КОМПЛЕКСНОЕ ПРИМЕНИЕ ПЕРСОНАЛЬНЫХ МОБИЛЬНЫХ УСТРОЙСТВ В ВОЕННО-УЧЕБНЫХ ЗАВЕДЕНИЯХ

Макатерчик А.В.

УО «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Abstract. A variety of personal mobile devices are firmly embedded in the life of modern man and society. However, the threats associated with them forced the security agencies to prohibit not only the use, but also the presence of these devices on the territory of special-purpose facilities. In turn, the capabilities of these devices, provided that the proposed model for building and managing the information security system of a special purpose object is created, can be applied to effectively solve a number of current problems.

Разнообразные персональные мобильные устройства прочно вошли в жизнь современного человека и общества. Трудно представить образ современного человека без собственного смартфона, планшета, ноутбука, умных часов, фитнес браслета и подобных им устройств. Целые сферы жизнедеятельности человека уже неразрывно связаны с ними. Кроме того, возрастает число компаний, перестроивших свои бизнес-процессы и информационные системы на использование концепции BYOD (Bring Your Own Device - принесите своё собственное устройство; использование персональных устройств в рабочих целях). При этом, специалистами в области информационной безопасности отмечается: «При видимом удобстве использования и мобильностью сотрудников возникает множество проблем и рисков информационной безопасности»[3].

Кроме того, вооруженные конфликты в Украине и Сирии, а прежде всего методы, используемые в своей деятельности интернет-издания Bellingcat вынудили многие, но прежде всего силовые ведомства запретить не только использование, но и нахождение персональных мобильных устройств на территории объектов специального назначения. Наиболее ярким стал пример авиабазы военно-космических сил Российской Федерации РФ в сирийском городе Хмэймим, на которой все обнаруженные и изъятые у личного состава персональные мобильные устройства прибиты к информационному щиту [2].

Вместе с тем, обеспечение постоянного контроля за выполнением подобных распоряжений является достаточно трудоемким процессом не обеспечивающим высокой эффективности.

Данные запреты коснулись и военно-учебных заведений в Республике Беларусь и в других странах мира. Что в век широко распространения инновационных образовательных технологий, основанных на базе различных инфокоммуникационных технологий, приводит к неизбежному отставанию военного образования и даже определенному регрессу. Так, данные запреты ограничивают использование обучающимися электронного образовательного контента, доступ к образовательным ресурсам сети Интернет, электронным библиотекам. Снижают возможности по использованию обучающих компьютерных программ и непосредственно возможности программ.

Наиболее остро данная проблема ощущается на военных факультетах (кафедрах) гражданских высших учебных заведений. Особенность образовательного процесса в таких учебных заведениях заключается в том, что в рамках военного факультета (кафедры) подготовка ведется только по ряду дисциплин, а большая часть изучаемых дисциплин изучается курсантами на других кафедрах высшего учебного заведения, широко использующих весь набор информационных образовательных технологий и соответственно требует их использования от курсантов.

В свою очередь, те возможности персональных мобильных устройств, которые послужили предпосылками для возникновения запретов на их использование, при условии создании определенной модели построения и управления системой защиты информации объекта специального назначения могут быть применены для эффективного решения целого ряда проблем, в том числе и в интересах обеспечения информационной безопасности.

Например:

1) Контроль в реальном времени за местонахождением личного состава (геопозиционирование, триангуляция по данным WiFi или сотовой сети). Так реализация данной функции могло позволить избежать трагедии с рядовым Александром Коржичем [1].

2) Учет находящихся на территории военно-учебного заведения персональных мобильных устройств, с указанием их принадлежности, местонахождения, выполняемых с его помощью операций.

3) Выдача предупреждений дежурной службе военно-учебного заведения об использовании персональных мобильных устройств в защищаемых помещениях (охраняемых территориях).

4) Контроль (управление) за используемыми на персональном мобильном устройстве функциями. Например, отключение или искажение данных геопозиционирования, запрет на использование фотокамеры, диктофона, регистрация запрещаемых действий с выдачей оповещения дежурной службе военно-учебного заведения и т.п.

5) Защита персональных данных личного состава за счет контроля и управления антивирусной защитой персональных мобильных устройств, средствами обнаружения вторжений и подобным программным обеспечением.

6) Контроль за используемой и обрабатываемой на персональных мобильных устройствах информацией.

7) Увеличение охвата личного состава инфо-

коммуникационной сетью с целью управления и связи.

Один из вариантов реализации данного подхода можно представить следующим образом (рисунок 1)

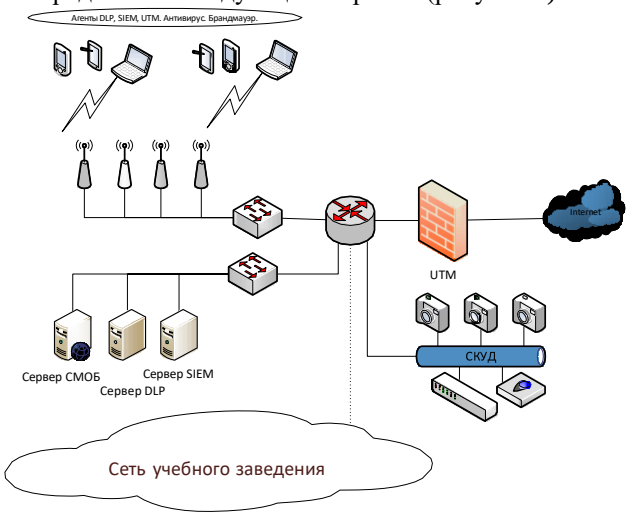

Рисунок 1 - Модель построения системы защиты информации

Она подразумевает развертывание сети беспроводной связи WiFi с безлимитным подключением к Интернет. При этом обязательным условием авторизации пользователей устанавливается наличие на персональном мобильном устройстве агентов используемых систем безопасности и специализированного программного обеспечения. Сеть оснащается системой UTM (Unified Threat Management объединенный контроль угроз) включающая в себя файервол, IDS/IPS (системы обнаружения и предупреждения вторжений), антивирус, прокси-сервер, контентный фильтр и антиспам-фильтр. В качестве систем безопасности развертываются и настраиваются системы контроля за информацией (DLP) и управления информационной безопасностью (SIEM). Кроме того, на базе действующей на объекте системы контроля и управления доступом и беспроводной сети запускается функционирование системы мониторинга общественной безопасности.

Объединение данных систем в рамках единой информационной системы позволит реализовать широкий набор функций контроля, управления и аналитики.

Правильная настройка и использование данных систем в интересах выше обозначенных проблем позволит использовать персональные мобильные устройства в военно-учебных заведениях как в интересах защиты информации, так и для решения повседневных задач.

Также будет обеспечены:

действенный и постоянных контроль за создаваемыми персональными мобильными устройствами каналами утечки информации;

пониженный уровень или исключение связанных с их использованием угроз;

безопасное использование широкого спектра информационных образовательных технологий как курсантами, так и управленческим и профессорско-преподавательским составом;

контроль за наличием и перемещением личного состава;

контроль за корректным использованием персональных мобильных устройств на объектах информатизации;

возможность контроля за доступом личного состава военно-учебного заведения к запрещенным информационным ресурсам;

расширенные возможности по организации связи управлению личным составом и подразделениями военного-учебного заведения;

возможность безопасного развертывания информационных систем (электронный документооборот, учет и т.п).

Кроме указанных выше, открываются и другие возможности, реализуемые на основе предлагаемого решения.

Однако, для построения данной модели потребуется нормативно-правовое урегулирование порядка ее использования, выбор сертифицированных программных продуктов, организация их совместного функционирования в интересах обеспечения выполнения описанных выше задач, развертывание необходимой технической инфраструктуры, разработка информационной системы управления военно-учебным заведением.

Литература

1. Гибель солдата-срочника в Печах. (13 Ноябрь 2018 г.). Получено из Sputnik.by: https://sputnik.by/trend/gibelsoldata/

2. На российской авиабазе в Сирии есть доска с прибитыми к ней смартфонами. (23 мая 2018 г.).

3. Сафонов, Л. (б.д.). BYOD — удобство против безопасности. Получено из Хабрахабр: https://habr.com/company/pentestit/blog/281463/