**Информационная безопасность ВУЗа**

**Information security in university**

*Максим Игоревич Шубинский   
Shubinskiy Maksim*

**ОРГАНИЗАЦИЯ**

Государственное бюджетное образовательное учреждение дополнительного педагогического профессионального образования Центр повышения квалификации Петроградского района Санкт-Петербурга «Информационно-методический центр»

Information and methodical center of the Petrograd district of St. Petersburg

**Город**

Санкт-Петербург

St Petersburg

**Телефон**

+7 812 3476791

**Факс**

+7 812 3476791

**e-mail**

[*shubinskiy@gmail.com*](mailto:shubinskiy@gmail.com)

***Аннотация***

В настоящей работе рассмотрены задачи управления образовательным учреждением по обеспечению его информационной безопасности. Сформулированы основные направления информационной безопасности школ и определены те аспекты, которые заслуживают наибольшего внимания руководителей ОУ.

The potential amount of information security tasks in educational institutions is given in the article. The main directions of information security establishment in general university are formulated. The key aspects to be concerned by the heads of university are determined in the text.

**Ключевые слова**

Управление, образовательное учреждение, информационная безопасность

University, information security, management

**Введение**

Один из самых важных вопросов стоящих сейчас перед ОУ с точки зрения информационных технологий – это вопрос информационной безопасности образовательного учреждения. Целью данной работы является определить управленческие задачи, стоящие перед администрацией ВУЗа и иных ОУ, связанные с защитой информации.

С нашей точки зрения, информационная безопасность ОУ включает в себя три больших направления

* Информационная безопасность компьютеров, локальной сети, серверов и информационных систем
* Защита персональных данных
* Минимизация педагогических и репутационных рисков учреждения.

Каждое из вышеперечисленных направлений будем рассматривать с точки зрения трех управленческих задач.

* Технические работы, включающие в себя работы по программно-аппаратному обеспечению информационной безопасности
* Организационные работы, определяющие перечень организационных мероприятий и необходимость выпуска локальных нормативных документов.
* Обучение, как персонала, так и учащихся, знаниям и навыкам, необходимым для работы в защищенной информационной среде образовательного учреждения.

**Информационная безопасность компьютеров, локальной сети, серверов и информационных систем**

Это направление наиболее близко к привычной деятельности специалистов, занимающихся информационной безопасностью. Здесь речь идет о защите от несанкционированного доступа, разграничении прав доступа, защиты от вирусов, и компьютерных атак. Современные образовательные учреждения, используют свыше 10 автоматизированных информационных систем (АИС) и имеют парк до нескольких тысяч современных компьютеров, объединенных в локальную сеть, файловые и почтовые сервера. При этом, на всех компьютерах должно стоять полноценное антивирусное ПО, защищающее от вирусов, троянов, сетевых атак и т.п.

Вторая важнейшая задача, которая стоит перед учреждением, это организационные меры по защите информации, которые включают в себя большой объем бумажной работы. Так необходимы регламенты о работе с локальной сетью, Интернетом, каждой информационной системой. Администрация учреждения, также, должна выпустить целый ряд приказов, например, о назначении ответственного за информационную безопасность учреждения.

В каждом учреждении должен быть утвержденный руководителем ОУ план работ по совершенствованию системы информационной безопасности учреждений, что позволит запланировать требуемое финансирование в рамках выделяемой учреждению субсидии или запросить его у учредителя как субсидию на иные цели.

Третья задача – это задача повышения квалификации специалистов в вопросах информационной безопасности. В большинстве своем, сотрудники, которых назначают ответственными за информационную безопасность, не имеют профильного образования в данной области. Следовательно, требуется повышение квалификации в данной сфере в размере не менее 72 часов.

Подводя итоги состояния дел по первому направлению, можно сделать вывод, что если бы речь шла о коммерческом предприятии с таким парком машин, стоимость полноценных работ по защите информации исчислялась бы миллионами рублей.

**Защита персональных данных**

Начиная с 2006 года согласно 152 ФЗ «О защите персональных данных любое государственное образовательное учреждение является оператором персональных данных, так как хранит у себя и ведет автоматизированную обработку персональных данных обучающихся и сотрудников.

Если говорить о технических работах, то в качестве примера можно рассмотреть пилотный проект по защите персональных данных школ Петроградского района Санкт-Петербурга, который проходил в 2012 году и включал в себя защиту локальной сети учреждения от НСД, межсетевой экран и установку специального криптографического ПО, защищающее рабочее место ИСПДн от НСД. Общая стоимость работ на одно учреждение (20 рабочих мест) превысила 1 млн. рублей.

Говоря о решении второй задачи, необходимо отметить, что в примерном перечне документов, которые необходимо разработать любому государственному учреждению имеются 27 документов.

**Минимизация педагогических и репутационных рисков учреждения**

Это направление деятельности обычно не затрагивается, когда говорят об информационной безопасности государственного учреждения. Но с точки зрения управления ОУ эта задача не менее, а может быть и более важная, чем 2 предыдущие.

В группу педагогических рисков, включаются те риски, которые могут повлиять на учебный процесс. Например, если в результате проблем с безопасностью будет невозможно использовать компьютерное оборудования при ведении занятий. Это может случиться при неполадках с локальной сетью учреждения или с файловыми серверами. И хотя все данные останутся целыми, а сеть удастся восстановить, время простоя может составить от нескольких часов до недель. В связи с отсутствием прямых финансовых потерь эта проблема считается несущественной, однако в настоящее время на занятиях повсеместно используются компьютеры, локальная сеть и специализированное программное обеспечение. Проблема состоит еще и в том, что согласно новым стандартам использование их при проведении занятий во многих случаях является обязательным.

Вторая группа педагогических рисков связана с непосредственным отрицательным влиянием получаемого нежелательного контента на студентов, что делает необходимым включение дополнительных тем и (или разделов) в учебный процесс, а также проведение дополнительных воспитательных мероприятий.

И, наконец, в группу репутационных рисков включим риски, отрицательно влияющие на имидж учреждения, что может сказаться на наборе, и может привести либо к ухудшению контингента учащихся, либо даже к его уменьшению, что при нынешних принципах финансирования может серьезно сказаться на бюджете.

Еще одна группа репутационных 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 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).

Конечно, конкретные наборы репутационных рисков могут отличаться в зависимости от региона, особенностей учреждения, его уровня информатизации.

Минимизация потерь от педагогических и репутационных рисков обычно связана с быстротой реакции администрации учреждения на произошедшие проблемы. Соответственно оптимальной защитой в данном случае будет план мероприятий, позволяющий перестроить деятельность за минимальные сроки. Но необходимо помнить, что если на данный момент эти риски кажутся незначительными, то через 5 – 7 лет уже трудно будет представить занятие без компьютера, выбор учебного заведения без сайта, а защита от нежелательного контента будет требоваться по закону.

**Заключение**

К сожалению, работы по каждому из вышеперечисленных направлений носят фрагментарный характер. Связано это с несколькими ключевыми моментами

* Не выделяется достаточное финансирование на работы по защите информации
* Нет единой политики информационной безопасности ни у самих вузов, ни у региональных органов, занимающихся информационными технологиями, ни у министерства образования.
* У администрации образовательных учреждений не всегда существует представление о том, что именно и как необходимо защищать.

Можно сделать вывод, что для решения задачи управления информационной безопасностью в ВУЗе необходимо сформулировать единый подход к информационной безопасности образовательного учреждения. При этом необходимо отметить, что только комплексная работа по всем перечисленным направлениям может привести к решению проблемы защиты информации и созданию безопасной информационной образовательной среды.