УДК 004.421

ПОВЫШЕНИЕ ПРОИЗВОДСТВЕННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЙ ОБРАЗОВАНИЯ И НАУКИ ЗА СЧЁТ ИСПОЛЬЗОВАНИЯ СЛУЖЕБНЫХ ГАДЖЕТОВ

[1] Дедович Д. К., [2] Евдокименко М. Н., [2] Микулик Т. Н., [2] Николаенко В. Л., [1] Сечко Г. В.

[1] *Белорусский государственный университет информатики и радиоэлектроники. Минск*

[2] *Белорусский национальный технический университет, Минск*

Введение.

Сотрудники любого научного учреждения или учреждения образования в своей работе используют большой объем конфиденциальной информации и информации, составляющей коммерческую тайну. Эта информация обязательно интересует конкурентов учреждения, а ее утечка непосредственно влияет на производственную безопасность учреждения.

Производственная безопасность, под которой понимается комплекс мер, принимаемых учреждением или предприятием для обеспечения безопасного и непрерывного их функционирования и противодействующих возникающим угрозам любого характера, является составной частью экономической безопасности [1]. В свою очередь экономическая безопасность Республики Беларусь согласно статьи 4 «Концепции национальной безопасности Республики Беларусь» (Указ Президента Республики от 9 ноября 2010 г. N575 «Об утверждении Концепции национальной безопасности Республики Беларусь») – это состояние экономики, при котором гарантированно обеспечивается защищенность национальных интересов Республики Беларусь от внутренних и внешних угроз.

Основная часть.

Опасности и угрозы производственной безопасности научного учреждения или учреждения образования 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. В частности, большинство сотрудников научного учреждения или учреждения образования 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, 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 научного учреждения или учреждения образования.

Для устранения этого недостатка в докладе предлагается административно запретить сотрудникам во время работы использовать личные гаджеты. Вместо личных гаджетов сотрудника ему в часы его работы должен выдаваться служебный – учреждения, где ценят свою конфиденциальную и коммерческую информацию

экономически могут позволить себе затраты на это. Если средств на гаджеты для всего учреждения не хватает, гаджеты для своих сотрудников может закупить отдельное структурное подразделение учреждения, например, научно-исследовательская лаборатория с высоким доходом от реализации своих разработок. Именно в гаджетах сотрудников такой лаборатории содержится самый большой объем конфиденциальной информации и информации, составляющей коммерческую и служебную тайну, которая интересует конкурентов.

Наиболее состоятельные учреждения разных стран уже выдают своим сотрудникам служебные гаджеты. На рис. 1 приведено фото, на котором полицейские Нью-Йорка бесплатно получают в феврале 2018 года новые смартфоны модели iPhone 7 и iPhone 7 Plus [2].

Рис. 1. Фото: полицейские Нью-Йорка получают новые смартфоны

В [3] сообщается также, что в 2017 году было куплено 15000 гаджетов для «Почты России».

При использовании служебного гаджета на отдел информационной безопасности учреждения 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.

Для решения поставленных целей в [4] реализован функционал по ограничению доступа к файлам приложений не входящих в список разрешённых. Запрещён доступ для работы с браузерами по умолчанию. Вместо них можно использовать браузер, который встроен в приложение. Качество приложения оценивается проведением тестирования и корректности работы всех модулей.

К документам входного заполнения относятся параметры, добавляемые администратором в список разрешённых ресурсов для пользователя, а также ограничение работы с приложениями и их доступом к сети интернет.

В базе данных хранятся данные посещённых, пользователем ресурсов с отражением даты и временем их посещения. В это же базе хранятся учётные данные администратора, логин и пароль. Для разработки программного средства использована среда программирования Android Studio.

Все данные хранятся в базе данных. Несколько процессов или потоков могут одновременно без каких-либо проблем читать данные из одной базы. Запись в базу можно осуществить только в том случае, если никаких других запросов в данный момент не обслуживается; в противном случае попытка записи оканчивается неудачей, и в программу возвращается код ошибки. Другим вариантом развития событий является автоматическое повторение

Для работы программного средства требуется гаджет с операционной системой Android версии 4.4 и выше. В системе должны быть получены права суперпользователя ROOT, которые предоставляют доступ к необходимым для работы приложения функциям системы.

Для комфортной работы с приложением диагональ экрана гаджета должна составлять не менее 3,5 дюймов и разрешение экрана не менее 480x800 пикселей. Рекомендуемой конфигурацией является размер экрана 5-5,2 дюйма, разрешение экрана 720x1280 пикселей и версия операционной системы Android 5.1.1.

Контекстная диаграмма программного средства показана на рис. 2.

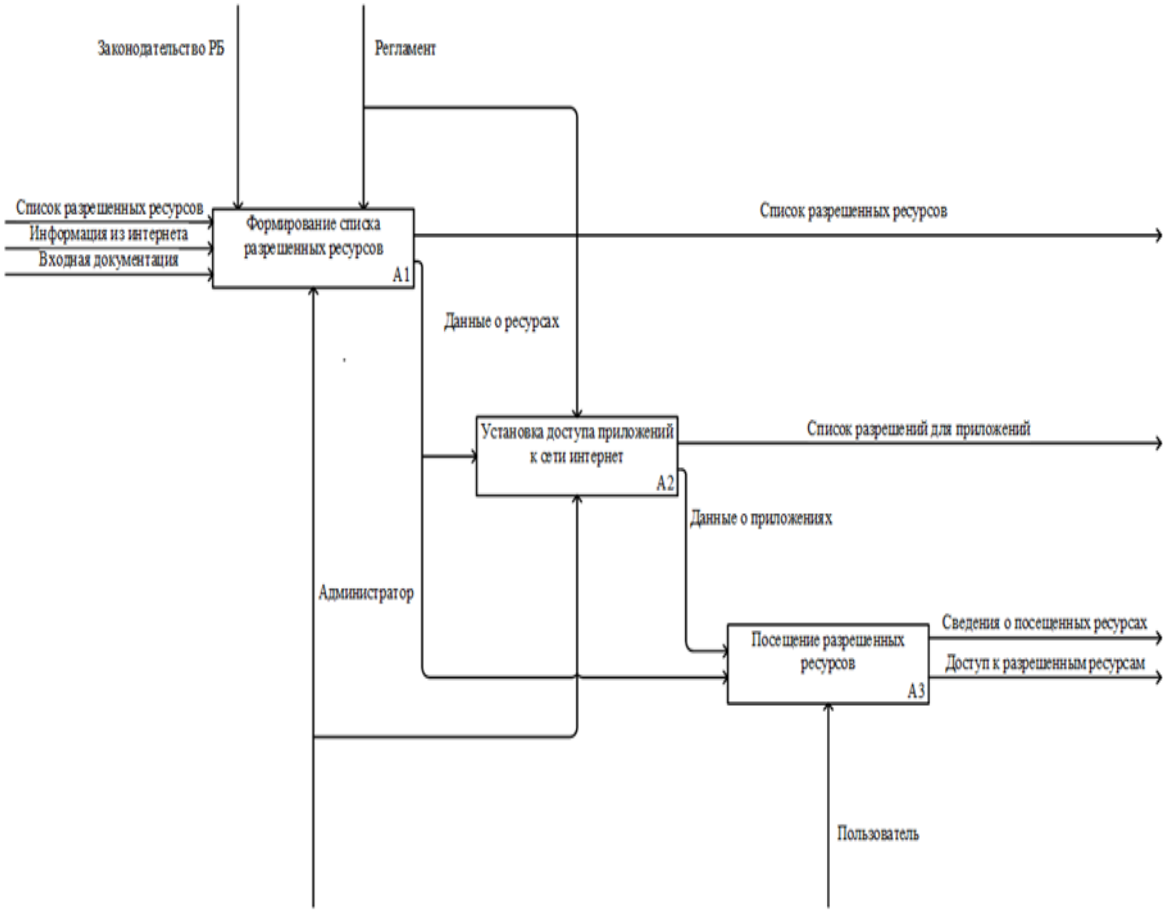

Рис. 2. Контекстная диаграмма программного средства

Алгоритм ухода с запрещенного ресурса, например, представлен в виде схемы алгоритма, изображенной на рис. 3. В качестве демонстрации интерфейса на рис. 4 изображена панель для входа под учётной записью пользователя.

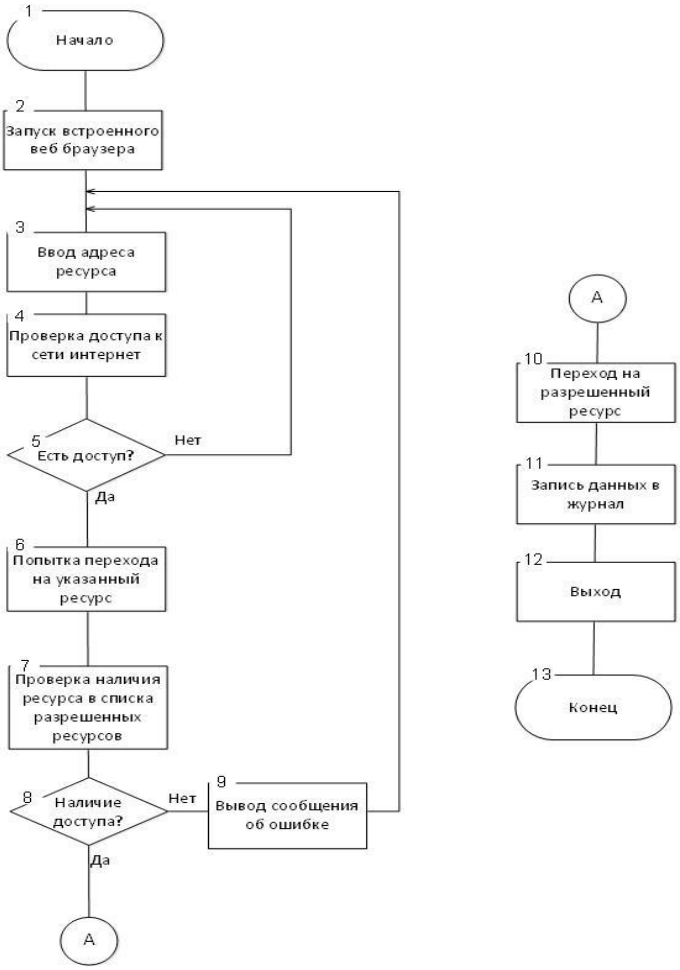

Рис. 3. Схема алгоритма ухода с запрещенного ресурса

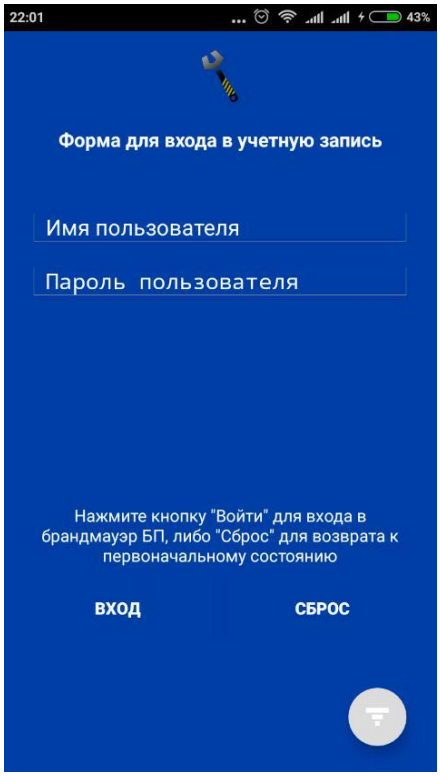

Рис. 4. Панель регистрации

Заключение.

Программное средство должно использоваться на любом предприятии, где есть необходимость ограничить доступ работников на сторонние сайты, с мобильных устройств, выданных предприятием для работы. Так же для увеличивается защищённость важной информации, за счёт контроля доступа к сети. Работники не смогут использовать трафик в личных целях, что положительно скажется на эффективности из работы.

Программное средство реализует следующие функции:

– ведение перечня ресурсов, разрешенных для посещения;

– добавление/удаление сайтов из списка разрешенных ресурсов;

– ведение списка установленных приложений и разрешений на доступ к сети;

– изменение прав приложениям на доступ к сети интернет;

– ведение журнал посещенных ресурсов и контроль за доступом к сайтам из списка разрешенных ресурсов;

– организация ограничения на доступ к настройкам и спискам ресурсов.

Практическая реализация программы, работающей на служебных гаджетах сотрудников, подтверждает возможность повышения производственной безопасности научного учреждения или учреждения образования за счёт использования служебных гаджетов.

ЛИТЕРАТУРА

1. *Производственная безопасность предприятия как ... - КиберЛенинка [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/.../proizvodstvennaya-bezopasnost-predpriyatiya-kak-element-... – Дата доступа: 16.12.2018.*
2. *Служебные смартфоны порой позволяют полицейским Нью-Йорка .. [Электронный ресурс]. – Режим доступа: https://www.ixbt.com/news/2018/02/08/sluzhebnye-smartfony-poroj-pozvoljajut-policejskim-njujorka-okazatsja-na-meste-prestuplenija-do-poluchenija-vyzova.html. – Дата доступа: 16.12.2018.*
3. *Федеральные чиновники будут пользоваться смартфоном на российской ОС [Электронный ресурс]. – Режим доступа: https://habr.com/post/412181/. – Дата доступа: 16.12.2018.*
4. *Дедович, Д. К. Программное средство для 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.*