**Тема: Улучшение безопасности путем ограничения использования служебных гаджетов.**

Выполнил: Будник Владислав Дмитриевич

Научный руководитель: к.т.н. Николаенко В.Л.

к.т.н. Микулик Т.Н.

**Введение**

Безопасность, под которой понимается комплекс мер, принимаемых предприятием для обеспечения безопасного и непрерывного функционирования и противодействующих возникающим угрозам любого характера, является составной частью экономической безопасности [1]. В свою очередь экономическая безопасность Республики Беларусь согласно статье 4 “Концепции национальной безопасности Республики Беларусь” (Указ Президента Республики Беларусь от 9 ноября 2010 г. №575 “Об утверждении Концепции национальной безопасности Республики Беларусь”) – это состояние экономики, при котором гарантированно обеспечивается защищенность национальных интересов Республики Беларусь от внутренних и внешних угроз.

В данной работе рассматривается специально разработанное программное средство, которое защищает мобильные устройство сотрудников от вредоносных или шпионских программ. Это сейчас очень актуально в связи с быстро развивающейся сферой мобильных устройств.

**Основная часть**

Опасность и угрозы безопасности условно можно разделить на две группы – внутренние и внешние, а каждую группу в свою очередь на субъективные и объективные [1]. Одной из важнейших внутренних субъективных угроз производственной безопасности являются опасности: со стороны сотрудников предприятия. В частности, большинство сотрудников предприятий ИТ-сферы используют во время работы личные гаджеты, к которым относятся: смартфоны, планшеты, ноутбуки и т. п. Эти гаджеты подключаются к сети предприятия, давая возможность злоумышлением проникнуть в эту сеть. Злоумышленник может установить на личный гаджет работника шпионскую программу, с помощью которой сможет получать доступ к служебной информации предприятия, хранящейся на гаджете сотрудника. Кроме того, сотрудник может зайти на вредоносные ресурсы в интернете. При заражении гаджета вирусом, сотрудник может утратить возможность использовать гаджет, что ведёт к потере производительности. Таким образом, использование личных гаджетов сотрудниками, резко снижает производственную безопасность предприятия.

Вопросы информационной безопасности предприятия, выдающего своим сотрудникам служебные гаджеты, на наш взгляд, впервые был поставлен в [2] в первой половине 2010-х годов (мнение Эндрю Хуга (AndrewHoog), генерального директора одной из ведущих в мире по вопросам информационной безопасности мобильных приложений американской компании NowSecure), описанное в [3]: «Специалисты по информационной безопасности должны начать разрабатывать проактивные стратегии для борьбы со всем разнообразием угроз, представляемых мобильными устройствами».

Эндрю Хуг ведущий эксперт в области мобильной криминалистики и безопасности, специалист в области информатики, главный исполнительный директор и соучредитель NowSecure, ведущей компании в области мобильной безопасности.

Он нашел своим призванием изучение мобильной безопасности; будь то проведение оригинального исследования, которое опровергает общие предположения о безопасности, предоставление решений для мобильной безопасности или создание более умных технологий, чтобы личная информация оставалась конфиденциальной и не подвергалась ненужным рискам [3].

Для устранения этого недостатка в докладе предлагается административно запретить сотрудникам во время работы использовать личные гаджеты. Вместо личных гаджетов сотрудника в часы его работы должен выдаваться служебный. При использовании служебного гаджета на отдел информационной безопасности предприятия совместно с отделом администрирования сети возлагается обязанность централизованной защиты служебных гаджетов сотрудников. Во-первых, служебным гаджетам технически запрещён доступ к вредоносным сайтам. Во-вторых, атаки злоумышленников на служебные гаджеты с целью проникновения в сеть предприятия отражаются централизованно.

В докладе приводится пример программы, работающей на служебных гаджетах, приведены в алгоритмы и скриншоты [4].

**Заключение.**

Практическая реализация программы, работающей на служебных гаджетах сотрудников, подтверждает возможность повышения безопасности за счёт использования служебных гаджетов.

**Литература**

1. Производственная безопасность предприятия как ... – КиберЛенинка [Электронный ресурс]. - Режим доступа https://cyberleninka.ru/.../proizvodstvennaya-bezopasnost-predpriyatiya-kak-element-...

2. Хуг, Эндрю Мобильная безопасность: битва вокруг вредоносного ПО /Эндрю Хуг // Безопасность ИТ-инфраструктуры. 2014. – № 7 (85). – С. 4-6.

3. Угрозы информационной безопасности при использовании мобильных устройств на рабочих местах и в школах и их парирование / В. Д. Аленин, В. Л. Николаенко, А. А. Охрименко, В. И. Пачинин, Г. В. Сечко, Т. Г Таболич, И. И. Шпак //Труды ХХІІІ МНТК «Информационные системы и технологии» ИСТ-2017, посвященной 100-летию НГТУ Нижегородского политехнического института, Нижний Новгород (21 апреля 2017 г.). Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2017. С. 569-573.

4. AndrewHoog - Co-Founder @ NowSecure - Crunchbase [Электронный ресурс]. Режим доступа: https://www.crunchbase.com/person/andrew-hoog.

5. Дедович, Д. К. Программное средстводля делегирования доступа к веб-ресурсам на платформе ANDROID / Д. К. Дедович // 54-я науч. конф. аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»: материалы конференции по направлению 8: Информационные системы и технологии (Минск, 21 апреля 2018 года). - Минск: БГУИР, 2018. - 115 с. - С. 39-40.