка Е. М. Обзор криптошлюзов для защиты информации в корпоративных сетях / Е. М. Чайка, С.П. Белов // Научный результат. Информационные технологии. – 2024. – Т.9, №1. – С. 3-9.*