**Тезисы доклада**

Начало формы

1. **НАЗВАНИЕ ДОКЛАДА:**

– Риски информационной образовательной среды

– Risk information educational environment

1. **АВТОРЫ:**

– Шубинский М.И.

– Shubinskiy M.

1. **ОРГАНИЗАЦИЯ (полное наименование, без аббревиатур):**

– Санкт-Петербургский национальный исследовательский университет информационных технологий механики и оптики (ИТМО)

– ITMO University

1. **ГОРОД:**

– Санкт-Петербург

– St.Petersburg

1. **ТЕЛЕФОН:** (812) 3476791
2. **ФАКС:** (812) 3476791
3. **E-MAIL:** **shubinskiy@gmail.com**
4. **АННОТАЦИЯ**:

– Сейчас один из самых важных вопросов стоящих сейчас перед ОУ с точки зрения информационных технологий – это вопрос информационной безопасности. В данной работе автором дается общий анализ рисков информационно-образовательной среды и предлагается критерии разбиения рисков на группы.

– Now one of the most important issues now facing the educational institution in terms of information technology - it is a question of information security. In this paper, the author gives an analysis of the risks of information-educational environment and proposes criteria for the partition of risk in the group.

1. **КЛЮЧЕВЫЕ СЛОВА**:

– риск, безопасность, образовательная среда

– risk, safety, learning environment

1. **ТЕКСТ ТЕЗИСОВ ДОКЛАДА:**

**Введение**

Скачкообразное насыщение компьютерами, случившееся в начале 2000-ых годов в России породило целый ряд насущных проблем, связанных с внедрением информационных технологий в образовательный процесс. В последние 10 лет одной из основных задач системы образования стало выстраивание информационной образовательной среды. Сейчас, когда уже можно говорить, о существующей информационной среде в образовательных учреждениях (ОУ), один из самых важных вопросов стоящих сейчас перед ОУ с точки зрения информационных технологий – это вопрос информационной безопасности, или говоря иначе – создание безопасной информационной среды ОУ.

В данной работе автором дается общий анализ рисков информационно-образовательной среды.

**I. Подход к обеспечению безопасности информационно-образовательной среды образовательного учреждения**

Опишем упрощенную модель информационной среды образовательного учреждения с точки зрения обеспечения ее безопасности. Наша модель будет основываться на теории рисков. В качестве определения риска выберем следующее:

Риск — это неопределённое событие или условие, которое в случае возникновения, приводит к обязательным неблагоприятным последствиям.

Из приведенного выше определения следует наличие у риска следующих обязательных характеристик

**Неопределённость**. Эта характеристика означает, что риск существует только тогда, когда различные варианты развития событий. Они могут осуществиться, а могут и нет.

**Ущерб**. Эта характеристика означает, что риск существует только тогда, когда исход может привести к ущербу или иному, но обязательно негативному последствию.

**Значимость**. Эта характеристика означает, что риск существует, когда предполагаемое событие имеет практическое значение и затрагивает интересы хотя бы одного субъекта.

Рассмотрим эти характеристики на примерах. В качестве первого примера выберем риск заражения сайта образовательного учреждения вирусом с дальнейшим уничтожением вирусом части материалов, вывешенных на сайте. У данного события присутствует характеристика – неопределенность. Сайт может быть заражен вирусом, а может быть и нет. В случае заражения образовательному учреждению будет нанесен и финансовый ущерб, который будет выражен в оплате работ по возвращению сайта в работоспособное состояние и репутационный ущерб, если потребуется значительное время на восстановление сайта. А это означает, что и вторая характеристика у данного риска присутствует. Субъектом, чьи интересы затрагивает предполагаемое событие (третья характеристика), в данном случае, является непосредственно образовательное учреждение. В качестве второго примера выберем следующее событие: окончание лицензии на антивирусное программное обеспечение (например, антивирус Касперского). После остановки работы антивирусного ПО, организация (субъект) понесет ущерб от заражения компьютеров вирусом. Но данный пример не является риском, поскольку не работает характеристика неопределенности. Лицензия действует четко обозначенный срок (обычно 1 или 2 года) и соответственно рассмотренное событие обязательно произойдет.

Второе ключевое понятие для модели безопасности информационно-образовательной среды – это понятие угрозы. Под угрозой будем понимать потенциально возможное событие, которое может привести к нанесению ущерба.

Риск – определяет степень опасности воздействия угрозы (или набора угроз) на систему (объект, ресурс или процесс).

Для каждой информационно-образовательной среды существуют риски, реализация которых приведет информационную среду в неработоспособное состояние или в состояние, в котором эффективность работы среды будет существенно снижена. Для каждого риска есть некоторый набор угроз (рисунок 1).

Часть из этих угроз являются актуальными. Актуальными угрозами считается те угрозы, которые имеют высокую степень опасности воздействия на систему.

Под безопасной информационно-образовательной средой мы будем понимать такую информационную среду, для которой определен набор актуальных угроз наступления рисков и для каждой из угроз выбран способ защиты, позволяющий

Рисунок 1

наиболее эффективно предотвратить угрозу или минимизировать возможные потери (рисунок 2).

Рисунок 2

На рисунке видно, что выбранная защита, частично нейтрализует угрозы, а частично минимизирует потери от реализованных рисков.

Таким образом, для получения конкретной модели безопасной информационно-образовательной среды необходимо описать возможные группы рисков данной среды, определить набор актуальных угроз, которые могут привести к реализации рисков и определить комплекс защитных мероприятий, позволяющих нейтрализовать угрозы или минимизировать их последствия. Необходимо отметить, что в комплекс мероприятий должны входить и технические и организационные и педагогические действия.

**II. Общее описание рисков информационной образовательной среды**

Рассмотрим риски информационной образовательной среды.

В данной работе предлагается следующий критерий разбиения рисков на группы. Риски группируются в соответствии с объектом (субъектом) образовательного процесса на который они воздействуют.

* Педагогические риски – отрицательные воздействия на учебный процесс.
* Психолого-медицинские риски – отрицательные воздействия на жизнь и здоровье учащихся и педагогов.
* Управленческие (или организационные) риски – отрицательное влияние на управленческие процессы.
* Финансовые риски – отрицательные воздействия на финансовое состояние учреждения (прямые финансовые потери).
* Политические риски - отрицательные воздействия на репутацию учреждения.

В группу педагогических рисков, включаются те риски, которые могут повлиять на учебный процесс. Здесь надо отметить риски, в результате реализации которых будет невозможно использовать компьютерное оборудования при ведении уроков. Стоит напомнить, что согласно новым ФГОС использование подобного оборудования является обязательным. Большие группы педагогических рисков связаны с влиянием на оценивание результатов учащихся и с непосредственным отрицательным влиянием на учащихся, что делает необходимым включение дополнительных тем и (или разделов) в учебный процесс и проведением дополнительных воспитательных мероприятий для детей, родителей и педагогического коллектива.

К группе психолого-медицинских рисков, прежде всего, относятся те риски, которые могут повлиять на здоровье, как учащихся, так и сотрудников ОУ.

В группу управленческих рисков, включим те риски, которые приведут к необходимости временной или постоянной перестройки организационной структуры образовательного учреждения. Ярким примером подобного риска может служить риск временной неработоспособности локальной сети учреждения при использовании школой электронного журнала.

В группу финансовых рисков, включим все те риски, которые связаны с понесением учреждением финансового ущерба. Это в первую очередь порча оборудования и программного обеспечения. Вторая группа финансовых рисков связанна с вопросами госзаказа, начисления заработной платы и иных экономических вопросов.

В группу политических рисков включим риски, отрицательно влияющие на имидж учреждения, что может сказаться на наборе желающих учиться в данном ОУ, и может привести либо к ухудшению контингента учащихся, либо даже к его уменьшению, что при нынешних принципах финансирования может серьезно сказаться на бюджете. Часть политических рисков связана с необходимостью выполнением ОУ федеральных и региональных законодательных актов и иных нормативных документов, связанных с информатизацией, а также требований надзорных органов. К сожалению, зачастую образовательное учреждение оказывается в «вилке» между двумя нормативными документами. Так, до недавнего времени, в Санкт-Петербурге проверка районных баз «льготное питание учащихся» в социальном регистре населения проводилась по регламенту, утвержденному правительством города. Однако этот регламент не соответствовал 152-ФЗ «О защите персональных данных». И районные информационно-методические центры, занимающиеся сбором данных на уровне района, должны были либо не выполнять требования федерального законодательства, либо региональные нормативные акты. К счастью, эта ситуация улучшилась после внедрения системы межведомственного электронного взаимодействия (СМЭВ).

Необходимо отметить, что иногда грани отделяющие одну группу рисков от другой достаточно условны. Так, например, есть часть рисков, которые можно отнести и к педагогическим рискам, и к психолого-медицинским.

Еще один важнейшим фактором является то, что существуют угрозы, которые могут привести к реализации сразу нескольких рисков. Сгоревшее оборудование приведет как к отмене занятия (педагогический риск), так и к прямым финансовым потерям (финансовый риск).

Конечно, конкретные наборы рисков могут отличаться в зависимости от региона, особенностей учреждения, его уровня информатизации, но значительная часть рисков, а также общие подходы к созданию безопасной информационной среды ОУ будут одинаковы.