СОВЕРШЕНСТВОВАНИЕ МЕТОДИК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ ОПЕРАТОРА СВЯЗИ

Коновалов С.Ю.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

В XXI веке невозможно представить свою жизнь без информационных технологий. Практически каждый человек постоянно пользуется различными устройствами: ноутбуком, планшетом, мобильным телефоном, умными часами, наушниками. Они предназначены для работы, развлечений, обучения и коммуникации. В связи с этим существует потребность в подключении устройств к мобильной связи, чтобы быть доступным в любое время.

Каждая компания уделяет внимание информационной безопасности своих устройств и сетей. Особенно это важно операторам связи, которые хранят и обрабатывают большие объемы трафика и данных абонентов.

Существующие методы защиты данных компаний операторов связи не всегда могут показать хорошие показатели своей эффективности. Это можно понять из исследований и статистик компаний, которые занимаются разработкой систем безопасности.

В 2020 году отмечался массовый всплеск числа угроз, связанных с шифрованием, внедрением RAT (Remote Access Trojans) программ, взломом протоколов удаленного рабочего стола, а также кражей учетных данных сотрудников.

Для борьбы с актуальными угрозами требуется совершенствовать существующие программные и технические методы информационной безопасности.

Учитывая существующие угрозы безопасности и современные средства защиты была проведена аналитическая работа, направленная на расширение существующих способов обеспечения информационной безопасности компаний. Результатом данной работы следует считать перечень рекомендаций для обеспечения информационной безопасности внутренней сети мобильного оператора. Компаниям операторов связи рекомендуется сделать:

– внедрить SIEM (Security information and event management) решения;

– установить и настроить межсетевые экраны;

– интегрировать системы обнаружения и предотвращения вторжений;

– разработать политики безопасности компании и обучить их знанию сотрудников;

– проводить периодическое обновление паролей к системам и личным аккаунтам сотрудников;

– запустить систему аналитики и выявления подозрительной активности работников;

– установить антивирусы на все устройства сотрудников и подключить облачный антивирус;

– провести обучение сотрудников правилам и политикам при обращении с конфиденциальной информацией, также периодически проводить повторные мероприятия по проверке знаний;

– устанавливать только лицензионное программное обеспечение;

– настроить регулярное автоматическое обновление программ и систем;

– увеличить резервную часть пропускной способности систем и каналов связи;

– внедрить VPN (Virtual Private Network) решения, для ограждения внутренней сети компании от глобальной сети;

– проводить периодический мониторинг активности в сети;

– использовать сквозное шифрование в каналах связи.

Описанные выше программные решения были учтены при составлении структуры системы безопасности внутренней сети мобильного оператора, которая представлена на рисунке 1.

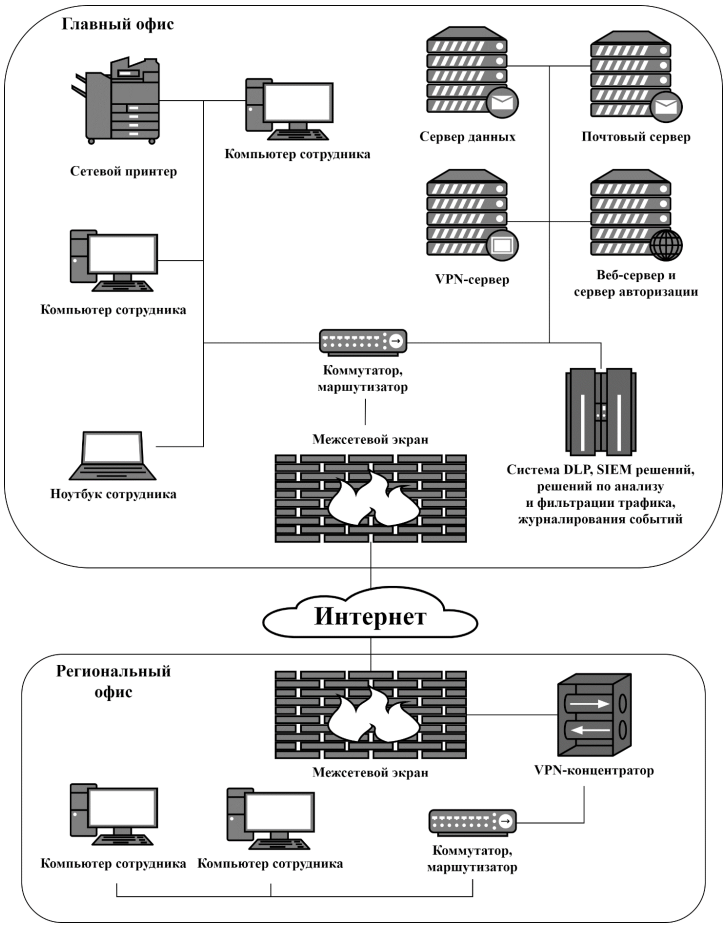

Рисунок 1 – Структура системы безопасности внутренней сети оператора связи

Для организации информационной безопасности компании следует установить дополнительное программное обеспечение на мобильные устройства и персональные компьютеры и ноутбуки. Помимо антивируса на телефон необходимо скачать VPN-клиент и приложение для генерации кодов двухфакторной аутентификации. На ноутбуках и персональных компьютерах нужно установить DLP (Data Leak Prevention) агент и VPN-клиент. Рекомендуемое программное обеспечение для информационных устройств можно увидеть на рисунке 2.

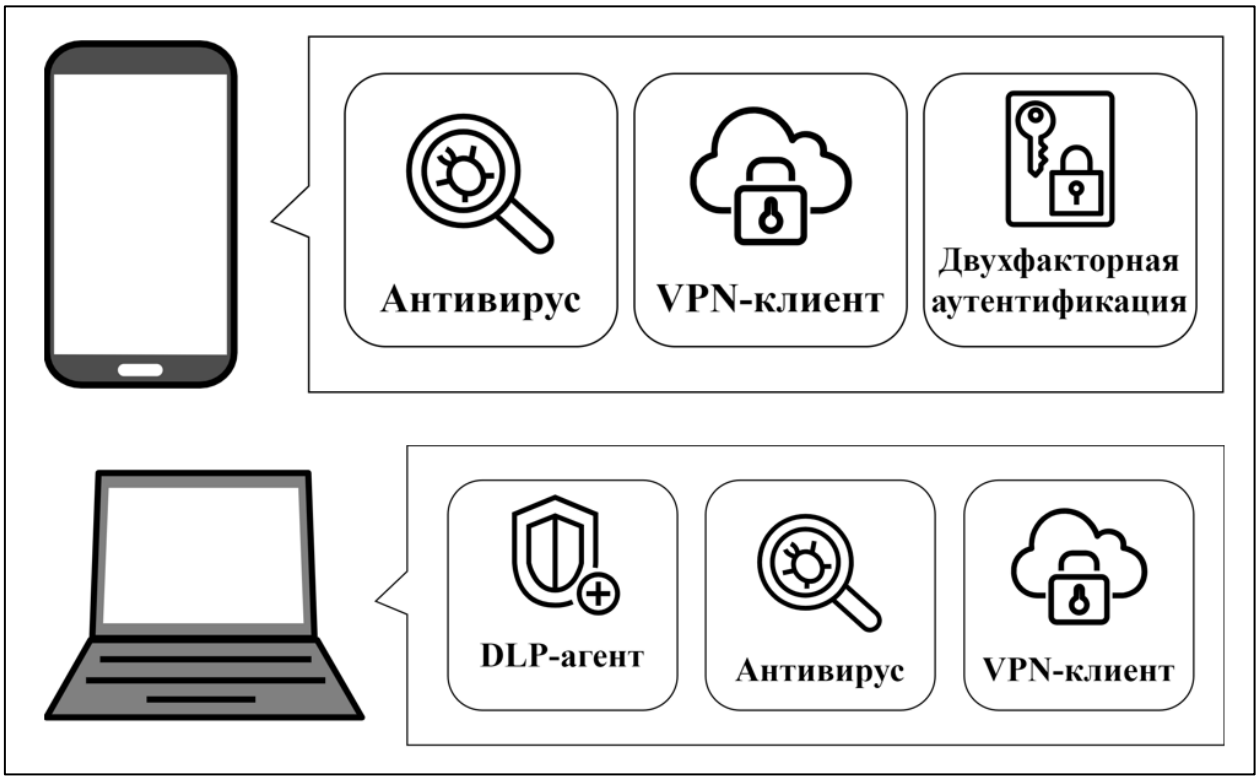

Рисунок 2 – Рекомендуемое программное обеспечение