DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.3.5

УДК 004.056.5
ББК 68.823

РАЗРАБОТКА ПОДСИСТЕМЫ БЕЗОПАСНОСТИ СИСТЕМЫ «СЕТЕВОЙ ГОРОД. ОБРАЗОВАНИЕ»

Ирина Сергеевна Рыбина

Студентка кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Антон Олегович Куприянов

Студент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Кристина Петровна Гужаковская

Кандидат физико-математических наук,
доцент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье проведен анализ информационной системы «Сетевой город. Образование» и сформулирована типовая архитектура данной информационной системы, выделены ее компоненты. Также была разработана подсистема безопасности для «Сетевого города» – система «Безопасность школьников». Для компонентов разработанной типовой архитектуры информационной системы были рассмотрены актуальные возможные угрозы. Рассмотрены механизмы защиты от выделенных угроз.

Ключевые слова: информационная система, «Сетевой город», безопасность школьников, информационная безопасность, модель угроз.

С недавних пор во многих районах РФ создаются условия для реализации согласованной сети общеобразовательных заведений, так как осуществляются поставки компьютерной техники на государственном и областном уровне, компьютерных машин, а также разрабатываются программы подключения школ к сети Интернет. «Сетевой город. Образование» – информационная система для организации общего информационной образовательного пространства в городе или районе [1; 7; 10]. В настоящее время в данной программе участвуют те муниципальные учреждения, которые подключены к выделенным сетям связи с недорогим трафиком [6].

Для выполнения задачи автоматизации контроля над образовательной структурой нужно продумывать решение не только для отдельных школ, а для всех учебных учреждений [2–5; 9;

12]. Это предполагает постепенную автоматизацию всех учебных заведений с формированием информационной среды для этих заведений и областных органов управления на основании согласованных информационных норм [7].

Целью данной работы является разработка подсистемы безопасности системы «Сетевой город. Образование» и повышение уровня защищенности этой системы.

Для рассмотрения школьной системы в виде формальной модели введем некоторые переменные. Состав школьной системы обозначен S. Таким образом, все составляющие школьной системы представляют множество:

$$S = \{x_i\}, \quad (1)$$

где x_i – подмодуль.

Рассмотрим подмодули, которые входят в модуль «Безопасность школьников», а также введем для составляющих этих подмодулей переменные:

1) x_1 – подмодуль КПП. Вектор для данного подмодуля имеет вид:

$$x_1 = (Vh_t,\ Vyh_t). \quad (2)$$

Состав:

Вход Vh_t ученика в школу. Выход Vyh_t ученика из школы.

2) x_2 – столовая. Вектор для данного подмодуля имеет вид:

$$x_2 = (\text{Menu}_{mn}, \text{Con}_{st}, \text{Buy}_s). \quad (3)$$

Состав:

Меню ($\text{Menu} = \{\text{Menu}_{mn}\}$, $mn = 1, \ldots, m$), где родители могут составлять список продуктов, которые ученик может приобрести в столовой.

Противопоказания Con_{st}, чтобы родители могли в личном кабинете карты ученика настраивать нужное меню, с помощью которого ученик может приобрести себе то, что не вредно для его здоровья (в случае наличия медицинских противопоказаний). Значение взято из подмодуля «Медицинский пункт» – $\text{Con}_{st} = \text{Con}_m$.

Список покупок Buy_s, где $s = 1, \ldots, r$. Предусматривает, что приобретет ученик в столовой.

3) x_3 – медицинский пункт. Вектор для данного подмодуля имеет вид:

$$x_3 = (\text{Con}_m). \quad (4)$$

Состав:

Противопоказания Con_m, которые заносятся в медицинскую карту. Значение данного параметра понадобится в подмодуле «Спортивный зал», а также для составления меню в школьной столовой на случай, если у ученика существуют аллергические реакции на какие-либо продукты (подмодуль «Столовая»). $\text{Con}_m = \{\text{Con}_{mj}\}$, $j = 1, \ldots, t$, где t – все противопоказания.

Далее разработана формальная модель для обеспечения безопасности системы «Безопасность школьников» на примере одной школы.

Рассмотрено значение $R_{\text{доп}}$ как процентное соотношение с величиной бюджета школы. Предположим, что допустимый риск в месяц равен 100 ($R_{\text{доп}} = 100$). Будет оценена безопасность использования системы «Безопасность школьников» в образовательном учреждении с помощью оценки рисков, возникающих в случае реализации угроз, направленных на систему «Безопасность школьников». Оценка рисков производится с помощью двухфакторной модели.

Риск определяется вероятностью реализации угрозы и величиной ущерба:

$$R_i = m_i \times P_i \times U_i, \quad (5)$$

где P_i – вероятность реализации угрозы; U_i – величина ущерба, измеряемая в денежных единицах; коэффициент m – степень перекрытия угрозы (характеристика, учитывающая механизмы защиты) (см. таблицу).

Толкование значений коэффициента *m*

Диапазон изменения m	Степень перекрытия угрозы
0,7–1	угроза перекрывается в малой степени
0,4–0,6	угроза перекрывается в средней степени
0–0,3	угроза перекрывается практически полностью

Когда расчет риска происходит без учета механизмов защиты, *m* равен 1.

Существуют объективные и субъективные оценки вероятности. В качестве объективной оценки выступает относительная частота появления какого-либо события в общем объеме наблюдений. Под субъективной оценкой вероятности подразумевают меру уверенности человека в том, что данное событие произойдет В нашем случае сделана оценка вероятности экспертным путем.

Величина R_c (средний риск) используется для оценки уровня защищенности *SL* модуля «Безопасность школьников». Для этого величина R_c сравнивается с допустимым средним риском $R_{доп}$ по всем угрозам:

$$SL \text{ (securite level) уровень защищенности} = \begin{cases} R_c > R_{доп}, \text{низкий уровень} \\ R_c \le R_{доп}, \text{приемлимый} \end{cases} \quad (6)$$

С помощью данных в таблице посчитаем средний риск:

$$R_c = \sum_{i=1}^{n} R_i / n, \quad (7)$$

где n – количество угроз.

Если *SL* низкий, необходимо применить механизмы защиты. В результате уровень *SL* должен повыситься. Для оценки изменения уровня защищенности *SL* рассчитывается риск с учетом механизмов защиты по каждой угрозе.

Архитектура программы представлена на рисунке 1 и включает в себя следующие модули:

1. Пользовательский интерфейс – предназначен для взаимодействия с программой. Он отображает формы для ввода данных пользователем и отображения результатов работы.

2. Модуль заполнения данных, где пользователь осуществляет ввод данных для того, чтобы посмотреть и оценить работу системы «Безопасность школьников». Введенные данных сохраняются в базе данных.

3. Модуль оценки безопасности – позволяет оценить уровень безопасности системы и состоит из следующих блоков:

– блок выделения угроз – позволяет осуществить выбор нескольких или всех угроз из списка для последующего расчета риска для каждой угрозы и величины среднего риска;

– блок оценки исходной безопасности; в данном блоке происходит проверка уровня безопасности (*SL*), в котором сравнивается средний риск R_c с допустимым риском $R_{доп}$ и осуществляется выдача сообщений пользователю, которые составляются на основе полученных результатов при сравнении среднего и допустимого риска;

– блок расчета с механизмами защиты; в данном блоке реализуется последовательность действий, которая выполняется после

Рис. 1. Архитектура программного комплекса системы «Безопасность школьников»

получения сообщения о недопустимом уровне среднего риска;

– блок оценки безопасности системы с учетом механизмов защиты. В данном блоке происходит проверка уровня безопасности (*SL*), в котором сравнивается средний риск R_c с допустимым риском $R_{доп}$ и осуществляется выдача пользователю сообщений, составляющихся на основе полученных результатов при сравнении среднего и допустимого риска.

Архитектура аппаратного обеспечения представлена на рисунке 2.

1. Модуль RFID-системы. В данном модуле осуществляется чтение смарт-карты ученика на разных считывателях (в зависимости от местонахождения ученика – КПП, столовая, медпункт). Далее данные передаются на микроконтроллер Arduino для их последующей обработки [8; 11].

2. Данные с микроконтроллера передаются на компьютер, который с ним соединен.

3. Данные отправляются на сервер баз данных для их хранения и последующего обращения к ним.

Схема монтажа представлена на рисунке 3.

Далее рассмотрим пользовательский интерфейс на рисунке 4. На пользовательс-

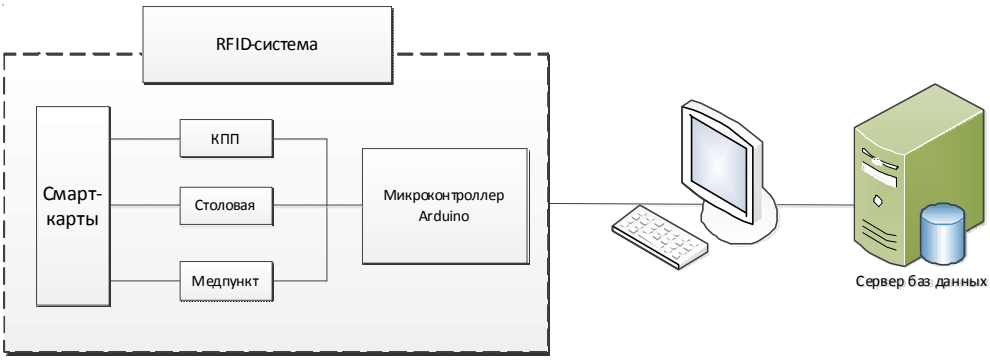

Рис. 2. Архитектура аппаратного обеспечения системы «Безопасность школьников»

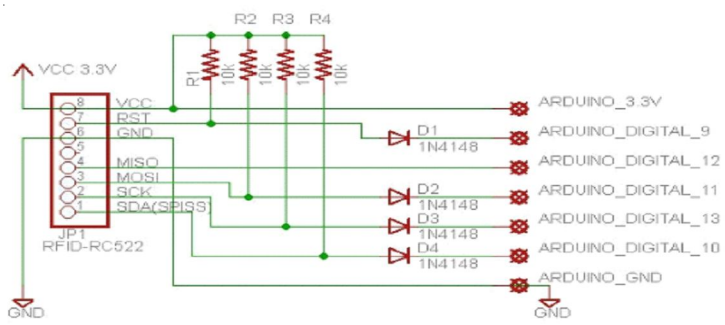

Рис. 3. Схема монтажа микроконтроллера и RFID-системы для работы системы «Безопасность школьников»

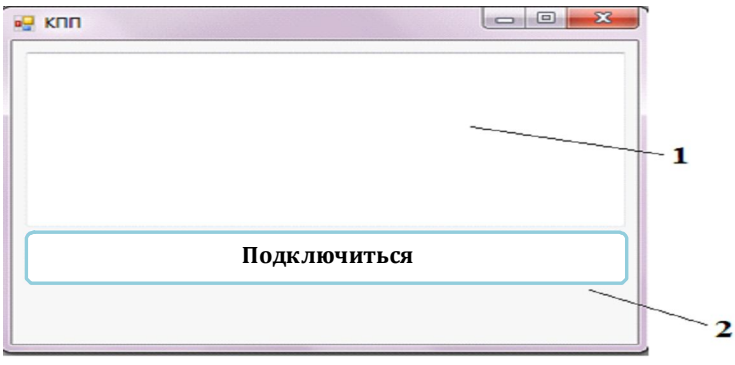

Рис. 4. Интерфейс программы (экранная копия)

ком интерфейсе «КПП» представлено: 1) окно для вывода идентификатора карты ученика, проходящего в школу; 2) кнопка для запуска работы микроконтроллера.

В пользовательском приложении «Столовая» (рис. 5) представлено: 1) окно для вывода информации о противопоказаниях ученика; при желании выбрать продукт в столовой, ученик прикладывает карту к считывателю, после чего на экране компьютера высвечивается информация о нем; 2) окно для вывода предлагаемых продуктов – меню; 3) окно для вывода продуктов, выбранных учеником; 4) окно для вывода итоговой суммы покупки; 5) окно для вывода статуса заказа; 6) кнопка для совершения покупки. Ученик прикладывает карту к считывателю еще раз, чтобы оплатить заказ.

После того как пользователь посмотрел работу системы, он переходит на приложение «Оценить безопасность». Для оценки безопасности нужно перейти на вкладку «Оценить безопасность». Оценивается безопасность без учета механизмов защиты (см. вкладку «Риск без учета механизмов защиты» на рис. 6). В соответствии с выбранными угрозами рассчитывается риск, а затем рассчитывается средний риск по всем угрозам. На данном интерфейсе представлено: 1) окно со списком угроз для RFID-системы; 2) окно со списком угроз для беспроводных точек доступа; 3) окно

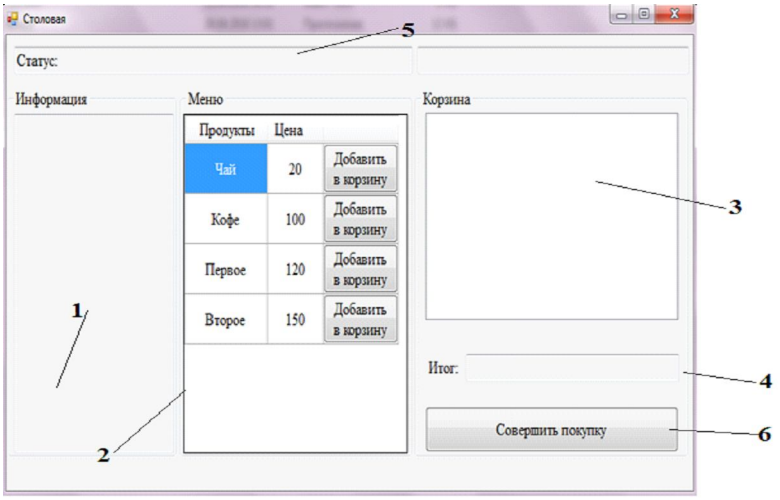

Рис. 5. Интерфейс приложения «Столовая» (экранная копия)

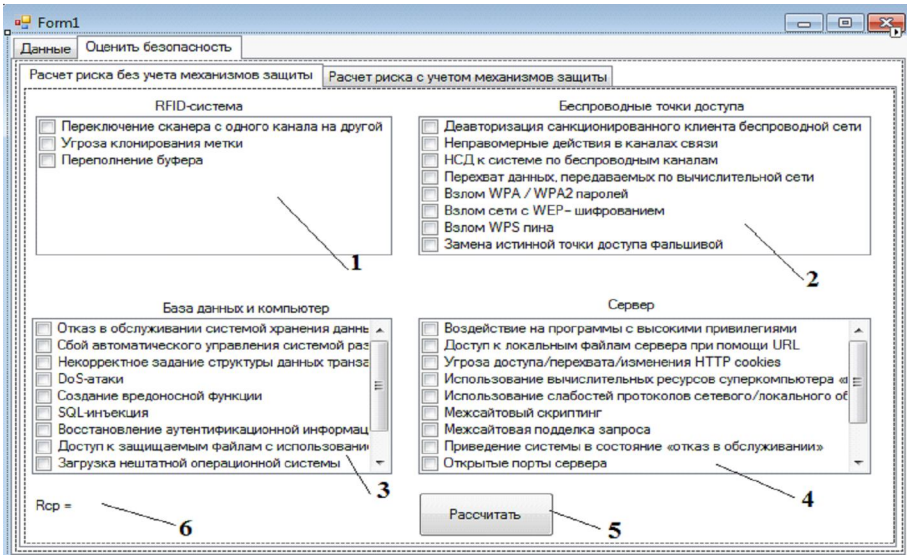

Рис. 6. Интерфейс программы для оценки рисков по компонентам системы «Безопасность школьников» (экранная копия)

со списком угроз для базы данных и компьютера; 4) окно со списком угроз для сервера; 5) кнопка для расчета среднего риска по выбранным угрозам; 6) поле для вывода значения посчитанного среднего риска.

После того как будет выведено сообщение о том, что пользователю необходимо применить меры защиты, он должен перейти на вторую вкладку «Расчет риска с учетом механизмов защиты».

Эксперименты показали, что протестированный программный комплекс справляется со своей задачей в качестве системы «Безопасность школьников». Также анализ полученных данных показал, что формализованная модель позволяет рассчитывать величину риска без учета механизмов защиты, а также рассчитывать риск с учетом механизмов защиты.

В результате проведенных экспериментов наблюдается повышение уровня информационной безопасности ИС «Сетевой город. Образование» при расчете риска с учетом механизмов защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Администрация школы. – Электрон. дан. – Режим доступа: www.gouo.ru/AZBUKA_GOU/A/Administratsiya_Shkoly.html.

2. БДУ ФСТЭК России. – Электрон. дан. – Режим доступа: https://bdu.fstec.ru/threat/ubi.008.

3. Виды атак на Wi-Fi. – Электрон. дан. – Режим доступа: https://hackware.ru/?p=158.

4. Защита папок и файлов: обзор инструментов для скрытия секретных данных. – Электрон. дан. – Режим доступа: https://itc.ua/articles/zashhita_papok_i_fajlov_56213/.

5. Идентификация и аутентификация субъектов доступа и объектов доступа. – Электрон. дан. – Режим доступа: https://www.itweek.ru/security/article/detail.php?ID=169230.

6. Положение о ЕИС Волгоградской области. – Электрон. дан. – Режим доступа: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjVzbjClfXYAhVE3iwKHaLaC1AQFggtMAE&url=http%3A%2F%2Fgor3.volgogradschool.ru%2Ffile%2Fdownload%2F2688&usg=AOvVaw1ORzEljPo-hyHQJyDXo4qL.

7. Построение единой информационно-образовательной среды муниципального образования на основе системы «Сетевой город. Образование». – Электрон. дан. – Режим доступа: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwiXn7G0__TYAhUJ_ywKHQKIAfAQFgg3MAI&url=http%3A%2F%2Fwww.ict.edu.ru%2Fvconf%2Ffiles%2F10236.doc&usg=AOvVaw0Z3yTENc2xmJXzQIDMF8qM.

8. Преимущества и недостатки использования Arduino. – Электрон. дан. – Режим доступа: http://tim4dev.com/2016/07/arduino-advantages-disadvatages/.

9. СДЗ DALLAS LOCK. – Электрон. дан. – Режим доступа: https://dallaslock.ru/products/sdz-dallas-lock/.

10. Сетевой город. Образование. – Электрон. дан. – Режим доступа: http://www.ir-tech.ru/?products=ais-setevoj-gorod-obrazovanie.

11. Считыватель RFID на примере RC522. Принцип работы, подключение. – Электрон. дан. – Режим доступа: http://arduino-kit.ru/textpage_ws/pages_ws/proekt-28_–schityivatel-rfid-na-primere-rc522.-printsip-rabotyi-podklyuchenie.

12. Усиливаем аутентификацию, или Зачем нужны одноразовые пароли. – Электрон. дан. – Режим доступа: http://www.infosecurity.ru/_gazeta/content/090512/art4.shtml#art3.

REFERENCES

1. *Administratsiya shkoly* [School Administration]. URL: https://www.gouo.ru/AZBUKA_GOU/A/Administratsiya_Shkoly.html.

2. *BDU FSTEK Rossii* [BSU FSTEC of Russia]. URL: https://bdu.fstec.ru/threat/ubi.008.

3. *Vidy atak na Wi-Fi* [Types of Attacks on Wi-Fi]. URL: https://hackware.ru/?p=158.

4. Zashchita papok i faylov: obzor instrumentov dlya skrytiya sekretnykh dannykh [Folder and File Protection: an Overview of Tools to Hide Secret Data]. URL: https://itc.ua/articles/zashhita_papok_i_fajlov_56213/.

5. *Identifikatsiya i autentifikatsiya subyektov dostupa i obyektov dostupa* [Identification and Authentication of Access Subjects and Access Objects]. URL: https://www.itweek.ru/security/article/detail.php?ID=169230.

6. *Polozhenie o EIS Volgogradskoy oblasti* [Provision on the EIS of the Volgograd Region]. URL: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjVzbjC1fXYAhVE3iwKHaLaC1AQFggtMAE&url=http%3A%2F%2Fgor3.volgogradschool.ru%2Ffile%2Fdownload%2F2688&usg=AOvVaw1ORzEljPo-hyHQJyDXo4qL.

7. *Postroenie edinoy informatsionno-obrazovatelnoy sredy munitsipalnogo obrazovaniya na osnove sistemy «Setevoy gorod. Obrazovanie»* [Construction of a Unified Information and

Educational Environment of the Municipality on the Basis of the System "The Network City. Education"]. URL: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwiXn7G0__TYAhUJ_ywKHQKIAfAQFgg3MAI&url=http%3A%2F%2Fwww.ict.edu.ru%2Fvconf%2Ffiles%2F10236.doc&usg=AOvVaw0Z3yTENc2xmJXzQIDMF8qM.

8. *Preimushchestva i nedostatki ispolzovaniya Arduino* [Advantages and Disadvantages of Using Arduino]. URL: http://tim4dev.com/2016/07/arduino-advantages-disadvatages/.

9. *SDZ DALLAS LOCK*. URL: https://dallaslock.ru/products/sdz-dallas-lock/.

10. *Setevoy gorod. Obrazovanie* [The Network City. Education]. URL: http://www.ir-tech.ru/?products=ais-setevoj-gorod-obrazovanie.

11. *Schityvatel RFID na primere RC522. Printsip raboty, podklyuchenie* [RFID Reader on the Example of RC522. Working Principle, Connection]. URL: http://arduino-kit.ru/textpage_ws/pages_ws/proekt-28_–schityivatel-rfid-na-primere-rc522.-printsip-rabotyi-podklyuchenie.

12. *Usilivaem autentifikatsiyu, ili Zachem nuzhny odnorazovye paroli* [Strengthening Authentication or Why One-Time Passwords Are Needed]. URL: http://www.infosecurity.ru/_gazeta/content/090512/art4.shtml#art3.

DEVELOPMENT OF THE SECURITY SUBSYSTEM WITHIN THE SYSTEM "THE NETWORK CITY. EDUCATION"

Irina S. Rybina

Student, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Anton O. Kupriyanov

Student, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Kristina P. Guzhakovskaya

Candidate of Sciences (Physics and Mathematics),
Associate Professor of Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. "The Network City. Education" is a comprehensive information program project that allows educational institutions and municipal authorities to interact with each other at the city or city district level. This information system is designed to automate the educational process and management activities in the field of education, as it allows you to create a common educational space.

To perform the task of automating the control over the educational structure, it is necessary to think over the solution not only for individual schools, but for all educational institutions. It assumes gradual automation of all educational institutions, with formation of the information environment for these institutions and regional governments on the basis of the coordinated information standards

The aim of this work is to develop a subsystem of security system “The Network City. Education”. The article analyzes the given information system and formulates a typical architecture of the information system, highlights its components. We also develop a security subsystem “The Network City” within the system “The Safety School”. Actual possible threats have been considered as the components of the developed standard architecture of the information system. Mechanisms of protection against the allocated threats are considered.

Key words: information system, “The Network City”, safety of schoolchildren, information security, model of threats.