Владлена С. Оладько
Финансовый университет при Правительстве Российской Федерации,
Ленинградский просп., 49, г. Москва, 125993 (ГСП-3), Россия
e-mail: oladko.vs@yandex.ru, https://orcid.org/0000-0003-0500-8928

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

DOI: http://dx.doi.org/10.26583/bit.2018.3.10

Аннотация. В статье проведен анализ области применения системы дистанционного обучения, рассмотрена архитектура и типовые подсистемы. Сделан вывод, что система дистанционного обучения учебного заведения представляет собой распределенную гетерогенную систему, имеющую веб-интерфейс и круглосуточный выход в глобальную сеть. Помимо общедоступной информации в ней обрабатываются различные виды сведений конфиденциального характера: персональные данные обучающихся и преподавателей, авторские учебные курсы и инновационные разработки, платежные данные, информация для служебного пользования. Эти сведения в процессе хранения, обработки и передачи подвергаются воздействию угроз случайного и умышленного характера, что приводит к нарушению составляющих информационной безопасности: доступности, целостности и конфиденциальности. При выборе мер защиты используются системный и экспертный подходы, позволяющие оценить эффективность меры для защиты от определенного перечня угроз. На практике в качестве индикаторов эффективности используются реестры рисков безопасности, тесты на проникновение в систему, показатели текущей безопасности системы и их отклонение от целевой защищенности или требований безопасности регуляторов. Для решения задачи оценки состояния текущей безопасности системы дистанционного обучения предложена функциональная модель исследования безопасности. В модели текущая безопасность рассматривается как функция от множества существующих мер защиты, результатов тестирования на проникновение и рисков ИБ от угроз различного характера. Для расчета рисков было предложено использовать трехфакторную модель, учитывающую частоту реализации угрозы, ущерб и коэффициент результативности контрмер по противодействию угрозе. Для качественной оценки функции безопасности системы предложено использовать балльно-рейтинговый подход и проводить сравнение текущей и целевой защищенности СДО. В заключении показана область применения модели и сделан вывод о необходимости ее автоматизации в виде программного комплекса.

Ключевые слова: защищенность, оценка рисков, тестирование на проникновение, угроза безопасности, ущерб, образовательное учреждение, веб-приложение.
Для цитирования: ОЛАДЬКО, Владлена С. ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ ДИСТАНЦИОННОГО ОБУЧЕНИЯ. Безопасность информационных технологий, [S.l.], n. 3, p. 101-111, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1144>. Дата доступа: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.10.

Vladlena S. Oladko
Financial University under the Government of the Russian Federation,
Leningradsky prosp., 49, Moscow, 125993 (GSP-3), Russian Federation
e-mail: oladko.vs@yandex.ru, https://orcid.org/0000-0003-0500-8928

Safety assessment functional model of distance learning system

DOI: http://dx.doi.org/10.26583/bit.2018.3.10

Abstract. The article analyzes the scope of the distance learning system and considers architecture and typical subsystems. Conclude that educational institution distance learning system is a distributed heterogeneous system with a web interface and round-the-clock access to the global network. The distance learning system processes, in addition to publicly available information, various types of confidential data, for example, personal data, electronic payments, author's training courses. Intentional and unintentional threats affect this information during storage, processing and transmission, which leads

to violation of the information security components: accessibility, integrity and confidentiality. Therefore, it is necessary to apply protection measures to counter threats. Security specialists use systematic and expert approaches to evaluate the measures effectiveness. The measures effectiveness indicators are safety risk registers, penetration tests, indicators of the system current security and their deviation from targeted security or regulatory safety requirements. The purpose of the work is the development of an approach to assessing the distance learning system current safety state. To achieve the goal, the author proposes a functional model for the safety investigation. The model describes the current system security as a function of the many implemented protection measures, the results of penetration testing and security risks. To calculate the risks, the author proposed to use a three-factor model that takes into account the threat frequency, damage and the protection measures effectiveness factor to counteract the threat. A qualitative scale evaluates the value of the resulting safety function. The value of the function is calculated using the ball-rating scale and the normalized value of the safety risk for each distance learning functional subsystem. The results of the work are a list of security threats for four distance learning functional subsystems, a functional safety assessment model in the IDEF0 notation and a mathematical description of the safety function. In conclusion, the author describes the scope of the model possible application and the relevance of automation in the form of a software.

Keywords: security, risk assessment, security threat, pen test, damage, educational institution, web application.

For citation: OLADKO, Vladlena S. Safety assessment functional model of distance learning system. IT Security (Russia), [S.l.], n. 3, p. 101-111, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1144>. Date accessed: 28 aug. 2018. doi:http://dx.doi.org/10.26583/bit.2018.3.10.

Введение

Становление цифровой экономики в Российской Федерации охватывает все сферы деятельности, в том числе и сферу образования, обеспечивая цифровую компетентность населению и предоставляя учащимся широкий спектр цифровых образовательных услуг, в том числе интерактивное взаимодействие с преподавателем, возможность дистанционного обучения в любое время суток, удаленный доступ к учебно-методическим материалам и фондам оценочных средств. Сегодня системы дистанционного обучения (СДО) позволяют наиболее адекватно и гибко реагировать на потребности общества и обеспечивать реализацию конституционного права на образование каждого гражданина. Во время функционирования любая СДО использует информационно - коммуникационные технологии и сети передачи данных для осуществления информационного взаимодействия между участниками образовательного процесса, хранения и обработки информации. Анализ источников [1,2] показывает, что СДО строится на базе информационной системы (ИС) учебного заведения и представляет собой распределенное, гетерогенное приложение с базой данных и веб-интерфейсами. Подобная архитектура и принцип функционирования порождает ряд проблем, связанных с безопасностью информации и сервисов СДО, а также качеством предоставляемых потребителям услуг. Данный вывод подтверждается данными статистики, представленными в отчете компании Positive Technologies в 2018 году [3, с.13-14], которые показывают, что 26 % всех атак на корпоративные ресурсы идут через веб-приложения и веб-интерфейсы, что в первую очередь связано с высоким процентом критически опасных уязвимостей веб-инфраструктуры и действием вредоносного программного обеспечения (ПО). Нарушение безопасности СДО в результате деструктивных информационных воздействий приводит и к нарушению информационной безопасности (ИБ) в сегменте и/или всей ИС учебного заведения. Поэтому для предотвращения различных негативных сценариев актуально решение задач, связанных с периодическим контролем над состоянием безопасности СДО, выявлением потенциальных рисков и своевременным принятием мер защиты, направленных на предотвращение угроз и минимизацию ущерба последствий.

Основные теоретические и практические аспекты проблем разработки, внедрения, эксплуатации и обеспечения безопасности СДО нашли свое отражение в работах

российских ученых: Тарасенко С.С., Устюговой В. Н., Валитова Р. А., Кузнецовой И.А., Полякова В. В., Воронова Р. В., Щеголевой Л. В., Булдаковой Т.И., Заводчиковой Н.И., Плясуновой У.В., Суворовой М.А. Проблемы управления рисками в образовании, вопросы исследования методов прогнозирования угроз для развития отечественных вузов и влияние на них угроз ИБ предпринимались В.Ю. Кричевским, Н.Ф. Родионовой, А.П. Тряпицыной, М.И. Шубинским, Богатыревой Ю.И., Жарниковой Ю.С., Куприяновским В.П., Добрыниным А.П. Анализ результатов исследований в научно-практических работах, представленных выше авторов, показал, что актуальными являются направления:

- решение задач эффективной интеграции образования, СДО и информационной инфраструктуры учебного заведения [4 – 7, 10];
- выявление и устранение технических проблем, связанных с разработкой и эксплуатацией СДО [5,8];
- оценка качества и технологии тестирования СДО [2, 9, 10];
- анализ угроз, рисков ИБ образовательного учреждения [11,12];
- разработка алгоритмов и механизмов защиты СДО [2, 9,13].

Объектом исследования в данной работе является модель СДО учебного заведения, предметом - состояние безопасности СДО. Цель исследования заключается в разработке и формализованном описании функциональной модели оценки уровня безопасности СДО. В качестве основных методов исследования при выполнении работы были использованы: метод описания, системного анализа, аналогии и обобщения.

Структура и активы системы дистанционного обучения

В соответствии с Федеральным законом об образовании от 29.12.2012 № 273-ФЗ [14] дистанционное обучение – важная часть гармонизации образовательного пространства, позволяющая обеспечить единый уровень учебных курсов и предоставить равный доступ к образованию для всех желающих с учетом разнообразия образовательных потребностей и индивидуальных возможностей. Поэтому на сегодняшний день практически все учебные заведения должны в состав информационной инфраструктуры включать СДО, решающие задачи [7, 15]:

- изучения нового и закрепления изученного материала посредством различных форм дидактических материалов (лекций, тестов, семинаров, интерактивных заданий, игр, форумов);
- актуализации и проверки знаний, обучающихся через Интернет, в локальных и корпоративных сетях;
- предоставления цифровых образовательных услуг в любом месте и в любое время;
- организации учебного процесса с различной степенью соответствия классической модели университетского образования;
- создания модели распределенной образовательной сети.

Анализ литературных источников [5, 7, 8, 15, 16] показывает, что на российском рынке существуют множество СДО, включая готовые программные продукты (например, «Прометей». «СТ Курс», Moodle, «Интразнание», «Батисфера», «Доцент», eLearning Server, WebCT Campus Edition, Sokai и др.) и собственные разработки учебного заведения (например, ПТК «Умник» в Волгоградском государственном университете, ИОП Финансового университета или СДО ОАО «РЖД»). СДО строится посредством:

- телекоммуникационной среды передачи информации (электронная почта, телерадиовещание, мультимедийные фото-видеоконференции, телефония, информационные коммуникационные сети), которые по технологии организации образования могут разделяться на 3 типа: синхронные, асинхронные, комбинированные;
- методов, зависимых от технической среды обмена информацией.

Таким образом, СДО представляет 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. Функционально включает элементы [7, 8]:

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

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

3) ядро системы (сервер СДО), обеспечивающее:

- регистрацию и управление учетными записями пользователей СДО;
- разграничение прав доступа к функциям и наполнению СДО;
- администрирование и защиту СДО;
- учет обучаемых, отслеживание результатов обучения и тестирования;
- создание и импорт учебных материалов;
- управление каталогами курсов;
- регистрацию информации о событиях в СДО;
- взаимодействие с другими компонентами внутренней информационной инфраструктуры учебного заведения.

Цель СДО обеспечить оптимальное взаимодействие субъектов учебного процесса за счет использования ресурсов и инструментов, заложенных в платформу [16, с. 38]. Основными субъектами взаимодействия являются внутренние (преподаватели, методисты, администраторы учебных курсов) и внешние пользователи (студенты и потенциальные обучающиеся), квалификация и мотивы которых будут оказывать влияние на состояние безопасности СДО, а следовательно, доступность и качество образовательного процесса.

Исходя из структуры, функций и подсистем в СДО можно выделить информационные активы: персональные данные пользователей (преподавателей и обучающихся); аутентификационные и идентификационные данные пользователей; 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 ценность, уровень доступа, что следует учитывать при анализе состояния информационной безопасности, составлении частной модели актуальных для СДО угроз и оценке рисков.

Киберугрозы в системах дистанционного обучения

Данные Positive Technologies, приведенные в отчете [3], показывают, что для сферы образования целевыми объектами киберугроз являются информационная инфраструктура, веб-приложения и пользователи. Воздействия реализуются посредством вредоносного ПО (28 %), компрометации учетных данных (24 %), социальной инженерии (16 %), эксплуатации уязвимостей в программном обеспечении (15 %) и веб-инфраструктуре (14 %). По характеру воздействия могут быть случайными и умышленными, согласно [12, с. 145] действия нарушителей могут быть индивидуальными и коллективными, обмен информацией и координация действий при целевых атаках возможна посредством социальных сетей, мессенджеров, электронной почты.

Согласно проекту методического документа ФСТЭК России по определению угроз безопасности в ИС [17] процесс определения киберугроз должен охватывать объекты защиты и сегменты в логических и физических границах системы. Поэтому при составлении модели угроз СДО предлагается выделить 4 основных структурных элемента

СДО, относительно которых будут рассматриваться потенциальные киберугрозы (см. табл. 1).

Таблица 1. Потенциальные киберугрозы СДО

	Элемент СДО	Угроза	Последствия
1	Веб-интерфейс СДО (доступ к сайту СДО, обмен сообщениями и информацией, получение доступа к учебным курсам и материалам)	1) SQL-инъекции и PHP-инъекции 2) XSS-атаки 3) подделка межсайтовых запросов – CSRF 4) атаки на браузер клиента 5) удаленное выполнение кода и отказ в обслуживании сервисов web-приложений 6) спам рассылки 7) фишинг	Нарушение конфиденциальности, целостности и доступности информации и сервисов веб-приложения СДО, финансовые и репутационные потери, проникновение на сервер СДО
2	Сервер СДО (подсистемы: управление учебными курсами; тестирование, календарный план, администрирование)	1) перебор паролей и атаки на систему аутентификации пользователей 2) вызов исключительных ситуаций 3) повышение привилегий пользователей 4) ошибки администрирования 5) сканирование портов 6) DDos и Dos-атаки 7) сбои и отказы поддерживающей инфраструктуры	Нарушение конфиденциальности, целостности и доступности информации, проникновение в ИС, прерывание бизнес-процессов
3	БД СДО (учебные курсы, списки групп, персональные данные, библиотеки, оценочные ведомости)	1) SQL-инъекции 2) случайное или намеренное удаление/модификация данных в БД и журналах транзакций 3) кража персональных данных 4) НСД к БД и журналам транзакций	Отказ от обязательств и совершенных действий, нарушение авторского права, нарушение целостности и конфиденциальности
4	Подсистема платежей и покупки курсов	1) НСД к платёжным данным пользователей 2) мошенничество 3) кража финансовых средств	Финансовые и репутационные потери

Идентифицированные киберугрозы СДО подлежат исследованию на предмет актуальности и необходимости применения защитных мер, направленных на блокирование и снижение тяжести последствий. Для этого исследуются такие характеристики угроз, как вероятность реализации и потенциальный ущерб [18]. Оценка может производиться на основании статистической информации [19], экспертной оценки, результатов проведения тестов на проникновение и моделирование угроз [20].

Разработка функциональной модели исследования безопасности системы дистанционного обучения

Согласно работам [18, 21 - 23], целевым назначением процедур контроля над состоянием ИБ системы является разработка частных моделей угроз, проверка существующих уязвимостей и состояния защищенности информации и сервисов от внутренних и внешних угроз, а также программного и аппаратного обеспечения, от которого зависит бесперебойная эксплуатация системы. Наиболее распространенными процедурами являются:

1) активный аудит, основанный на применении инструментальных средств поиска уязвимостей, и проведение тестов на проникновение в систему (pen test);
2) мониторинг конфигураций системы и сравнение с «эталонным образом» системы;

3) аттестация ИС и проверка соответствия системы требованиям безопасности, содержащимся в отраслевых стандартах, нормативно-методических документах регуляторов в области ИБ, политике безопасности;
4) мониторинг и анализ событий безопасности;
5) оценка рисков и уровня защищенности системы.

При проведении оценки безопасности СДО предлагается использовать комбинированный теоретико-практический подход, включающий четыре этапа работ (см. табл. 2).

Таблица 2. Этапы исследования безопасности СДО

№	Название этапа	Описание
1	Планирование	1) Определение целей и средств проведения оценки безопасности. 2) Формирование задания и определение критериев для оценки безопасности
2	Сбор данных, проведение проверки	1) Анализ документации по вопросам ИБ, изучение подсистем и ресурсов, анализ организационных мер и инфраструктуры ИБ. 2) Инструментальная проверка защищенности, моделирование атак злоумышленника.
3	Анализ и обработка результатов	1) Обобщение результатов, анализ угроз и оценка рисков. 2) Оценка возможного ущерба. 3) Формирование отчета по результатам исследования.
4	Повышение эффективности ИБ	1) Разработка мер по устранению недостатков или усовершенствованию ИБ 2) Составление план-графика проведения работ. Проведение мероприятий. 3) Анализ итогов и планирование графика проведения следующего исследования.

Предлагаемый подход основан на оценке общего уровня защищенности СДО и проведении тестов на проникновение, что позволит сделать упор в сторону практической безопасности. Описание «черного ящика» процесса проведения оценки безопасности СДО, в виде контекстной функциональной диаграммы в нотации IDEF0, представлено на рис. 1.

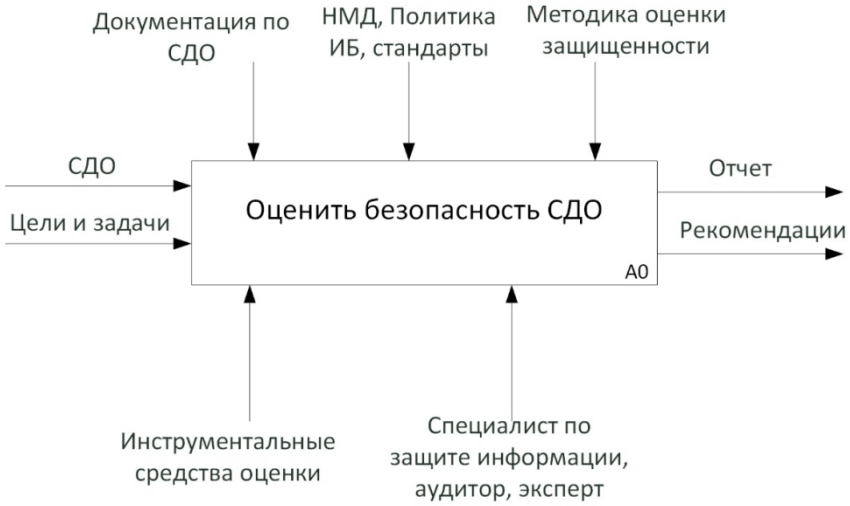

Рис. 1. Контекстная диаграмма процесса оценки безопасности СДО
(Fig. 1. Safety assessment context diagram of the distance learning system)

Процесс, с учетом содержания этапов табл. 2, декомпозируется на несколько связанных между собой подзадач, представленных на рис. 2.

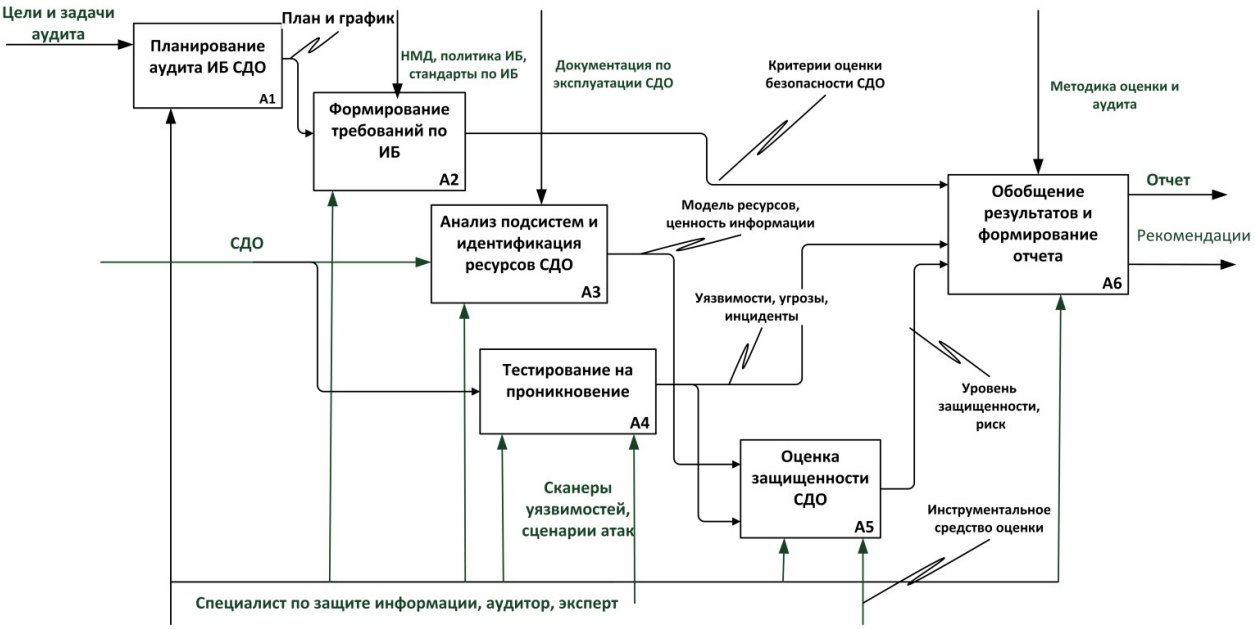

Рис.2. Декомпозиция процесса оценки безопасности СДО
(Fig. 2. Decomposition of the safety assessment of the distance learning system)

Безопасность СДО можно рассматривать как функцию $SL = f(SM, R, NPT) \mid SL \in \{критичный, низкий, средний, высокий\}$, где SM – множество, привлекаемых на обеспечение безопасности СДО ресурсов и средств защиты, R – суммарный уровень риска от угроз, NPT – доля успешно проведенных тестов на проникновение, которые могут привести к нарушению безопасности системы и/или ее отказу. При решении задач планирования и формирования требований необходимо установить допустимое значение приемлемого уровня защищенности, а также определить набор организационных и технических мер защиты, существующих в СДО и ИС учебного заведения.

Сбор данных о СДО позволяет идентифицировать ресурсы и отнести их к одной из четырех подсистем $DLS = \{WI, SERV, DB, PAYS\}$, где WI – пользовательская подсистема СДО, включая веб-интерфейс и удаленные сервисы, $SERV$ – сервер СДО, DB – база данных учебных курсов и методических материалов, $PAYS$ – система электронных платежей и покупки курсов.

Для получения значения суммарного риска R (формула 1) необходимо идентифицировать угрозы для каждой подсистемы и ресурсов СДО, определить количественные характеристики частоты реализации и потенциального ущерба, задать значение коэффициента результативности средств защиты в каждой подсистеме.

$$R_i = \sum_j R(TR_{ij}) = \sum_j p_{ij} h_{ij} QSM_i, \quad (1)$$

где $i = WI, SERV, DB, PAYS$– подсистема СДО, j-номер угрозы в каждой i-й подсистеме, u – потенциальный ущерб от угрозы, h – частота реализации угрозы, спрогнозированная в результате проведения тестирования на проникновение, $QSM_i \in [0;1]$ – значение коэффициента результативности средств защиты в каждой подсистеме. Для перехода между численной оценкой риска безопасности каждой подсистемы СДО и показателем безопасности СДО предлагается ввести нормированный коэффициент риска по каждой подсистеме KR_i^{norm}, указывающий на соотношение величины риска от подсистемы СДО угроз и стоимости ресурсов и информации в данной подсистеме СДО (см. формулу 2).

$$KR^{norm} = \sum_i KR_i^{norm} \Big| i = WI, SERV, DB, PAYS, \quad KR_i^{norm} = \begin{cases} 1, если & \frac{R_i}{C_i} < 1 \\ 0.5, если & \frac{R_i}{C_i} = 1, \\ 0, если & \frac{R_i}{C_i} > 1 \end{cases} \qquad (2)$$

где C_i- суммарная стоимость активов в каждой подсистеме СДО, оценённая на этапе сбора данных, анализа подсистем и идентификации ресурсов. Для получения значения безопасности СДО предлагается использовать бальную - рейтинговую шкалу, описание значений которой представлено в табл. 3.

Таблица 3. Возможные значения функции безопасности СДО

Значение функции безопасности	Описание
$SL = критичная \mid KR^{norm} = 0 \wedge NPT > 1$	В СДО отсутствуют меры защиты, высокая вероятность реализации угроз и нанесения ущерба. При проведении тестов на проникновение больше 50 % успешно проходит. Необходимо срочно снизить риски за счет создания и внедрения системы защиты СДО
$SL = низкая \mid KR^{norm} \in (0;2) \wedge NPT > 1$	В СДО меры защиты представлены в минимальном количестве и обладают низкой эффективностью. При проведении тестов больше 50 % успешно проходит. Необходимо принять меры по снижению риска. Переконфигурировать СЗИ СДО и внедрить дополнительные средства защиты, уменьшающие вероятность реализации угрозы или ее ущерб
$SL = средняя \Big\vert KR^{norm} \in [2;4) \wedge NRT \le 1$	Часть рисков ИБ в СДО не являются допустимыми, необходимо принять меры к их снижению, например, за счет использования дополнительных мер защиты, страхования риска или отказа от использования подверженного угрозе ресурса СДО. При проведении теста на проникновения может наблюдаться успех в менее 50 % случаев.
$SL = высокая \Big\vert KR^{norm} = 4 \wedge NRT = 0$	Существующие риски ИБ являются допустимыми и могут быть приняты.

Если текущее значение функции безопасности не соответствует целевому, то это указывает на необходимость принятия мер по управлению рисками ИБ СДО учебного заведения и проведение повторного исследования после внесения изменений.

Заключение

Разработана и математически описана функциональная модель исследования безопасности СДО учебного заведения, которая основана на объединении нескольких существующих подходов к оценке защищенности. В модели безопасность СДО рассматривается как функция рисков ИБ от угроз различного характера. Для расчета рисков было предложено использовать трехфакторную модель, учитывающую частоту реализации угрозы, ущерб и коэффициент результативности контрмер по противодействию угрозе. Для оценки качественного значения функции безопасности

предлагается использовать балльно-рейтинговый подход и проводить сравнение текущей и целевой защищенности СДО.

Результаты исследования безопасности СДО являются маркером при оценке эффективности существующей системы защиты информации учебного заведения и принятие решений о необходимости ее реконфигурации, если в отчете делается вывод о низком уровне защищенности системы и необходимости его повышения. В дальнейшем с целью обеспечения удобства работы пользователя и более наглядного представления результатов использования предложенной модели оценки безопасности СДО, нужно разработать программный комплекс, автоматизирующий ее. Программный комплекс должен иметь графический пользовательский интерфейс для удобного ввода данных и представления результатов.

СПИСОК ЛИТЕРАТУРЫ:

1. Кошкина Е.Н. SWOT-анализ дистанционного обучения в России//Вестник Международного института экономики и права. 2013. № 4 (13). С.28 - 31.
2. Колгатин А.Г. Информационная безопасность в системах открытого образования//Образовательные технологии и общество. 2014. Т.17, № 1. С. 417 – 425.
3. Positive Research 2018//Аналитика компании Positive Technologies 2018. [Электронный ресурс] URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf.
4. Зуева В. Что такое дистанционная система обучения//Интернет-образование. 2015. № 13 [Электронный ресурс] URL: http://fb.ru/article/184124/chto-takoe-distantsionnaya-sistema-obucheniya
5. Тарасенко О.С. Опыт внедрения дистанционных технологий обучения в ТТИ ЮФУ//Известия Южного федерального университета. Технические науки. 2013. № 10. С. 141-147.
6. Маликов А.В., Целиковский А.С. Модель системы дистанционного образования, основанная на онтологии предметных областей курсов обучения//Образовательные технологии и общество. 2011. Т.14, № 3. С.387 - 394.
7. Заводчикова Н.И., Плясунова У.В., Суворова М.А. Использование системы дистанционного обучения Moodle для организации самостоятельной работы студентов дневной формы обучения// Вестник Костромского государственного университета. Серия: Педагогика. Психология. Социокинетика. 2016. С.170 – 174. URL: https://cyberleninka.ru/article/v/ispolzovanie-sistemy-distantsionnogo-obucheniya-moodle-dlya-organizatsii-samostoyatelnoy-raboty-studentov-dnevnoy-formy-obucheniya
8. Валитов Р.А., Устюгова В.Н. Технические вопросы и проблемы, возникающие при создании и эксплуатации системы дистанционного образования на базе Moodle//Образовательные технологии и общество. 2011. № 4. Т. 11. С. 342 - 346.
9. Усков А. В. Иванников А. Д. Усков В. Л. Технологии обеспечения информационной безопасности корпоративных образовательных сетей//Образовательные технологии и общество. 2008. Т.11, № 1. С. 472 – 479.
10. Куприяновский В.П., Сухомлин В.А., Добрынин А.П. Навыки в цифровой экономике и вызовы в системе образования//International Journal of Open Information Technologies. 2017. Vol. 5. N. 1. Pp. 19 – 25.
11. Жарникова Ю. С. Угрозы информационной безопасности образовательного учреждения // Молодой ученый. 2017. № 11(2). С. 60 - 63. URL https://moluch.ru/archive/145/40613/
12. Брумштейн Ю.М., Бондарев А.А. Системный анализ вопросов информационной безопасности вузовских сайтов// Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2014. № 2. С. 138 – 147. URL: https://cyberleninka.ru/article/v/sistemnyy-analiz-voprosov-informatsionnoy-bezopasnosti-vuzovskih-saytov
13. Богатырева Ю.И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного учреждения// Известия Тульского государственного университета. Гуманитарные науки. 2013. № 3 - 2. С. 14 - 26. URL: https://cyberleninka.ru/article/v/model-obespecheniya-informatsionnoy-bezopasnosti-shkolnikov-pri-sozdanii-infobezopasnoy-sredy-obrazovatelnogo-uchrezhdeniya
14. Федеральный закон "Об образовании в Российской Федерации" от 29.12.2012 N 273-ФЗ//КонсультантПлюс. [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_140174/
15. Калашникова Т.Г. Использование СДО «Прометей» для организации самостоятельной работы студентов очной формы обучения// Известия Южного федерального университета. Технические науки. 2005. №9. Т. 53 [Электронный ресурс] URL: https://cyberleninka.ru/article/v/ispolzovanie-sdo-prometey-dlya-organizatsii-samostoyatelnoy-raboty-studentov-ochnoy-formy-obucheniya
16. Мухаметзянова Ф.Ш., Камалеева А.Р., Грузкова С.Ю., Хадиуллина Р.Р. Организация взаимодействия субъектов образовательного процесса при использовании платформ дистанционного обучения//Открытое образование. 2016. Т. 20. №3. С. 36 – 42. URL:

https://cyberleninka.ru/article/v/organizatsiya-vzaimodeystviya-subektov-obrazovatelnogo-protsessa-pri-ispolzovanii-platform-distantsionnogo-obucheniya.
17. Методика определения угроз безопасности информации в информационных системах. Проект методического документа//Официальный сайт ФСТЭК России. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/812
18. Царегородцев А.В., Макаренко Е.В. Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации//Национальные интересы: приоритеты и безопасность. 2014. № 44 (28). С. 30 - 41. URL: http://cyberleninka.ru/article/n/metodika-kolichestvennoy-otsenki-riska-v-informatsionnoy-bezopasnosti-oblachnoy-infrastruktury-organizatsii-1
19. Зефиров С.Л., Щербакова А.Ю. Оценка инцидентов информационной безопасности//Доклады ТУСУРа. 2014. № 2(32). С. 77 - 81. URL: http://cyberleninka.ru/article/n/otsenka-intsidentov-informatsionnoy-bezopasnosti
20. Omelchenko Tatiana, Umnitsyn Mikhail, Nikishova Arina, Sadovnikova Natalia and Maksimova Elena. Approaches to information systems modeling for the study of the reliability and safety of their functioning / Proceedings of the 5th International Conference on System Modeling and Advancement in Research Trends, SMART 2017. – pp. 128-133.
21. Абрамов А.А., Горбатов В.С., Гришина М.Н. Угрозы безопасности информации при эксплуатации веб-портала на платформе Open Journal System // Безопасность информационных технологий Безопасность информационных технологий, [S.l.], n. 2, p. 86-105, 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1113. doi:http://dx.doi.org/10.26583/bit.2018.2.08.
22. Оладько В.С. Программный комплекс для оценки защищенности систем электронной коммерции// Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2015. № 4. С. 46-53. DOI: 10.17223/19988605/33/6.
23. Omelchenko Tatiana, Umnitsyn Mikhail, Nikishova Arina, Sadovnikova Natalia. Model of enterprise's information security management// Information Technologies in Science, Management, Social Sphere and Medicine' (ITSMSSM 2016): proceedings of III International Scientific Conference (Tomsk, Russian Federation, 2017) / Tomsk Polytechnic University. – [Published by Atlantis Press], 2017.

REFERENCES:

[1] Koshkina Ye.N. SWOT-analysis of distance learning in Russia. Vestnik Mezhdunarodnogo instituta ekonomiki i prava. 2013. №4 (13). pp.28-31. (in Russian).
[2] Kolgatin A.G. Information security in open education systems. Obrazovatel'nyye tekhnologii i obshchestvo. 2014. T.17, №1. pp. 417 – 425. (in Russian).
[3] Positive Research 2018. Analytics of the company Positive Technologies 2018. [Electronic resource] URL: https://www.ptsecurity.com/upload/corporate/ru-en/analytics/Positive-Research-2018-rus.pdf. (in Russian).
[4] Zuyeva V. What is the distance learning system. Internet-obrazovaniye. 2015. №13. [Electronic resource] URL: http://fb.ru/article/184124/chto-takoe-distantsionnaya-sistema-obucheniya. (in Russian).
[5] Tarasenko O.S. Experience in implementing distance learning technologies in TIT SfedU. Izvestiya Yuzhnogo Federal'nogo universiteta. Tekhnicheskiye nauki. 2013. №10. pp. 141-147. (in Russian).
[6] Malikov A.V., Tselikovskiy A.S. Model of distance learning system based on ontology of subject areas of training courses. Obrazovatel'nyye tekhnologii i obshchestvo. 2011. T.14, №3. pp. 387 -394. (in Russian).
[7] Zavodchikova N.I., Plyasunova U.V., Suvorova M.A. Using the system of distance learning Moodle for organizing independent work of full-time students. Vestnik Kostromskogo gosudarstvennogo universiteta. Seriya: Pedagogika. Psikhologiya. Sotsiokinetika.2016. pp.170 – 174. URL: https://cyberleninka.ru/article/v/ispolzovanie-sistemy-distantsionnogo-oucheniya-moodle-dlya-organizatsii-samostoyatelnoy-raboty-studentov-dnevnoy-formy-obucheniya. (in Russian).
[8] Valitov R.A., Ustyugova V.N. Technical issues and problems arising in the creation and operation of the system of distance education based on Moodle. Obrazovatel'nyye tekhnologii i obshchestvo.2011.№4.T.11.pp .342-346. (in Russian).
[9] Uskov A. V. Ivannikov A. D. Uskov V. L. Technologies for Information Security of Corporate Educational Networks. Obrazovatel'nyye tekhnologii i obshchestvo. 2008. T.11, №1. pp. 472 – 479. (in Russian).
[10] Kupriyanovskiy V.P., Sukhomlin V.A., Dobrynin A.P. Skills in the digital economy and challenges in the education system. International Journal of Open Information Technologies. 2017. Vol. 5. N. 1. pp. 19 – 25. (in Russian).
[11] Zharnikova Y. S. Threats to information security of an educational institution. Molodoy uchenyy. 2017. №11.2. P 60-63. URL. (in Russian).
[12] Brumshteyn Y.M., Bondarev A.A. System analysis of information security questions of university sites. Bulletin of Astrakhan State Technical University. Series: Management, Computer Science and Informatics. №2. pp. 138 - 147. URL: https://cyberleninka.ru/article/v/sistemnyy-analiz-voprosov-informatsionnoy-bezopasnosti-vuzovskih-saytov. (in Russian).
[13] Bogatyreva Y.I. A model for ensuring information security of schoolchildren when creating an infosecurity environment for an educational institution. Izvestiya Tul'skogo gosudarstvennogo universiteta. Gumanitarnyye

nauki. 2013. № 3-2. pp. 14-26. URL: https://cyberleninka.ru/article/v/model-obespecheniya-informatsionnoy-bezopasnosti-shkolnikov-pri-sozdanii-infobezopasnoy-sredy-obrazovatelnogo-uchrezhdeniya. (in Russian).

[14] Federal'nyy zakon "Ob obrazovanii v Rossiyskoy Federatsii" ot 29.12.2012 N 273-FZ. Konsul'tantPlyus. [Electronic resource] URL: http://www.consultant.ru/document/cons_doc_LAW_140174/.(in Russian).

[15] Kalashnikova T.G. The use of the SDO "Prometheus" for the organization of independent work of full-time students. Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskiye nauki.2005.№9. T.53 [Electronic resource] URL: https://cyberleninka.ru/article/v/ispolzovanie-sdo-prometey-dlya-organizatsii-samostoyatelnoy-raboty-studentov-ochnoy-formy-obucheniya. (in Russian).

[16] Mukhametzyanova F.S., Kamaleyeva A.R., Gruzkova S.Y., Khadiullina R.R. Organization of the interaction of subjects of the educational process using the distance learning platforms. Open Education 2016. T. 20. № 3. pp. 36 - 42. URL: https://cyberleninka.ru/article/v/organizatsiya-vzaimodeystviya-subektov-obrazovatelnogo-protsessa-pri-ispolzovanii-platform-distantsionnogo-obucheniya. (in Russian).

[17] Methodology for determining threats to information security in information systems. Draft Methodical Document. Official site of FSTEC of Russia. [Electronic resource] URL: http://fstec.ru/component/attachments/download/812. (in Russian).

[18] Tsaregorodtsev A.V., Makarenko Y.V. Methodology of quantitative risk assessment in information security of the cloud infrastructure of the organization. National interests: priorities and security. 2014. No. 44 (28). pp. 30-41. URL: http://cyberleninka.ru/article/n/metodika-kolichestvennoy-otsenki-riska-v-informatsionnoy-bezopasnosti-oblachnoy-infrastruktury-organizatsii-1. (in Russian).

[19] Zefirov S.L., Shcherbakova A.Y. Information security incidents assessment. Proceedings of TUSUR University. 2014. No. 2 (32). pp. 77-81. URL: http://cyberleninka.ru/article/n/otsenka-intsidentov-informatsionnoy-bezopasnosti. (in Russian).

[20] Omelchenko Tatiana, Umnitsyn Mikhail, Nikishova Arina, Sadovnikova Natalia and Maksimova Elena. Approaches to information systems modeling for the study of the reliability and safety of their functioning. Proceedings of the 5th International Conference on System Modeling and Advancement in Research Trends, SMART 2017. – pp. 128-133.

[21] Abramov, Anton A.; Gorbatov, Victor S.; Grishina, Marina N.. Information security threats in web-portals on the open journal systems platform. IT Security (Russia), [S.l.], n. 2, p. 86-105, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1113>.doi:http://dx.doi.org/10.26583/bit.2018.2.08. (in Russian).

[22] Oladko Vladlena S. The program is assessing the level of security of e-commerce. Tomsk State University Journal of Control and Computer Science. 2015. № 4. C. 46-53. DOI: 10.17223/19988605/33/6. (in Russian).

[23] Omelchenko Tatiana, Umnitsyn Mikhail, Nikishova Arina, Sadovnikova Natalia. Model of enterprise's information security management. Information Technologies in Science, Management, Social Sphere and Medicine' (ITSMSSM 2016): proceedings of III International Scientific Conference (Tomsk, Russian Federation, 2017) / Tomsk Polytechnic University. – [Published by Atlantis Press], 2017.

Поступила в редакцию - 23 июля 2018 г. Окончательный вариант – 28 августа 2018 г.
Received – July 23, 2018. The final version – August 28, 2018.