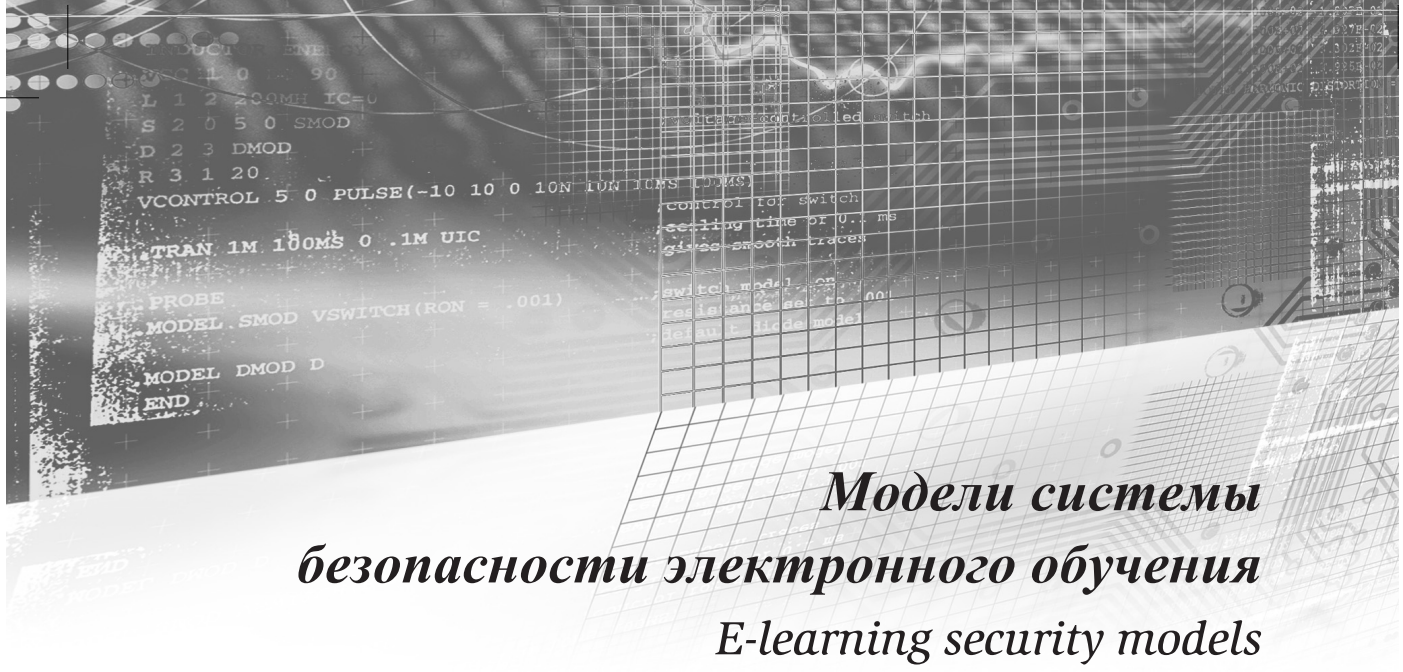

Модели системы безопасности электронного обучения

E-learning security models

Зуев В.И. (Vladimir I. Zuev)

The present article concerns methods and models that are useful when analyzing the risks and vulnerabilities of complex e-learning systems in a emergency management context. Definitions of vulnerability and emergency response capabilities, such as "VLE/PLE attack surface", are suggested.

Article provides insight into some of the issues related to analysis of risks and vulnerabilities of e-learning systems, but more research is needed to address this difficult and comprehensive task.

Характерной особенностью современного образовательного процесса является перенос методов и технологий электронного обучения (e-learning) в традиционные образовательные среды. Таким образом, происходит трансляция в традиционное образовательное пространство системных признаков электронного обучения, базирующегося на использовании новейших цифровых технологий и устройств. Технологическое усложнение образовательного процесса, переход к электронному обучению неизбежно влечет за собой рост уязвимости системы. Причем, на этом этапе происходит интерференция традиционных рисков системы образования (педагогических, психологических и пр.) с рисками, характерными, в первую очередь для ИТ-сферы. Для создания адекватной защиты системы электронного обучения необходимо попытаться построить, в первую очередь, модель электронного учебного заведения и выбрать метрики, определяющие параметры безопасности.

Определим некоторые специфические черты электронного обучения в среде Web 2.0. Это, прежде всего:

- активное участие обучающихся в создании и наполнении баз учебных материалов,
- возможность пирингового взаимодействия между обучающимися,
- объединение разнородных потоков учебной информации,
- сочетание формального и неформального обучения,
- использование социальных сервисов.

Цепочка потока знаний в процессе электронного обучения включает в себя компьютеры, как физические носители и хранилища информации, Интранет и Интернет, как среду передачи и, опять же, хранения информации. Кроме того, необходимо принимать во внимание архитектуру таких виртуальных образований, как информационно-образовательная среда

учебного заведения, персональная образовательная среда учащегося и персональная среда преподавателя.

Информационно-образовательная среда современного ВУЗа должна обеспечивать:

- адекватное наполнение учебного пространства мультимедийными ресурсами,
- актуализацию и верификацию последних,
- удобство работы с учебными объектами,
- гибкость учебной траектории студента,
- возможность адекватной оценки знаний учащегося,
- надежную обратную связь «преподаватель-учащийся»,
- защиту персональных данных студента, и т.д.

Все перечисленные выше элементы технологической цепочки являются потенциальными объектами взлома, атаки, последующей неавторизованной модификации и, в предельном случае, уничтожения. Кроме этого, администрация учебного заведения, реализующего дистанционные образовательные технологии, должна решать вопросы, связанные с аутентификацией студента, недобросовестным выполнением последним учебных заданий (плагиат), а также с защитой авторских прав на материалы профессорско-преподавательского состава, размещенные в Сети. При этом возникает необходимость защиты как целостности электронных ресурсов (учебных, информационных), так и обеспечения бесперебойного функционирования автоматизированных систем управления учебным процессом, контентом образовательного сайта и т.д.

Самые общие требования к системе безопасности электронного обучения подразумевают следующее:

- Защита должна быть, в первую очередь, ориентирована на отражение наиболее вероятных и разрушительных атак;
- Система защиты должна обеспечивать непрерывный контроль состояния электронного ВУЗа, выявляя малейшие несанкционированные изменения;
- Для адекватного и быстрого реагирования на угрозы система защиты должна быть максимально автоматизирована;
- Особую важность приобретает применение элементов деловой разведки (Business Intelligence) для анализа состояния безопасности во всем множестве электронных учебных заведений с целью выявления возможных зловредных трендов;
- Для оперативной оценки эффективности состояния системы защиты должны быть определены соответствующие количественные характеристики (метрики).

Традиционный подход к рассмотрению безопасности электронного обучения включает в себя следующие компоненты [1]:

- информационная безопасность электронного обучения,
- психологическая безопасность электронного обучения,
- дидактическая безопасность электронного обучения,
- физическая безопасность электронного обучения.

Между тем, возможно и интегральное рассмотрение этой проблемы, подразумевающее выделение наиболее общих, характерных элементов системы безопасности e-learning.

Как правило, все требования обеспечения безопасности электронного обучения сводятся к основным четырем, незначительно отличающимся от триады AIC информационной безопасности. Это:

- Обеспечение секретности (пользователь может получить доступ лишь к тем объектам, к которым ему этот доступ разрешен);
- Обеспечение целостности (только авторизованные пользователи могут осуществлять модификацию информации и программ);
- Обеспечение доступности (работоспособность приложений и программ резко снижается в результате атак);
- Обеспечение штатной работы приложения в соответствии с заложенным алгоритмом.

Можно перечислить следующие уязвимости системы e-learning, это:

- Уязвимость физической (hardware) инфраструктуры;
- Уязвимость программного обеспечения;
- Уязвимость человеческих ресурсов;
- Уязвимость баз данных;
- Уязвимость перед действием природных факторов.

При этом, безопасность информационной системы электронного обучения должна быть обеспечена на нескольких уровнях:

- Уровне сетевой инфраструктуры,
- Уровне операционной системы и базовых сервисов,
- Уровне приложений,
- Уровне баз данных.

Ниже перечислены следующие типичные угрозы нормальному функционированию системы электронного обучения:

- Неавторизованный доступ к цифровому контенту (неавторизованное копирование и модификация данных), включая физический доступ к серверам.
- Нарушение целостности и неадекватность учебных ресурсов (часто электронные учебные пособия, наряду с ресурсами Интернета, являются основными источниками учебной информации для студента)
- Нарушение безопасности процедур тестирования и электронных экзаменов (проблемы идентификации студентов, списывания, плагиата и адекватного функционирования системы оценивания знаний)
- Нарушение нормального функционирования служб и сервисов учебного заведения.
- Нарушение законодательства (в частности, законов, регулирующих авторские и иные права).

Рассматривая вопросы безопасности системы электронного обучения необходимо учитывать все риски и уязвимости такой структуры. При этом, характерной особенностью данной системы является дуализм «субъект/объект атаки». Один и тот же участник (или элемент) образовательного процесса может выступать и как источник, и как объект атаки.

В работе [2] сделана попытка представления этого дуализма с помощью модели «куба электронного обучения». По одной из осей модели отложены уровни взаимодействия (персональная образовательная среда студента или преподавателя, виртуальная образовательная среда учебного заведения, всемирная сеть); по другой – типы цифровых

ресурсов (программное обеспечение, информационные объекты, учебные объекты); по третьей – категории участников процесса (студенты, ППС, АУП).

На рис. 1 представлена атака на ППС на уровне виртуальной образовательной среды учебного заведения. Источником угрозы является программное обеспечение (это может быть его видоизменение, модификация, уничтожение и т.д.). На рис. 2 – обратная ситуация: атака на ПО на уровне виртуальной образовательной среды учебного заведения со стороны ППС.

Рассмотрим отдельно риски дидактической системы e-learning. Прежде всего, это риски, связанные с профессорско-преподавательским составом.

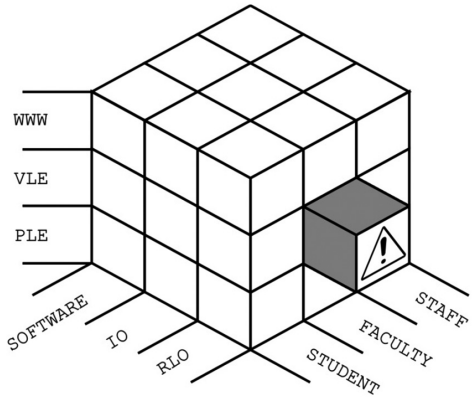

Рис. 1. *Атака на ППС на уровне виртуальной образовательной среды учебного заведения. Источник – ПО*

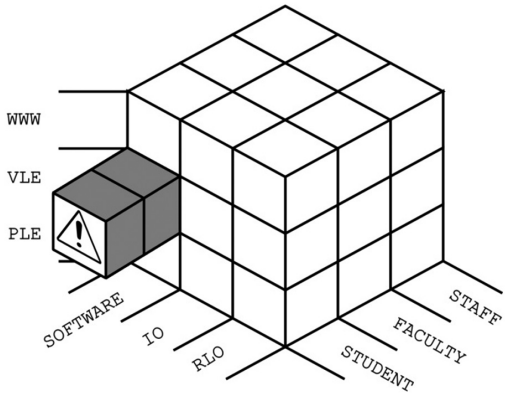

Рис. 2. *Атака на ПО на уровне виртуальной образовательной среды учебного заведения со стороны ППС*

Во-первых – это риски, связанные с компетентностью ППС. Можно выделить следующие уровни рисков:

- Дидактический риск (возникает, когда преподаватель не уделяет должного внимания обновлению учебного курса).
- Технологический риск (возникает вследствие неспособности преподавателя в полной мере использовать современные средства ИКТ).
- Научный риск связан с качеством учебного материала, предлагаемого преподавателем.
- Риск делегирования полномочий возникает, когда преподаватель полностью перекладывает на систему электронного управления учебным процессом (LMS) ответственность за процедуру аттестации студента.

Во-вторых, это риски связанные с организацией учебного процесса. Они возникают при неправильном планировании и недостаточном контроле учебного процесса, консультаций, аттестационных мероприятий. Источником этих рисков могут стать неадекватная задачам учебного процесса система информирования студентов, слабая кооперация между преподавателями, ведущими смежные дисциплины (повтор отдельных элементов дисциплин, несогласованность понятийного аппарата).

И, наконец, последняя группа рисков, связанных с ППС, – это риски, возникающие непосредственно в ходе учебного процесса в результате неадекватного поведения студентов, низкого уровня профессиональной ответственности преподавателя и нарушения последним трудовой дисциплины.

Едва ли не большее количество рисков связано со студентами.

Во-первых, это риск, связанный с неспособностью студента выдерживать заданный преподавателем и электронной системой темп обучения (зачастую он связан с низким уровнем подготовки студента).

Во-вторых, это риск, связанный с необходимостью постоянной мотивации студента.

В-третьих, это риск, связанный с неадекватной самооценкой и поведением студента.

В-четвертых, это риск, связанный с неспособностью студента наладить контакт с преподавателем

В-пятых, это технологический риск, который в этом случае связан с высокой компетенцией студента в области ИКТ, программного обеспечения и сервисов Web 2.0.

Кроме того, в деятельности любого учебного заведения возникают риски, связанные с административным персоналом, который в данном случае также может выступать и как объект, и как субъект атаки на систему электронного обучения.

Формализация оценок системы безопасности электронного учебного заведения и создание адекватной модели безопасности представляет собой, таким образом, довольно сложную задачу.

Полный анализ системы безопасности электронного учебного заведения включает в себя топологический анализ структуры e-learning, учет цикломатической сложности используемого программного обеспечения, психологических и педагогических составляющих учебного процесса.

Между тем, оказывается возможным предложить несколько более простых путей к решению этой проблемы.

Во всех случаях атаки на систему электронного обучения атакующий вступает в контакт с системой, используя каналы передачи информации, используя и имитируя методы работы системы, отправляя или получая из системы информацию. Аналогичные действия совершает злоумышленник и при атаке на чисто «информационные» объекты. Воспользуемся разработанной для этого случая методикой.

Вслед за работами [3,4] введем понятие «поверхности атаки на электронную образовательную среду».

Назовем «поверхностью атаки на ЭОС» – множество (геометрическое место) возможных уязвимых мест системы безопасности электронного образовательного учреждения. Это – каналы передачи информации, элементы системы LMS, базы данных, программное обеспечение, методики и процедуры электронного обучения, точки ввода и вывода информации из системы и т.д. Чем больше компонентов включает в себя электронная образовательная среда, тем больше число потенциально уязвимых мест и, соответственно, поверхность атаки.

Между тем, не все элементы системы электронного обучения являются частью «поверхности атаки», а те, что действительно являются источниками возможных уязвимостей,

вносят в нарушение безопасности системы неодинаковый вклад. Следовательно, необходимо определить критерии, по которым мы оцениваем эти уязвимости (вклад каждого из возможных элементов).

Элемент электронной образовательной среды (ресурс) становится частью «поверхности атаки», если злоумышленник может использовать его для нарушения нормальной работоспособности системы. Для оценки такого элемента логично на первом этапе ввести критерий на основе соотношения:

[затраты на восстановление системы / ущерб от действий злоумышленника].

Другим вариантом оценки может стать соотношение времени отказа системы и времени ее восстановления.

Таким образом, «поверхность атаки» является интегральной характеристикой уязвимости всей системы в целом. Она дает представление о том ущербе, который злоумышленник может нанести системе и одновременно о тех действиях, которые он должен предпринять для нанесения этого ущерба.

Вслед за работой [3] для определения «поверхности атаки» введем понятие «вектора атаки». Фактически «вектор атаки» представляет собой возможный вариант действий злоумышленника для нарушения нормальной работоспособности системы.

Множество «векторов атаки» определяется, таким образом, множеством угроз и рисков системы электронного обучения, упомянутых выше.

Адекватное оценивание всех уязвимостей, рисков и угроз системе электронного обучения позволит создать модель, на основе которой может быть разработана соответствующая стратегия защиты. Моделирование угроз при этом является неотъемлемой частью жизненного цикла разработки системы безопасности электронного обучения. Уделяя внимание проблеме на начальном этапе создания защищенной системы электронного обучения, мы сможем осуществить анализ планирования и архитектуры системы с целью обнаружения и устранения проблем защиты уже на уровне проектирования.

Литература

1. Weippl E.R. Security in E-Learning (Advances in Information Security Volume 16). – Springer Science+Business Media, Inc., 2005. – 193 p.
2. Зуев В.И. Безопасность электронного обучения // Сборник научных трудов «Совершенствование подготовки IT-специалистов по направлению «Прикладная информатика» для инновационной экономики»– М.: Московский государственный университет экономики, статистики и информатики, 2010. – С. 81-85.
3. Howard M. Fending off future attacks by reducing attack surface. http://msdn.microsoft.com/en-us/library/ms972812
4. Manadhata P.K., Wing J.M. An Attack Surface Metric // IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, Vol. 37, Issue 3, 2010.- P. 371 – 386

Vladimir I. Zuev
Institute for social sciences and humanities
vzuev@ksu.ru

Зуев В.И.
Институт социальных и гуманитарных знаний
vzuev@ksu.ru