Особенности реализации политики безопасности дистанционного курса

Вадим Алексеевич Шуйгин
студент
Уфимский государственный авиационный технический университет
Уфа, Россия
Shuydvadal91@ya.ru
0000-0000-0000-0000

Газиз Даутович Шугуров
студент
Уфимский государственный авиационный технический университет
Уфа, Россия
Shugurgaz92@gmail.com
0000-0000-0000-0000

Сапият Загировна Магомедова
студент
Национальный исследовательский университет ИТМО
Москва, Россия
Sapmagom100801@ya.ru
0000-0000-0000-0000

Данила Александрович Радайкин
студент
Московский государственный университет имени М.В.Ломоносова
Москва, Россия
danilaradajkin@yandex.ru
0000-0000-0000-0000

Кирилл Григорьевич Грязнов
студент
Российский государственный аграрный университет — МСХА им. К. А. Тимирязева
Москва, Россия
Gryaznovvv20@ya.ru
0000-0000-0000-0000

Поступила в редакцию 20.04.2022
Принята 19.05.2022
Опубликована 20.06.2022

10.25726/h2261-5220-4977-z

Аннотация

Обеспечение информационной безопасности дистанционно курса предусматривает создание системы защиты его информационных ресурсов от злоумышленников, которые захотят эти ресурсы использовать, модифицировать или просто уничтожить. Во время онлайн-обучения увеличилось количество кибер инцидентов с участием ресурсов, используемых для организации образовательного процесса. «Лидером» стало программное обеспечение Zoom, которое позволяет создавать онлайн-конференции. Основным вектором атак является установка вредоносного программного обеспечения

под видом программы Zoom от оригинального поставщика. На втором месте оказалась система управления образовательным содержимым MOODLE, где основным вектором атак стала рассылка электронных писем со ссылками на фишинговые страницы для авторизации. Нарушение доступности является следствием отказа в обслуживании. Проще говоря, ресурс, на котором размещены нужные файлы, становится недоступным для пользователей. Студенты не могут получить задание, загрузить отчет или пройти тестирование. Преподаватель не может добавить новые файлы или проверить ранее загруженные отчеты. Фактически такая проблема является критической для учебного процесса.

Ключевые слова

политика безопасности, дистанционный курс, техническая защита, информационная безопасность.

Введение

Политика информационной безопасности дистанционного курса по отношению к пользователям-студентам должна быть доступной в каждом учебном заведении и конкретизирована в виде правил по информационной безопасности.

Необходимыми мерами защиты дистанционного курса учебной среды от умышленных и неумышленных действий студентов являются: контроль со стороны администратора, настройка и ограничение доступа к критическим ресурсам, контроль и реагирование на несанкционированные действия программных средств защиты (Галямова, 2017).

Основной целью политики безопасности дистанционного курса является неукоснительное выполнение пользователями-студентами правил информационной безопасности, которые делают невозможным или сводят к минимуму вред, который они могут повлечь своими действиями. Эта цель реализуется организационными, программно-аппаратными и воспитательными мероприятиями.

К организационным мероприятиям относится разработка, внедрение и контроль за соблюдением политики безопасности системы информационной безопасности дистанционного курса пользователями-студентами. Контроль за выполнением возложен на администратора (Журавлев, 2005).

Материалы и методы исследования

Особого внимания требует проблема доступа пользователей-студентов к сети Интернет.

Правила по доступу в сеть Интернет, установленные в учебном заведении, должны быть формализованы, то есть иметь вид обязательного документа. Эти правила обязательно должны включать инструкцию по публикации в сети личных данных студентов, их фотографий, аудио - и видеоматериалов и тому подобное.

Часть правил политики безопасности, касающейся доступа пользователей студентов к сети Интернет, должна быть уведомлена перед началом соответствующих занятий самим преподавателем (ГенДокс, 2009).

Программно-аппаратные средства принятой политики безопасности реализуются через систему управления (контроля) доступа пользователей к ресурсам, которая включает идентификацию и аутентификацию пользователей, управление (контроль) доступа к ресурсам, протоколирование и аудит действий пользователей.

Программно-аппаратные средства должны гарантировать защищенность критически важных компонентов программного обеспечения учебного компьютерного комплекса от несанкционированных и ошибочных действий пользователей. В правилах разграничения доступа необходимо запретить доступ этих пользователей к системным областям диска, а также запретить модификацию ими программного обеспечения, учебной и другой важной информации.

Рекомендуется предоставлять доступ к сети Интернет только с тех компьютеров, которые постоянно находятся в поле зрения преподавателя. Также стоит использовать программы, позволяющие отображать содержимое экранов всех компьютеров на мониторе преподавателя и тем самым позволяют следить за действиями студентов.

Результаты и обсуждение

Основными в реализации политики безопасности дистанционного курса учебной среды являются воспитательные меры, поскольку они используются как для предотвращения несанкционированного доступа, так и для воздействия на нарушителей правил безопасности с целью их перевоспитания. Очень важно установить правила наказания тех, кто злоупотребляет доступом; нарушение могут быть и не столь значительными, но должны быть обсуждены, а за серьезные проступки должны быть предусмотрены серьезные меры наказания.

Главной целью воспитательных мероприятий является осознание студентами ответственности за свои действия даже в виртуальной среде, усвоение этических норм поведения в этой среде, результатом чего является формирование у студентов компетентности в области информационной безопасности.

К методам, которые используются для повышения защищенности и возобновляемости программной составляющей информационной системы дистанционного курса, является резервирования и периодическая проверка его целостности (Семенов, 2005). Эти методы могут реализовываться системными утилитами, входящими в состав операционной системы или другими программами, например, антивирусными.

Итак, проанализировав приведенную выше информацию, можно предложить следующие правила обеспечения политики безопасности дистанционного курса:

1. Пользователь типа администратор и преподаватель должен иметь пароль для своей учетной записи, который удовлетворяет установленным требованиям;
2. Пользователи типа студент, гость, пользователь аутентифицируется должны иметь минимальный набор прав на работу с электронным курсом.
3. При создании дистанционного курса, и при создании каждого электронного ресурса, необходимо настраивать права на работы с ним.
4. После создания дистанционного курса, необходимо создать его резервную копию.
5. После создания дистанционного курса необходимо настроить особенности регистрации пользователей на него и обязательно отключить возможность саморегистрации на курс.
6. Во время работы с дистанционным курсом, на персональном компьютере пользователя необходимо активировать и обновить антивирусное программное обеспечение, которое защитит от нежелательных вирусов, которые могут повредить часть дистанционного курса.
7. После завершения срока обучения на дистанционном курсе, преподаватель должен очистить его от старой статистики, отчетов, удалить все выполненные задания, отчислить с курса всех бывших пользователей.
8. После очистки дистанционного курса, его необходимо скрыть и закрыть доступ студентов к нему.

Что касается работы с платформой, для начала определим активы учебного процесса и соответствующие угрозы. Основными активами являются следующие:

- файлы (лекции, задания на лабораторные работы и др);
- банк вопросов (общее множество вопросов, по которым создаются тесты для контроля знаний);
- оценки (лабораторные работы и модульный контроль знаний).

Активом называется объект, для которого обеспечивается состояние защищенности (Научно-исследовательская, 2020).

Далее определим возможные угрозы для указанных активов.

Компрометация банка вопросов может возникнуть путем эксплуатации уязвимостей системы или путем получения доступа к панели администратора системы (Урсул, 1968). Сценарии таких атак рассмотрены в (Шеннон, 1956). Банк вопросов содержит вопросы, варианты ответов и правильные ответы, если таковые имеются.

Модификация оценок по лабораторным работам и модулям появляется у нарушителя по тем же причинам, что и компрометация банка вопросов.

Платформами, которые рассматриваются, являются:

- системы управления образовательным контентом с открытым исходным кодом;
- системы управления образовательным содержанием индивидуальной разработки;
- сервис Google Classroom;
- электронная почта и облачные хранилища.

Конечно же, это не все платформы, которые могут быть использованы для дистанционного обучения. Выбор именно этих платформ обусловлен их популярностью во всем мире, все они используются на кафедре компьютерных систем МГУ.

Системы управления образовательным контентом с открытым исходным кодом представляют класс систем, которые позволяют развертывать веб-ресурсы для осуществления образовательного процесса. Примерами таких систем являются MOODLE и Sakai, количество их инсталляций измеряется сотнями тысяч (Шершнева, 2011). Особенностью таких систем является наличие сообщества, которое выявляет проблемы безопасности и может выявить проблемы быстрее злоумышленников. Разработчики системы оповещаются о найденной проблеме, которая устраняется путем выпуска новой версии или установки патча для существующей версии.

Для корректного функционирования при большом количестве активных пользователей система требует достаточно большое количество ресурсов, поэтому целесообразно такие системы разворачивать на отдельном сервере. Хостинг-провайдеры не рекомендуют (а иногда и запрещают) установку таких систем на общем хостинге.

Основным отличием в аспекте безопасности систем управления образовательным содержанием индивидуальной разработки является отсутствие большого сообщества, способного выявить проблемы безопасности. Очень большую роль играет уровень профессионализма разработчиков такой системы, поскольку риск написания опасного кода у начинающих разработчиков гораздо выше.

Поскольку такая система принадлежит классу «mission critical», логичным и обоснованным является выполнение тестирования на проникновение как этапа жизненного цикла программного обеспечения (Эшби, 1959; Валянский, 2005).

Сервис Google Classroom является бесплатным, позволяет размещать образовательные материалы и управлять участниками образовательного процесса. Особенностью является то, что для создания нового ресурса нет необходимости в использовании дополнительной сторонней информационной инфраструктуры. Сервис имеет гораздо меньшую гибкость, чем системы управления образовательным контентом, которые позволяют расширять функциональность путем установки различных модулей.

Электронную почту и облачные хранилища сложно назвать полноценной платформой для дистанционного образования, однако этот подход также используется из-за своей простоты. При этом гибкость и удобство пользования являются минимальными среди рассматриваемых платформ.

Предположением является то, что системы управления образовательным содержимым развернуты на веб-сервере традиционным способом – без балансировщика нагрузки и без возможности динамического масштабирования в пределах инфраструктуры. Также предположением является равнозначность критериев оценки, но также возможно использование подхода со взвешенными коэффициентами.

Различные оценки вероятности нарушения доступности различных платформ обусловленные особенностями реализации – первые две платформы, как правило, создаются в виде централизованного ресурса, другие две платформы реализованы на децентрализованной инфраструктуре.

Различия в возможности модификации и компрометации данных обусловлены возможными уязвимостями в платформах. Lcms с открытым исходным кодом имеют оценки ниже, чем lcms индивидуальной разработки из-за того, что первые, как правило, имеют большое сообщество, которое способно выявлять проблемы безопасности быстрее, чем злоумышленники. Вероятность компрометации данных выше, чем вероятность модификации, что подтверждается информацией из баз данных уязвимостей о многочисленных уязвимостях систем управления образовательным содержимым.

Рассматривая атаки, связанные с модификацией запросов к базе данных (SQL-инъекция), проблема чаще встречается в запросах на получение данных, чем в запросах на вставку и обновление.

Для представленных в таблице 1 платформ справедливым является такой порядок (в порядке увеличения вероятности реализации угроз):

- электронная почта и облачные хранилища;
- сервис Google Class;
- LCMS (открытый исходный код);
- LCMS (индивидуальной разработки).

Представленный выше порядок был основан лишь на аспекте кибербезопасности платформ. Этот же порядок является справедливым для сортировки платформ по гибкости и удобству использования – наиболее удобная система является самой опасной.

Заключение

Проблема выбора – это поиск компромисса между безопасностью и удобством в виде широкой функциональности системы. При развертывании системы управления образовательным содержимым важно помнить, что эта система является объектом критической информационной инфраструктуры, и для нее должны выполняться требования к критическим системам, в частности использоваться механизмы создания резервных копий, должны быть разработаны схемы максимально быстрого восстановления рабочего состояния.

Дальнейшие исследования могут быть направлены на исследование проблем безопасности в рамках одного класса систем управления образовательным контентом с открытым исходным кодом.

Список литературы

1. Валянский С.И. Теория информации и образование. Условия выживания России. М.: АИРО-XX; «Крафт+», 2005. 140 с. http://internat.msu.ru/wp-content/uploads/2013/08/%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_ %D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC.pdf

2. Галямова Е.В., Павлов Ю.Н. История науки «Теория информации» / МГТУ им. Н.Э. Баумана. М., 2017. http://engineering-science.ru/doc/48780.html

3. ГенДокс. Информационные технологии в управлении. 2009. http://gendocs.ru/v39822/?cc=6

4. Журавлев Ю.И. Фундаментально-математический и общекультурный аспекты школьной информатики // Вопросы образования. 2005. № 3. https://vo.hse.ru/2005--3/27044703. html

5. Научно-исследовательская лаборатория «Бизнес-школа информационных технологий». Теоретические основы информатики. Имитационное моделирование: Исходные понятия информатики. https:// it.rfei.ru/course/~uibT/~GInfy6uu

6. Семенов А.Л. Качество информатизации школьного образования // Вопросы образования. 2005. https://vo.hse. ru/2005--3/27044823.html

7. Урсул А.Д. Природа информации. М., 1968. http://inion.ru/site/assets/files/1474/ursul_a_d_priroda_informacii.pdf

8. Шеннон К., Уивер Л. Математическая теория связи. М.: Физматгиз, 1956. С. 46. https://books.google.ru/books?id = lo__AgAAQBAJ&pg=PA398&lpg=PA398&dq

9. Шершнева В.А. Формирование математической компетентности студентов инженерного вуза на основе полипарадигмального подхода: монография. Красноярск, 2011. https://search.rsl.ru/ru/record/01005420610

10. Эшби У.Р. Введение в кибернетику. М.: ИЛ, 1959. С. 27. http://publ.lib.ru/ARCHIVES/E/ESHBI_Uil'yam_Ross/_Eshbi_U.R..html

Features of the implementation of the security policy of the distance course

Vadim A. Shujgin
student
Ufa State Aviation Technical University
Ufa, Russia
Shuydvadal91@ya.ru
0000-0000-0000-0000

Gaziz D. Shugurov
student
Ufa State Aviation Technical University
Ufa, Russia
Shugurgaz92@gmail.com
0000-0000-0000-0000

Sapiiat Z. Magomedova
student
ITMO National Research University
Moscow, Russia
Sapmagom100801@ya.ru
0000-0000-0000-0000

Danila A. Radaikin
student
Lomonosov Moscow State University
Moscow, Russia
danilaradajkin@yandex.ru
0000-0000-0000-0000

Kirill G. Griaznov
student
Russian State Agrarian University — K. A. Timiryazev Agricultural Academy
Moscow, Russia
Gryaznovvv20@ya.ru
0000-0000-0000-0000

Received 20.04.2022
Accepted 19.05.2022
Published 20.06.2022

10.25726/h2261-5220-4977-z

Abstract

Ensuring information security remotely of the course provides for the creation of a system to protect its information resources from intruders who want to use, modify or simply destroy these resources. Information security is understood as "the state of information security, in which its confidentiality, accessibility and integrity are ensured. The complex nature of the protection problem suggests that a combination of legislative, organizational, and software and technical measures is necessary to solve it. Knowledge of possible threats, as well as vulnerabilities of the information system, is necessary in order to choose the most effective means of

ensuring security. One of the most dangerous and frequent are unintentional errors of users, operators, system administrators and other persons serving information systems. Sometimes such errors lead to direct losses (incorrectly entered data, an error in the program that caused the system to stop or collapse). Sometimes they create weaknesses (most often due to administrative errors) that can be exploited by attackers. The second place in terms of damage is occupied by theft and falsification. In most cases, the perpetrators turned out to be full-time employees of organizations who were well acquainted with the working hours and protective measures. The key stage for building a reliable information system is the development of a security policy. There are several definitions of this concept.

Keywords
security policy, distance learning, technical protection, information security.

References

1. Valjanskij S.I. Teorija informacii i obrazovanie. Uslovija vyzhivanija Rossii. M.: AIRO-HH; «Kraft+», 2005. 140 s. http://internat.msu.ru/wp-content/uploads/2013/08/%D0%A2%D0%B5%D0%BE%D1%80%D0%B8%D1%8F_ %D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC.pdf
2. Galjamova E.V., Pavlov Ju.N. Istorija nauki «Teorija informacii» / MGTU im. N.Je. Baumana. M., 2017. http://engineering-science.ru/doc/48780.html
3. GenDoks. Informacionnye tehnologii v upravlenii. 2009. http://gendocs.ru/ v39822/?cc=6
4. Zhuravlev Ju.I. Fundamental'no-matematicheskij i obshhekul'turnyj aspekty shkol'noj informatiki // Voprosy obrazovanija. 2005. № 3. https://vo.hse.ru/2005--3/27044703. html
5. Nauchno-issledovatel'skaja laboratorija «Biznes-shkola informacionnyh tehnologij». Teoreticheskie osnovy informatiki. Imitacionnoe modelirovanie: Ishodnye ponjatija informatiki. https:// it.rfei.ru/course/~uibT/~GInfy6uu
6. Semenov A.L. Kachestvo informatizacii shkol'nogo obrazovanija // Voprosy obrazovanija. 2005. https://vo.hse. ru/2005--3/27044823.html
7. Ursul A.D. Priroda informacii. M., 1968. http://inion.ru/site/assets/files/1474/ ursul_a_d_priroda_informacii.pdf
8. Shennon K., Uiver L. Matematicheskaja teorija svjazi. M.: Fizmatgiz, 1956. S. 46. https://books.google.ru/books?id = Io__AgAAQBAJ&pg=PA398&lpg=PA398&dq
9. Shershneva V.A. Formirovanie matematicheskoj kompetentnosti studentov inzhenernogo vuza na osnove poliparadigmal'nogo podhoda: monografija. Krasnojarsk, 2011. https://search.rsl.ru/ru/record/01005420610
10. Jeshbi U.R. Vvedenie v kibernetiku. M.: IL, 1959. S. 27. http://publ.lib.ru/ARCHIVES/ E/ESHBI_Uil'yam_Ross/_Eshbi_U.R..html