сетевой научный журнал ISSN 2518-1092

НАУЧНЫЙ РЕЗУЛЬТАТ

RESEARCH RESULT

Том 2 | № 1
Volume 2

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

INFORMATION TECHNOLOGY

Сайт журнала:
rrinformation.ru
сетевой научный рецензируемый журнал
online scholarly peer-reviewed journal

НАУЧНЫЙ РЕЗУЛЬТАТ
RESEARCH RESULT

СЕРИЯ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION TECHNOLOGIES SERIES

Журнал зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Свидетельство о регистрации средства массовой информации Эл. № ФС77-69101 от 14 марта 2017 г.

The journal has been registered at the Federal service for supervision of communications information technology and mass media (Roskomnadzor)
Mass media registration certificate El. № FS 77-69101 of March 14, 2017

Том 2, № 1. 2017

СЕТЕВОЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
Издается с 2016 г.
ISSN2518-1092

Volume 2, № 1. 2017

ONLINESCHOLARLYPEER-REVIEWEDJOURNAL
First published online: 2016
ISSN 2518-1092

Учредитель: Федеральное государственное автономное образовательное учреждение высшего образования
«Белгородский государственный национальный исследовательский университет»
Издатель: НИУ «БелГУ». Адрес издателя: 308015 г. Белгород, ул. Победы, 85.
Журнал выходит 4 раза в год

Founder: Federal state autonomous educational establishment of higher education
«Belgorod State National Research University»
Publisher: Belgorod State National Research University
Address of publisher: 85 Pobeda St., Belgorod, 308015, Russia
Publication frequency: 4 /year

СОДЕРЖАНИЕ

CONTENTS

СИСТЕМНЫЙ АНАЛИЗ
И УПРАВЛЕНИЕ

SYSTEMANALYSISANDPROCESSING
OFKNOWLEDGE

ИНФОРМАЦИОННО-
ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

SYSTEMANALYSISANDPROCESSING
OFKNOWLEDGE

УДК 004.56 **DOI:10.18413/2518-1092-2017-2-1-20-27**

Оладько В.С.[1]
Бабенко А.А.[2]
Алексина А.А.[2]

ОЦЕНКА ЗАЩИЩЕННОСТИ СИСТЕМЫ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ ВУЗА

[1)] Финансовый университет при Правительстве Российской Федерации
Ленинградский просп., 49, г. Москва, 125993 (ГСП-3), Россия
[2)] Волгоградский государственный университет. Проспект Университетский, 100, г. Волгоград, 400062, Россия
e-mail: oladko.vs@yandex.ru, ba_benko@mail.ru, ulesova_anastasia@mail.ru

Аннотация
Исследование посвящено проблеме информационной безопасности системы дистанционного образования вуза. Выделены функции, задачи, субъекты и элементы системы дистанционного образования. Определены ценные активы и информационные ресурсы. Описан технологический процесс обработки информации в системе дистанционного образования и выделены его уязвимости. Составлена модель угроз и выделены основные направления обеспечения безопасности системы дистанционного образования. Показана необходимость проведения регулярной оценки защищенности, как средства контроля эффективности системы защиты. Предложен и формализован подход к выбору рационального метода оценки защищенности системы дистанционного образования. В соответствии с разработанным подходом проведен сравнительный анализ методов оценки защищённости, показавший, что при разработке модели оценки защищенности СДО вуза наиболее рациональными являются методы количественно-качественной оценки защищенности по уровням и квалиметрическим шкалам.
Ключевые слова: информационная безопасность; угроза; атака; информационная система; образовательное учреждение; модель угроз.

UDK 004.56

Oladko V.S.[1]
Babenko A.A.[2]
Aleksina A.A.[2]

SECURITY ASSESSMENT OF UNIVERSITY DISTANCE EDUCATION

[1)] Financial University under the Government of the Russian Federation,
49 Leningradsky prosp., Moscow, 125993 (GSP-3), Russia
[2)] Volgograd State University, 100 Prospect Universitetskiy, Volgograd, 400062, Russia
e-mail: oladko.vs@yandex.ru, ba_benko@mail.ru, ulesova_anastasia@mail.ru

Abstract
Research is devoted to information security problem of distance education university system. The functions, tasks, subjects and elements have been determined in the system of distance education. The technological process of processing information in the system of distance education is described and are marked its vulnerability. The model of threats is made and identified basic directions of the security system of distance education. The need for regular assessment of the security as a means of monitoring the effectiveness of the protection system is shown. The authors have proposed and formalized approach to the choice of rational method of distance education system security assessment. A comparative analysis of the vulnerability assessment methods showed that the development model of the university LMS security assessment is the most rational methods of quantitative and qualitative evaluation of security through the levels.
Keywords: information security; threats; attacks; information system; educational institution; threat model.

Введение

В настоящее время одним из важных направлений в глобализации образовательного пространства является применение средств и систем дистанционного образования (СДО), позволяющих адекватно и гибко реагировать на потребности общества и обеспечивать реализацию конституционного права на образование каждого гражданина [3]. Любая СДО использует информационно-коммуникационные технологии и сети передачи данных для осуществления взаимодействия между участниками образовательного процесса, хранения и обработки информации. СДО строится на базе информационной системы (ИС) учебного заведения и представляет собой распределенное, гетерогенное приложение с базой данных и web-интерфейсами. Как показано в работах [1, 2] подобная архитектура и принцип функционирования порождает ряд проблем связанных с безопасностью сервисов СДО, а также качеством предоставляемых пользователям услуг. Нарушение безопасности СДО в результате воздействий различной природы, приводит и к нарушению информационной безопасности (ИБ) в сегменте или всей ИС учебного заведения. Вывод подтверждается статистикой представленной компанией Positive Technologies в 2016 году [5], показывающей, что 30% всех атак на корпоративные ресурсы идут через web-приложения, что связано с высоким процентом критически опасных уязвимостей web-инфраструктуры (70%). Следовательно, для предотвращения различных сценариев нарушения ИБ, как СДО, так и базовой ИС учебного заведения, необходимо осуществлять периодический контроль над состоянием защищенности системы, выявлять потенциальные риски и своевременно применять механизмы безопасности, направленные на предотвращение угроз и минимизацию рисков.

Анализ систем дистанционного образования вуза

В настоящее время существуют множество СДО вузов. Это готовые программные продукты – «Прометей». «СТ Курс», Moodle, «Интразнание», «Батисфера» и собственные разработки учебного заведения – ПТК «УМКа» в ВолГУ. СДО – комплекс различных программных продуктов и решений, часть из которых находится на сервере, часть – на персональных компьютерах учащихся. Взаимодействие между ними, основанное на передаче данных, происходит через глобальную сеть. Вся информация, которая относится к учебному процессу, хранится на сервере вуза.

СДО позволяют решать следующие основные задачи:

1) организация проверки знаний обучающихся через интернет;
2) организация учебного процесса с различной степенью соответствия классической модели университетского образования;
3) создание модели распределенной образовательной сети.

Для решения описанных выше функций в СДО выделяют следующие возможные подсистемы (табл. 1).

Таблица 1

Подсистемы СДО вуза

Table 1

Subsystems LMS university

Подсистема	Функции
Регистрации	Позволяет просматривать списки учебных курсов, получать подробную информацию по курсам и программам обучения, формировать «корзину», вводить персональные данные, отправлять заказ на обработку, для входа в систему пользователи проходят процедуры идентификации и аутентификации на основе пары – логин, пароль.
Библиотека	Хранение учебных материалов в виде файлов, разграничение доступа участников учебного процесса к курсам и файлам, сбор статистики.
Подсистема календарного плана	Создание и редактирование плана-графика учебного процесса и мероприятий, установка оценок обучающимся по выполнению мероприятий плана-графика.
Тестирование	Проверка знаний обучающихся, проведение тестирования для самостоятельного контроля знаний и проведение экзаменационного тестирования, подсчет оценок и набранных балов, формирование отчета об успеваемости и прохождении курса.
Обмен информацией	Общение участников образовательного процесса посредством: форума, чата, почтовый рассылки, обмена сообщениями, доски объявлений, обмена файлами

Анализ структуры, функций и подсистем СДО выделил информационные активы: персональные данные пользователей, аутентификационные и идентификационные данные, авторские учебные материалы,

тесты и курсы, оценочные ведомости, списки студентов и групп, списки курсов, платежные данные и данные о покупке курсов, образовательные материалы, файлы, фото, изображения, видеоматериалы, учебные планы, стандарты, инструкции по работе пользователей в СДО.

Активы имеют свою ценность, уровень доступа, что следует учитывать при анализе ИБ СДО, составлении модели актуальных для СДО угроз и оценке рисков.

Функциональными компонентами СДО являются:

1) веб-приложение – внешний интерфейс, предназначенный для организации удаленного доступа студентов к содержанию учебных курсов, презентациям, мультимедийным материалам, тестам и интерактивного взаимодействия с преподавателем;

2) база данных, в которой храниться наполнение учебных курсов, размещаются оценочные материалы, электронные учебники, информация для студентов и данные об успеваемости;

3) сервер СДО, являющийся ядром системы и обеспечивающий основные функциональные возможности.

Основными субъектами взаимодействия в СДО являются внутренне и внешние пользователи, которых можно разделить на следующие группы: преподаватели вуза; методисты вуза; администраторы, программисты, специалисты по ИБ информационных подразделений вуза; студенты.

В соответствии с выделенными функциональными подсистемами и субъектами типовой технологический процесс обработки информации в СДО допустимо представить следующим образом:

1) подключение пользователя к веб-сайту СДО;

2) предоставление пользователем регистрационных данных необходимых для прохождения процедур идентификации и аутентификации и входа в личный кабинет;

3) авторизация пользователя на сервере СДО;

4) запрос на сервер СДО на предоставление информации и доступа к ресурсам курсов и подсистем СДО;

5) ввод, модификация или вывод информации открытого и/или ограниченного доступа;

6) получение пользователем запрошенного материала и данных;

7) отключение пользователя от ресурсов СДО.

В этом случае наиболее уязвимыми с точки зрения ИБ будут процессы:

- передачи идентификационных и аутентификационных данных пользователя СДО;
- обмен данными между браузером удаленного пользователя и веб-сайтом СДО.
- авторизации пользователя в СДО;
- извлечение и запись данных в БД СДО и ИС вуза;
- обмен данными между сервером СДО и сервером ИС вуза;
- система организации платежей и покупки курсов СДО;
- администрирование СДО.

Данный вывод обусловлен тем, что именно в процессе выполнения данных действий, наиболее вероятна попытка злоумышленника реализовать атаку на СДО и получить доступ к ее ресурсам, сервисам и данным.

Исследование угроз безопасности СДО

Анализ отчетов по нарушениям и инцидентов ИБ от ведущих компаний в области ИБ [5, 6] показывает, что в 82% ИС существует возможность преодоления сетевого периметра и НСД к ресурсам из внешней сети. Это особенно характерно для распределенных в сети систем, к которым относится СДО, часть архитектуры которой вынесена за периметр основной сети вуза и находится в круглосуточном доступе пользователей глобальной сети и может стать объектом целевых атак злоумышленника. Согласно [5] наиболее распространёнными стали атаки, направленные на: браузер пользователей и веб-приложения (26%), отказ в обслуживании веб-приложений и серверов (22%), на систему аутентификации пользователей (18%), которые реализуются с помощью вредоносного программного обеспечения.

Согласно проекту методического документа ФСТЭК по определению угроз безопасности в ИС [4] процесс определения ИБ должен охватывать все объекты защиты и сегменты в логических и физических границах системы. Поэтому при составлении модели угроз СДО, предлагается выделить четыре основных структурных элемента (таблица 2).

Таблица 2

Модель угроз безопасности СДО вуза

Table 2

Model security threats university LMS

	Элемент СДО	Угроза	Последствия
1	Веб-интерфейс СДО	1) SQL и PHP-инъекции; 2) XSS-атаки; 3) подделка межсайтовых запросов ; 4) атаки на браузер; 5) удаленное выполнение кода и отказ в обслуживании сервисов; 6) спам рассылки; 7) фишинг.	Нарушение конфиденциальности, целостности и доступности информации и сервисов веб-приложения СДО, финансовые потери, потери репутации вуза, проникновение на сервер СДО и ИС вуза.
2	Сервер СДО	1) перебор паролей и атаки на систему аутентификации пользователей; 2) вызов исключительных ситуаций; 3) повышение привилегий; 4) ошибки администрирования; 5) сканирование портов; 6) DDos и Dos-атаки; 7) сбои и отказы программно-аппаратных средств сервера; 8) отказ поддерживающей инфраструктуры.	Нарушение конфиденциальности, целостности и доступности информации, проникновение в ИС вуза, прерывание бизнес-процессов, нарушение доступности сервисов.
3	БД СДО	1) SQL-инъекции; 2) случайное удаление/модификация данных в БД и журналах транзакций в результате ошибок пользователей; 3) кража персональных данных; 4) НСД к БД и журналам транзакций; 5) намеренное уничтожение и модификация данных; 6) уничтожение БД в результате сбое и отказов технических средств.	Отказ от обязательств и совершенных действий, нарушение авторского права, нарушение целостности и конфиденциальности.
4	Подсистема платежей и покупки курсов.	1)НСД к платёжным данным; 2) мошенничество; 3) кража финансовых средств.	Финансовые и репутационные потери.

При реализации целевых атак, злоумышленник использует [7]:

- уязвимости в веб-приложении (CMS) и сервисах СДО;
- уязвимости в веб-браузерах пользователей СДО;
- уязвимости в прикладных программах и плагинах Adobe Reader, Adobe Flash Player и OracleJava, которые используются при выполнении скриптов, а также чтении и загрузки документов и мультимедиа файлов;
- слабые пароли и недостатки процесса аутентификации на сервере СДО;
- ошибки в конфигурировании и администрировании СДО;
- вредоносное программное обеспечение;
- слабости системы защиты информации ИС вуза и СДО.

В среднем для получения доступа к СДО внешнему злоумышленнику требуется использовать лишь две уязвимости.

Идентифицированные в общей модели угрозы безопасности СДО подлежат исследованию на предмет актуальности и необходимости применения защитных средств и механизмов, направленных на блокирование угрозы и снижение тяжести ее последствий. Для этого исследуются такие характеристики угроз как вероятность реализации и потенциальный ущерб. Оценка может производиться как на основании статистической информации, так и по результатам экспертной оценки.

Как показывает [8,10] при формировании экспертной группы привлекаются несколько категорий специалистов от аналитиков, специалистов по защите информации, разработчиков, пользователей и руководителей, которые оценивают угрозы и их параметры по количественной или качественной шкале, затем на основании оценок формируется интегральный показатель каждой угрозы. Соотношение между ущербом, вероятностью или частотой возникновения угрозы определяет уровень риска от реализации угрозы, использующийся при ранжировании угроз по степени опасности. Чем опасней угроза, тем более актуальной она является для СДО вуза. Оценку актуальности угроз рекомендуется проводить периодически на всех этапах жизненного цикла СДО, поскольку именно она указывает насколько необходимо использовать средства и механизмы, противодействующие угрозе.

Для противодействия угрозам ИБ и удержания рисков в пределах допустимого, используются различные механизмы и средства защиты информации, организационно-правового, технического и программного характера, которые реализуют общую стратегию защиты информации как в СДО, так и в вузе в целом. При реализации стратегии защиты СДО необходимо учитывать ряд особенностей, связанных с процессом функционирования СДО вуза:

− СДО должна быть доступна для пользователей 24 часа 7 дней в неделю;

− межсетевые экраны и применение SSL не всегда обеспечивают защиту от взлома СДО поскольку, доступ к веб-сайту СДО из внешних сетей должен быть всегда открыт;

− СДО часто имеет прямой доступ к данным, обрабатываемым в ИС вуза: базы данных, ERP-системы, информация об инновационных разработках и научной деятельности вуза, учебные ведомости, персональные данные;

− узконаправленные СДО, собственной разработки вуза, более восприимчивы к атакам, так как они не подвергаются такому длительному тестированию и эксплуатации, как известные коммерческие СДО;

− традиционные сетевые средства защиты не предназначены для отражения специализированных атак на веб-приложения СДО, поэтому злоумышленники при помощи браузеров легко проходят через периметр ИС вуза и получают доступ к внутренним системам и серверам;

− ручное обнаружение и устранение уязвимостей в СДО часто не дает положительных результатов – разработчики могут находить и исправлять сотни уязвимостей в коде, но злоумышленнику для проведения результативной атаки достаточно обнаружить всего одну.

Следовательно, обеспечение защиты СДО должно осуществляться на различных этапах жизненного цикла СДО. Поскольку даже если в программном коде СДО уязвимостей нет, необходима комплексная защита, учитывающая наличие базы данных, веб-приложений, сервера СДО и прочих элементов информационной инфраструктуры вуза. В соответствии с требованиями государственных стандартов по защите информации в информационных системах и регуляторов в области ИБ защита должна строиться по следующим основным направлениям:

1) составление моделей актуальных угроз ИБ в СДО;

2) контроль над безопасностью кода и наличием уязвимостей в СДО, своевременное обновление программного обеспечения;

3) использование специализированных средств защиты информации;

4) проведение периодического контроля уровня безопасности СДО и выработка управляющих решений в области ИБ в случае необходимости.

Данные направления в защите СДО вуза должны реализовываться в рамках единого комплекса мер для оценки качества и эффективности которых необходимо проводить периодический мониторинг текущей защищенности СДО, которая в сравнении с «эталонной», целевой защищенностью, будет играть роль метрики-индикатора состояния уровня общей безопасности СДО вуза. При этом частота проведения подобной оценки, как показано в [9], должна зависеть от уровня показателя защищённости, полученного в результате предыдущего контроля, чем ближе было значение показателя защищенности к целевой защищенности, тем больше временной интервал между контрольными оценками.

Выбор подхода к оценке защищенности СДО вуза

В настоящее время наиболее распространенными являются следующие подходы к оценке защищенности систем: количественно-качественная оценка защищенности по уровням и квалиметрическим шкалам, оценка защищенности как величины предотвращенного ущерба, оценка защищенности на основе

непрерывного бетта-распределения плотности вероятности ущерба, оценки количественного показателя защищенности на основе вероятностно-статистического подхода, оценка количественной защищенности с помощью сетей Петри, оценка количественной защищенности с помощью графов атак и конечных автоматов, методика CRAMM, методика RiskWatch, методика ГРИФ, методика векторного анализа ИБ.

Каждый подход имеет свои достоинства и недостатки, сложность и особенности реализации, а также форму представления показателя общей защищенности системы. Поэтому для сравнительного анализа и выбора подхода к оценке защищенности, была использована критериальная оценка. Для сравнения методик использовались следующие частные показатели оценки:

– квалификация аудитора – $Q^{\text{МОЗ}}$;
– сложность реализации $Q^{\text{МОЗ}}$;
– трудоемкость проведения оценки $Q_3^{\text{МОЗ}}$;
– открытая методика $Q_4^{\text{МОЗ}}$;
– возможность обновления $Q_5^{\text{МОЗ}}$;
– количество входных параметров $Q_6^{\text{МОЗ}}$;
– возможно получение значений входных параметров на практике $Q_7^{\text{МОЗ}}$;
– удобно применять для реальных систем $Q_8^{\text{МОЗ}}$;
– учитывает различные виды угроз $Q_9^{\text{МОЗ}}$;
– наглядность представления итогового результата оценки $Q_{10}^{\text{МОЗ}}$.

Каждый частный показатель выбора подхода к оценке защищенности $Q_i^{\text{МОЗ}}|i = 1\ldots10$ имеет свой вес, сумма весов показателей нормирована в единицу, и принимает значения в соответствии с правилами, указанными в таблице 3.

Таблица 3

Правила расчета частных показателей выбора подхода к оценке защищенности

Table 3

Rules of calculation of particular indicators choice approach to security assessment

Частный показатель	Правила выставления значений частного показателя
$Q_{10}^{МОЗ}$	$Q_{10}^{МОЗ} = \begin{cases} 1, \textit{если высокая} \\ 0.5, \textit{если средняя} \\ 0, \textit{если низкая} \end{cases}$
$Q_8^{МОЗ}, Q_5^{МОЗ}, Q_4^{МО}$ $Q_7^{МОЗ}, Q_9^{МО}$	$Q_{i=4,5,7,8,9}^{МОЗ} = \begin{cases} 1, \textit{если возможно} \\ 0, \quad \textit{если невозможно} \end{cases}$
$Q_6^{МОЗ}$	$Q_6^{МОЗ} = \begin{cases} 0, \textit{если один парамтер} \\ 0.5, \textit{если 2 параметра} \\ 1, \textit{если 3 и более параметров} \end{cases}$
$Q^{МОЗ}$ $Q_3^{МОЗ}$ $Q^{МОЗ}$	$Q_{i=1,2,3}^{МОЗ} = \begin{cases} 1, \textit{если низкая} \\ 0.5, \textit{если средняя} \\ 0, \textit{если высокая} \end{cases}$

Значения показателей используются для получения интегральной оценки см. формулу 1.

$$Q_0^{МОЗ}(j) = \sum_{i=1}^{n} w_i Q_i^{МО}$$
$$w = \sum_{i=1}^{n} w_i = 1 \qquad (1)$$

где w_i – вес, важность i частного критерия оценки, $Q_i^{МОЗ}$ – частные показатели оценки подхода, j – подход к оценке защищенности системы из списка альтернативных подходов J.

Результаты сравнения подходов представлены в таблице 4. Все оценки выставлены экспертным путем, на основе информации полученной из источников. При расстановке весов показателей выбора учитывались предпочтения и важность того или иного показателя в рамках данной работы.

Таблица 4

Результат анализа подходов к оценке защищенности

Table 4

The result of the analysis of the security assessment methods

Подход к оценке защищенности	$Q^{МОЗ}$	$Q^{МОЗ}$	$Q_3^{МОЗ}$	$Q_4^{МОЗ}$	$Q_5^{МОЗ}$	$Q_6^{МОЗ}$	$Q_7^{МОЗ}$	$Q_8^{МОЗ}$	$Q_9^{МОЗ}$	$Q_{10}^{МОЗ}$	$Q_0^{МОЗ}$
	Веса показателей выбора w_i										
	0,05	0,2	0,1	0,1	0,05	0,05	0,15	0,1	0,1	0,1	
по уровням и квалиметрическим шкалам	1	1	1	1	1	0,5	1	1	1	0,5	0,925
как величины предотвращенного ущерба	1	1	1	1	1	0	0	1	1	0,5	0,75
на основе непрерывного бетта-распределения плотности вероятности ущерба	0,5	0,5	1	1	1	0,5	0	1	0	0,5	0,55
с помощью сетей Петри	0,5	0	0	1	1	1	1	1	0	1	0,575
с помощью графов атак и конечных автоматов	0,5	0	0,5	1	1	1	0	1	1	1	0,575
методика CRAMM	1	0,5	0,5	0	0	0,5	1	1	1	1	0,675
методика RiskWatch	1	0,5	1	1	0	1	0	1	1	0,5	0,65
методика векторного анализа ИБ	1	1	1	1	1	0,5	0	1	0	0,5	0,675
методика ГРИФ	1	1	1	1	0	0,5	1	1	1	0,5	0,875

В результате сравнительного анализа получено, что наилучшем образом для основы в качестве разработки модели оценки СДО вуза подходят количественно-качественная оценка защищенности по уровням и квалиметрическим шкалам (0,925), а также оценка защищенности по методики ГРИФ (0,875), получившие максимальные значения обобщенного показателя выбора.

Заключение

При разработке модели оценки защищенности СДО необходимо использовать комбинированный подход, построенный на применении нескольких методик оценки, который учитывает требования стандартов и внутренних нормативных документов вуза, объективную информацию о наличие угроз ИБ СДО вуза и выдает ранжированный список рекомендаций, которые необходимо выполнить для построения эффективной и удовлетворяющей требованиям системы защиты информации.

Список литературы

1. Бабенко А.А. Использование дистанционных технологий при подготовке специалистов в области информационной безопасности // Известия Балтийской государственной академии рыбопромыслового флота: психолого-педагогические науки. 2011. № 4. С. 44-52

2. Колгатин А.Г. Информационная безопасность в системах открытого образования // Образовательные технологии и общество. 2014. Т.17, №1. С. 417 – 425.

3. Кошкина Е.Н. SWOT-анализ дистанционного обучения в России // Вестник Международного института экономики и права. 2013. №4 (13). С.28-31.

4. Методика определения угроз безопасности информации в информационных системах. Проект методического документа//Официальный сайт ФСТЭК России. URL: http://fstec.ru/component/attachments/download/812 (дата обращения 03.10.2016).

5. Отчет Positive Research 2016 // Аналитика компании Positive Technologies 2016. URL: http://www.ptsecurity.ru/upload/ptru/analytics/Positive-Research-2016-rus.pdf (дата обращения 29.09.2016).

6. Отчет McAfee Labs об угрозах за февраль 2015 [Электронный ресурс] // Компания McAfee Labs. URL: http://www.mcafee.com/ru/resources/reports/rp-quarterly-threat-q4-2014.pdf?cid=BHP035 (дата обращения 03.10.2016).

7. Callegari C., Vaton S., Pagano M. A. New statistical approach to network anomaly detection .Proc. of Performance Evaluation of Computer and Telecommunication Systems (SPECTS). 8 (2008); p.441–447.

8. Landoll, D.J. The security risk assessment handbook (Second Edition). Boca Raton, BC: CRC Press, 2011. 474 p.

9. Rahman, M., & Al-Shaer, E.A. Formal Framework for Network Security Design Synthesis. Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems (2013): P. 560-570.
10. Whitman, M.E., & Mattord, H.J. Management of Information Security (Fourth Edition). Cencage Learning, 2014. 566 p.

References

1. Babenko A.A. The use of remote sensing technologies in the preparation of information security professionals // Proceedings of the Baltic State Fishery Academy: psychological and pedagogical sciences. 2011. No 4. P. 44-52/
2. Kolgatin A.G. Information security in open education systems // Educational Technology and Society. Vol.17 2014, No1. P. 417 – 425.
3. Koshkin E.N. SWOT-analysis of distance learning in Russia // Bulletin of the International Institute of Economics and Law. 2013. №4 (13). S.28-31.
4. Method of determining the information security threats in information systems. The draft guidance document // Official site FSTEC Russia. URL: http://fstec.ru/component/attachments/download/812 (reference date 10/03/2016).
5. Positive Research Report 2016 // Analysis company Positive Technologies 2016. URL: http://www.ptsecurity.ru/upload/ptru/analytics/Positive-Research-2016-rus.pdf (9/29/2016 treatment date).
6. Report McAfee Labs threats for February 2015 [Electronic resource] // Company McAfee Labs. URL: http://www.mcafee.com/ru/resources/reports/rp-quarterly-threat-q4-2014.pdf?cid=BHP035 (reference date 10/03/2016).
7. Callegari C., Vaton S., Pagano M. A. New statistical approach to network anomaly detection .Proc. of Performance Evaluation of Computer and Telecommunication Systems (SPECTS). No. 8 (2008); P.441-447.
8. Landoll, D.J. The security risk assessment handbook (Second Edition). Boca Raton, BC: CRC Press, 2011.474 p.
9. Rahman, M., & Al-Shaer, E.A. Formal Framework for Network Security Design Synthesis. Proceedings of the 2013 IEEE 33rd International Conference on Distributed Computing Systems (2013): P. 560-570.
10. Whitman, M.E., & Mattord, H.J. Management of Information Security (Fourth Edition). Cencage Learning, 2014. 566 p.

Оладько Владлена Сергеевна, кандидат технических наук, преподаватель
Бабенко Алексей Александрович, доцент, кандидат педагогических наук, доцент кафедры Информационной безопасности
Алексина Анастасия Александровна, студент

Oladko Vladlena Sergeevna, Lecture, Candidate of Engineering Sciences
Babenko Aleksey Alexandrovich, PhD in Pedagogics,
Associate Professor, Department of Information Security
Aleksina Anastasiya Aleksandrovna, student