

**Всероссийская олимпиада школьников по Технологии**

**Профиль: «Информационная безопасность», 9 класс**

**Пояснительная записка**  
к проектной работе по теме:

«Проблемы информационной безопасности в сфере образовательных услуг»

Научный руководитель:

К. Ю. А., учитель информатики,

\*\*\*\*\*

Работу выполнил:

Р.М.Д., ученик 9 класса

\*\*\*\*\*

Москва

2023

## РЕФЕРАТ

Пояснительная записка: 9 страниц, 6 источников, 3 приложения.

Ключевые слова: ИНФОРМАЦИОННЫЕ СИСТЕМЫ, УЯЗВИМОСТИ, ИНТЕРНЕТ, БРУТФОРС, CWE, АВТОРИЗАЦИЯ, АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Объектом исследования являются состояние и методы обеспечения информационной безопасности в АИС «Контингент» (далее — Система, ИС), расположенной в сети «Интернет» по адресу <https://contingent.mos.ru>

В ходе выполнения работы получены следующие результаты:

1. Обнаружена уязвимость Системы к угрозе информационной безопасности, зарегистрированной в базе уязвимостей информационных систем CWE под номером CWE-209.<sup>1</sup>
2. Обнаружена уязвимость Системы к угрозе информационной безопасности, зарегистрированной в базе уязвимостей информационных систем CWE под номером CWE-1295.<sup>2</sup>
3. Обнаружена уязвимость Системы к угрозе информационной безопасности, зарегистрированной в базе уязвимостей информационных систем CWE под номером CWE-540.<sup>3</sup>
4. Предложены возможные сценарии реализации угроз информационной безопасности, уязвимость системы к которым обнаружена в ходе настоящей НИР.
5. Разработана концепция закрытия возможности реализации вышеупомянутых угроз информационной безопасности в Системе.
6. Разработан прототип интегрируемой информационной системы, в которой возможность реализации исследованных угроз информационной безопасности сведена к нулю.

---

<sup>1</sup> MITRE CWE-209: Generation of Error Message Containing Sensitive Information, <https://cwe.mitre.org/data/definitions/209.html>

<sup>2</sup> MITRE CWE-1295: Debug Messages Revealing Unnecessary Information, <https://cwe.mitre.org/data/definitions/1295.html>

<sup>3</sup> MITRE CWE-540: Inclusion of Sensitive Information in Source Code, <https://cwe.mitre.org/data/definitions/540.html>

## ВВЕДЕНИЕ

Актуальность данной темы заключается в том, что в условиях продолжающейся цифровизации в сфере образовательных услуг контроль прав доступа в образовательные учреждения начального и основного общего образования города Москвы начал происходить с использованием информационных технологий (пр. КИС «ГУСОЭВ», «МЭШ», АИС «Контингент»), а значит, при условии допустимости сценария, реализовывающего угрозу информационной безопасности для указанных информационных систем, возникает угроза конфиденциальности персональных данных учащихся, а также возможная угроза целостности информации, проходящей через указанные информационные системы.

Более того, эта тема затрагивает миллионы пользователей, таких как учащиеся, педагоги, работники административного состава образовательных учреждений, за счёт чего данная тема становится ещё актуальнее.

Целью проектной работы является анализ уязвимостей, выявленных в АИС «Контингент» (далее — Система), а также разработка программного решения для закрытия возможности реализации угроз информационной безопасности в Системе.

Объектом исследования являются состояние и методы обеспечения информационной безопасности в АИС «Контингент», расположенной в сети «Интернет» по адресу <https://contingent.mos.ru>

Предметом исследования являются уязвимости, выявленные в АИС «Контингент».

Актуальность описанных угроз информационной безопасности для данной системы также увеличивается за счёт того, что в системе АИС «Контингент» отсутствует эффективный инструмент для защиты от подобных угроз.

Для изучения этой темы информационной базой послужили базы данных с описанием векторов компьютерных атак (CAPEC, OWASP), расположенные в сети «Интернет», база уязвимостей информационных систем MITRE CWE, а также методический документ ФСТЭК России «Методика оценки угроз безопасности информации».

## ОСНОВНАЯ ЧАСТЬ

В ходе личного исследования работы систем «Проход и Питание» в Московских школах мною была найдена АИС «Контингент», она же — АИС «Зачисление в ОУ». Система расположена в сети Интернет по адресу <https://contingent.mos.ru>. Насколько известно из открытых источников (информация с сайта ДИТ Москвы, с сайтов общеобразовательных учреждений, с сайта ДОНМ Москвы), АИС «Контингент» отвечает в том числе за привязку учащегося к образовательной организации, формирование личных дел обучающихся, работу с единой базой образовательных достижений обучающихся, а также взаимодействие по защищённому каналу связи с внешними информационными системами.

Таким образом, при несанкционированном доступе в систему, нарушается как минимум конфиденциальность персональных данных обучающихся.

После изучения Системы, мною были замечены следующие моменты:

1. Основной портал аутентификации пользователей находится по адресу <https://contingent.mos.ru/portal/> (далее — основной портал). Сайт делает редирект на него при запросе на <https://contingent.mos.ru>.
2. В исходном коде страницы <https://contingent.mos.ru/portal/> имеется строка с закомментированной гиперссылкой (см. Приложение 1), которая ведёт на страницу <https://contingent.mos.ru/portal/restore-password.html>, внешне не отличающуюся от основного портала аутентификации (далее — дополнительный портал).

После небольшого изучения ответов Системы на разных порталах, я заметил, что основной портал в ответ на неправильную связку логин-пароль выдаёт только ошибку «Указан неверный логин или пароль. Попробуйте ещё раз» (см. Приложение 2), а дополнительный портал обладает схожим поведением, однако после 10 неправильных связок логин-пароль с существующим логином выдаёт ошибку «Ваша учетная запись заблокирована на 5 минут, так как 10 раз подряд был введен неправильный пароль» (см. Приложение 3), тем самым раскрывая пользователю факт существования пользователя с таким логином.

В конце 2022 года компания NordPass опубликовала своё ежегодное исследование, в котором назвала 200 самых используемых паролей в мире.<sup>4</sup> Нас, в частности, интересуют пароли «guest», «12345», «123» и «1234». Согласно данным исследования, их использовали 376417, 188602, 60795 и 106929 человек соответственно. Это — одни из самых распространённых паролей в мире.

На данный момент создано большое количество инструментов для реализации атаки подбора паролей «грубой силой», а также для подбора с использованием так называемых «словарей» — списков паролей, по которым идёт перебор.

---

<sup>4</sup> NordPass, 2022 год, <https://nordpass.com/most-common-passwords-list/>

Примерами таких инструментов являются утилиты «TNC-Hydra», «ffuf».

Предположим, что нам необходимо реализовать атаку с конечным результатом в виде проникновения в Систему путём перебора данных для входа.

Таким образом, нам понадобится сначала получить логин для входа, а после — пароль для него.

Для получения логина воспользуемся словарём паролей с 1 миллионом строк от компании SecLists.<sup>5</sup>

Рассчитаем время получения логина при условии его нахождения в списке. Мы знаем, что если логин существует, то после 10 попыток доступа к дополнительному portalу аутентификации, вход по этому логину будет заблокирован на 5 минут, о чём будет сказано в ответе сервера.

В таком случае каждый логин надо попробовать 10 раз. Предположим, что поток утилиты для автоматизации процесса подбора отправляет 10 запросов в секунду, а злоумышленник ведёт подбор с использованием трёх потоков. Тогда формула времени, необходимого для получения логина будет равна:

$$t_{\text{логин}} = 1\,000\,000 \text{ строк} * 10 \text{ раз} \div \left(10 \frac{\text{строк}}{\text{сек}} * 3 \text{ потока}\right) \div 60 \text{ сек} \div 60 \text{ мин} \approx 92 \text{ часа} \approx 4 \text{ дня}$$

Злоумышленнику будет необходимо максимум 4 дня для получения существующего логина путём перебора по словарям.

Далее необходимо получить пароль. Воспользуемся упрощённой версией словаря «rockyou.txt» от вышеупомянутой компании SecLists.<sup>6</sup> Он содержит 100 тысяч строк. Скорость отправки запросов и количество потоков оставим теми же, что и в предыдущем примере. Учтём, что каждые 10 строк система будет блокировать аккаунт на 5 минут (300 секунд). При этом, если система на основном portalе авторизации не блокирует аккаунт, время простоя будет равно нулю. Таким образом:

$$t_{\text{простоя}} = 100\,000 \text{ строк} \div 10 \frac{\text{строк}}{\text{сек}} * 300 \text{ сек} \div 60 \text{ сек} \div 60 \text{ мин} \div 24 \text{ часа} \approx 34 \text{ дня}$$

$$t_{\text{пароль}} = \left(100\,000 \text{ строк} \div \left(10 \frac{\text{строк}}{\text{сек}} \div 60 \text{ сек} \div 60 \text{ мин} \div 24 \text{ часа}\right)\right) + t_{\text{простоя}} \approx 35 \text{ дней}$$

$$t_{\text{доступ}} = t_{\text{логин}} + t_{\text{пароль}} \approx 39 \text{ дней}$$

Исходя из вышеуказанных вычислений, для получения доступа к системе злоумышленнику понадобится максимум 39 дней, что ничтожно мало, поскольку в системе хранятся конфиденциальные данные учащихся.

---

<sup>5</sup> SecLists, 2019 год, <https://github.com/danielmiessler/SecLists/blob/master/Usernames/xato-net-10-million-usernames-dup.txt>

<sup>6</sup> SecLists, 2019 год, <https://github.com/danielmiessler/SecLists/blob/master/Passwords/Leaked-Databases/rockyou.txt.tar.gz>

Поскольку АИС «Контингент» содержит конфиденциальные данные учащихся, необходима срочная реализация программного решения, предотвращающего реализацию описанной угрозы информационной безопасности. Соответствующее программное решение можно реализовать с использованием языка программирования Python и его устанавливаемых библиотек Flask и Flask-Limiter.

За основу исходного кода «фронтенда» решения можно взять имеющуюся кодовую базу из части аутентификации в Системе, убрав страницу `restore-password.html` из кодовой базы, а также убрав комментарий, содержащий гиперссылку на эту страницу.

В случае невозможности исключения страницы `restore-password.html` из кодовой базы, следует изменить ответ сервера на неверную связку логин-пароль с существующим логином: блокировать доступ к этому аккаунту на 5 минут после 10 неправильных попыток, но не сообщать об этом пользователю, выводя лишь стандартную заглушку вида «Указан неверный логин или пароль. Попробуйте ещё раз». Это максимально ограничит возможность атаки перебором в данном направлении.

После анализа доступных вариантов решения мною было принято решение использовать второй вариант, не исключая страницу восстановления пароля из кодовой базы.

Для сохранения функционала восстановления забытого пароля мною был разработан дополнительный сервис, отвечающий за отправку писем на почту пользователя, которому нужно сменить пароль. Для этого был поднят отдельный почтовый сервер, настроены DMARC, DKIM и SPF записи DNS.

Итоговое решение включает в себя сервис с механизмами аутентификации, регистрации новых пользователей и сброса пароля с помощью уникальной ссылки, передающейся пользователю с помощью e-mail. В связи с исчерпывающими, но скорректированными ответами сервера на запросы пользователя, угроза перебора логина или пароля, описанная выше, исключается.

Решение было развёрнуто мною в сети «Интернет» по адресу \*\*\*\*\*

Исходный код решения находится в открытом доступе на сервисе GitHub в сети «Интернет» по адресу \*\*\*\*\*.

## ЗАКЛЮЧЕНИЕ

В заключение, хотелось бы отметить, что информационные системы, особенно находящиеся в т.н. «государственном секторе», требуют частого анализа кода и проведения аудита информационной безопасности. Это необходимо во избежание возникновения ситуаций со взломом информационных систем, появления т.н. «утечек» персональных данных в сети «Интернет».

Разработанное мной решение полностью устранило проблему перебора пароля с использованием метода грубого перебора («брутфорса») в информационной системе, обрабатывающей важные данные, а значит и устранило потенциальную возможность критической атаки.

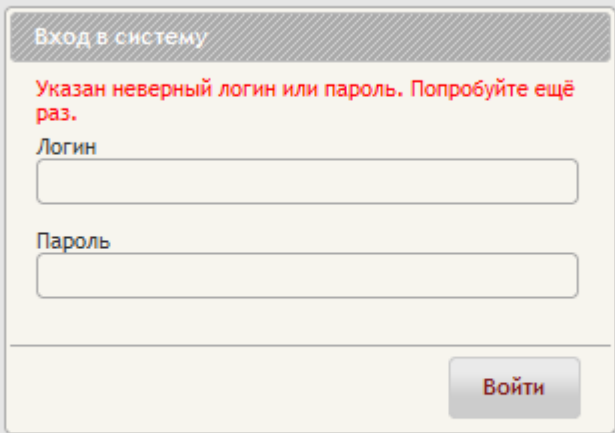
Использование библиотеки Flask-Limiter и отсутствие «чувствительной» информации в системных ошибках вкупе помогает не только не давать лишнюю информацию потенциальному злоумышленнику, но и блокирует чрезмерную активность, создавая ещё один барьер между атакующим и конфиденциальной информацией.

## ПРИЛОЖЕНИЯ

### Приложение 1:

```
121 <body>
122 <div class="demo">
123 <div class="ui-widget-overlay"></div>
124 <div id="dialog" title="Вход в систему">
125   <form name="clogin" method="POST" action='j_security_check'>
126     <fieldset>
127       <label for="name">Логин</label>
128       <input type="text" name="j_username" id="name" class="text ui-widget-content ui-corner-all" />
129
130       <label for="password">Пароль</label>
131       <input type="password" name="j_password" id="password" value="" class="text ui-widget-content ui-corner-all" />
132       <!--<a href="restore-password.html">Забыли пароль?</a><br/>-->
133     </fieldset>
134   </form>
135 </div>
136
137 </div>
138
139 <div class="bottom-panel ui-widget">
140   Техническая поддержка: <strong>+7 (495) 539-38-38</strong><br/>e-mail: <a href="mailto:contingent@mos.ru">contingent@mos.ru</a>
141 </div>
142
143 </body>
```

### Приложение 2:



Вход в систему

Указан неверный логин или пароль. Попробуйте ещё раз.

Логин

Пароль

Войти



### Приложение 3:

Вход в систему

Ваша учетная запись заблокирована на 5 минут, так как 10 раз подряд был введен неправильный пароль.

Логин

Пароль

Войти