ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2016» атты XI Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XI Международной научной конференции студентов и молодых ученых «НАУКА И ОБРАЗОВАНИЕ - 2016»

PROCEEDINGS of the XI International Scientific Conference for students and young scholars «SCIENCE AND EDUCATION - 2016»

2016 жыл 14 сәуір
Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2016» атты XI Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XI Международной научной конференции студентов и молодых ученых «Наука и образование - 2016»

PROCEEDINGS of the XI International Scientific Conference for students and young scholars «Science and education - 2016»

2016 жыл 14 сәуір

Астана

ӘӨЖ 001:37(063)
КБЖ 72:74
Ғ 96

Ғ96 «Ғылым және білім – 2016» атты студенттер мен жас ғалымдардың XI Халық. ғыл. конф. = XI Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2016» = The XI International Scientific Conference for students and young scholars «Science and education - 2016» . – Астана: http://www.enu.kz/ru/nauka/ nauka-i-obrazovanie/, 2016. – .... б. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-764-4

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

ӘОЖ 001:37(063)
КБЖ 72:74

ISBN 978-9965-31-764-4

ожидается, значительно расширить западноевропейский туризм в крупнейшей стране в Центральной Азии. Члены группы включают в себя большинство стран ЕС, США, Канада, Мексика, Чили, Турции, Японии, Южной Кореи, Австралии и Новой Зеландии. Но самые глубокие и самые выносливые связи между народами Казахстана, и Западной Европы существуют в их общей приверженности к сохранению и продвижению их обществ путем мирного и взаимного сотрудничества. Европейский союз вырос из приверженности среди своих народов, чтобы избежать ужасов двух мировых войн, которые опустошали свой континент в первой половине 20-го века. Как только Казахстан стал независимым, Президент и народ принял историческое решение об отказе от всех видов ядерного оружия и работать для мира, свободного от бедствия ядерного оружия. Это сближение ценностей между Казахстаном и странами ЕС выставляет ложь мифа, что цивилизации обречены на столкновение. Наоборот, эти два региона разделяют приверженность международного мира, сотрудничества и мирного распространения открытых обществ и демократических институтов. [8, с.13]

Список использованных источников

1. Абыкаев Н. Казахстан - Европейский Союз: партнерство и сотрудничество// Казахстанская Правда. 2000, 24 июня, № 158.С.7.
2. Назарбаев Н.А. Пять лет независимости. - Алматы: Казахстан, 1996. С.153.
3. Воронина К. Казахстан и ЕС подписали Соглашение об углубленном партнерстве// Казахстанская Правда. 2015, 22 декабря, №243. С.5.
4. Назарбаев Н. Указ Президента Республики Казахстан о государственной программе «Путь в Европу» на 2009-2011 годы// Казахстанская Правда, 2008, 4 сентября, №193. С.398.
5. Лаумулин М.Т. Казахстан в современных международных отношениях: безопасность, геополитика, политология. – Алматы: Казахстан, 2000. С. 201.
6. Ибрашев Ж., Енсебаева Э. Европейский Союз во внешней политике Казахстана. – Алматы: ПД «Домино», 2001. С.374.
7. Нигматуллин М. Привлекая западные капиталы// Финансы Казахстана. 1997. №8. С.256.
8. Назарбаев Н.А. Моя цель – построить нормальное демократическое общество//Казахстанская Правда. 2002, 7 февраля, №167. С.13.

УДК 346.5

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ПРЕДПРИНИМАТЕЛЬСТВА

Жанартов Искандер Даулетович
Eskinn1@gmail.com
Студент второго курса юридического факультета в ЕНУ им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – С.Г. Кожахметова

На сегодняшний день мало предпринимателей задумывается о безопасности информаций так или иначе связанной с их бизнесом. Но с каждым годом опасность утечки информаций всё больше и больше затрагивает как мировых, так и казахстанских бизнесменов. Согласно недавним исследованиям Лаборатории Касперского, в Казахстане только треть компаний (32%) беспокоит вопрос защиты данных, а больше половины (52%) опрошенных пренебрегают разработкой и внедрением политик информационной безопасности. Еще одно исследование говорит о том, что две трети казахстанских компаний теряли данные из-за внешних или внутренних угроз, причем случайные утечки в силу человеческого фактора, намеренные утечки из-за сотрудников и корпоративный шпионаж

заняли 55% от всех угроз. С каждым годом эти цифры не уменьшаются, а растут большими темпами.

Но что мы подразумеваем под «информационной безопасностью»? В пункте 5, статьи 4 Закона Республики Казахстан «О Национальной безопасности» содержится термин: «Информационная безопасность - состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны» [1].

Основным нормативно-правовым актом, регулирующим отношения в сфере обеспечения безопасности в Казахстане, является Закон Республики Казахстан «О национальной безопасности», который регулирует правовые отношения в области национальной безопасности Республики Казахстан и определяет содержание и принципы обеспечения безопасности человека и гражданина, общества и государства, систему, цели и направления обеспечения национальной безопасности Республики Казахстан. Среди видов национальной безопасности в качестве отдельного вида выделяется информационная безопасность. В статье 6 этого Закона среди основных угроз национальной безопасности определяются следующие: снижение уровня защищённости информационного пространства страны, а также национальных информационных ресурсов от несанкционированного доступа; информационное воздействие на общественное и индивидуальное сознание, связанное с преднамеренным искажением и распространением недостоверной информации в ущерб национальной безопасности. Соответственно, уровень защищенности определяет качество национальной безопасности, позволяя оценивать эффективность мер предупреждения современных угроз и мероприятий по их предупреждению и устранению.

О проблемах информационной безопасности обеспокоен генерал – лейтенант, председатель КНБ РК Н.Н. Дутбаев, и вот что он говорит:- «В целях защиты информационных ресурсов страны технические средства защиты информации разрабатываются казахстанскими предприятиями, а также соответствующими подразделениями Комитета национальной безопасности. Введенная в действие сеть передачи данных специального назначения разработана нами для организации обмена информацией между государственными органами. Все оборудование этой сети проверено на наличие закладок и побочных излучений. В 2015 году к сети подключено 97 государственных пользователей. Это всего 26% от имеющихся возможностей. Что касается мощности сети, то она такова, что позволяет обеспечить работу «электронного правительства республики». В то же время имеют место нарушения требований нормативных правовых актов, когда отдельные работники государственных органов для ведения служебной переписки нередко используют открытые каналы связи. В республике разрабатывается ряд нормативных правовых актов в области обеспечения информационной безопасности, при соблюдении требований которых подобные угрозы представляют минимальную опасность» [2].

Законодатель старается оградить информационную безопасность государства, обычных граждан и предпринимателей. Существует перечень нормативных правовых актов, посредством которых регулируется информационная безопасность в Республике Казахстан:

1) Законы Республики Казахстан "О государственных секретах", "Об электронном документе и электронной цифровой подписи", "Об информатизации", "О техническом регулировании", "О лицензировании", "О средствах массовой информации", "О связи" и другие;

2) отраслевая Программа в сфере защиты государственных секретов;

3) отраслевая Программа по обеспечению информационной безопасности РК на 2011-2014 годы, утвержденная постановлением Правительства РК от 31 января 2011 года №45 дсп;

4) Программа по развитию информационных и коммуникационных технологий в Республике Казахстан на 2010-2014 годы, утвержденная постановлением Правительства Республики Казахстан от 29 сентября 2010 года №983;

5) стратегические планы государственных органов.

6) Концепция «информационной безопасности Республики Казахстан до 2016 года».

Госорганами республики рассматривается вопрос о присоединении Казахстана к «Конвенции о киберпреступности», принятой Советом Европы в 2001 году, что позволит расширить географию борьбы с компьютерными преступлениями, а также перенимать опыт зарубежных правоохранительных органов в данной сфере.

В предпринимательском кодексе Республики Казахстан от 14 января 2016 года предусмотрены две нормы по охране и неправомерному использованию информации, составляющей коммерческую тайну. В статье 28 законодатель определяет, какой круг лиц, к какой информаций имеет доступ, и в чём заключается охрана информации, составляющей коммерческую тайну. Охрана коммерческой тайны заключается в запрете незаконного получения, распространения либо использования информации, составляющей коммерческую тайну в соответствии с настоящим Кодексом и законодательством РК. В статье 189 сказано, что неправомерным использованием информации, составляющей коммерческую тайну, является использование без разрешения правообладателя при осуществлении предпринимательской деятельности сведений, составляющих в соответствии с законодательством Республики Казахстан коммерческую тайну. Понятия и термины только начинают вводиться в нормотворчестве Казахстана, тем самым показывая, что законодатель начинает беспокоиться о данной проблеме, но исходя из Уголовного кодекса и Кодекса об административных правонарушениях, мы видим, что мера наказания низкая [3].

Статьи с указанными санкциями за совершение правонарушений связанные с инсайдерской деятельностью указаны в Уголовном кодексе и Кодексе об административных правонарушениях Республики Казахстан. В статье 230 Уголовного кодекса указано, что умышленное использование инсайдерской информации при совершении сделки (сделок) с ценными бумагами (производными финансовыми инструментами) или умышленная незаконная передача инсайдерской информации третьим лицам либо умышленное незаконное предоставление третьим лицам доступа к инсайдерской информации, а равно умышленное предоставление третьим лицам рекомендаций о совершении сделки (сделок) с ценными бумагами (производными финансовыми инструментами), основанных на инсайдерской информации, если эти деяния причинили крупный ущерб гражданину, организации или государству, наказываются штрафом в размере до пятисот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до трехсот часов, либо арестом на срок до девяноста суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового [4].

В части 2 статьи 185.6. «Неправомерное использование инсайдерской информаций» Уголовного кодекса Российской Федераций [5], в котором сказано, что умышленное использование инсайдерской информации путем ее неправомерной передачи другому лицу, если такое деяние повлекло возникновение последствий, - наказывается штрафом в размере от пятисот тысяч рублей до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от двух до четырех лет либо лишением свободы на срок от двух до шести лет со штрафом в размере до ста тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет либо без такового с лишением права занимать определенные должности либо заниматься определенной деятельностью на срок до четырех лет или без такового. Из Уголовного кодекса Российской Федераций мы видим, что санкция за одинаковые преступления в сфере инсайдерской деятельности отличаются, казахстанский законодатель применяет наказание не столь суровое, тем самым предоставляя правонарушителем поле для манёвра, точнее для совершения правонарушения.

Законодатель определяет инсайдерскую деятельность как преступление небольшой тяжести, что показывает незначительное внимание к данной проблеме. Кодекс об административных правонарушениях содержит статью «Незаконное использование инсайдерской информации», в которой говорится что действия инсайдеров по использованию инсайдерской информации при совершении сделок с ценными бумагами и (или) производными финансовыми инструментами, незаконной передаче инсайдерской

информации третьим лицам, предоставлению третьим лицам рекомендаций или предложений о совершении сделок с ценными бумагами и (или) производными финансовыми инструментами, основанных на инсайдерской информации, а также невыполнение требований законодательства РК по предоставлению эмитентам информации юридическими лицами, признанными инсайдерами, в отношении данных эмитентов, если эти действия не причинили крупный ущерб, влекут штраф на физическое лицо в размере двухсот, на должностное лицо - в размере четырехсот, на юридическое лицо - в размере шестисот месячных расчетных показателей [6]. Инсайдеры на продаже некоторой информаций могут получить намного больше, и откупиться небольшой, по сравнению с его прибылью, суммой, что является не честным по отношению к предпринимателю, который несёт огромные потери вследствие деятельности этих самых «чёрных» инсайдеров. Желательно на законодательном уровне пересмотреть санкции, назначаемые при данных правонарушениях.

Так как, в суде доказать виновность инсайдера нужно заключать с работниками договор о неконкуренции согласно 29 статье Трудового кодекса Республики Казахстан [7]. По соглашению сторон между работодателем и работником может заключаться договор о неконкуренции, которым предусматривается обязательство работника не осуществлять действий, способных нанести ущерб работодателю. Так же в договоре о неконкуренции устанавливаются ограничения и условия их принятия, а также может устанавливаться компенсация на период действия этого условия.

Как же защититься субъектам предпринимательства от утечки информации? В первую очередь необходимо определить каналы утечки информации и средства их контроля, а, при необходимости, и перекрытия. Важнейшим инструментом в этом является аудит информационной безопасности. Аудитинформационной безопасности – независимая экспертная оценка защищенности информационной системы компании с учетом таких факторов как персонал, процессы и технологии. Основной целью аудита является определения соответствия применяемых в организации защитных мер выбранным критериям информационной безопасности. Аудит позволит выявить каналы утечки, оценить их критичность и вероятность утечки по ним. Анализ данных, собранных во время аудита, даст возможность выбора средств контроля каналов, исходя из бизнес-модели предприятия и типов каналов.

Один из аспектов, представляющих серьезную угрозу информационной безопасности для бизнеса - внутренние утечки данных. Сотрудники компаний теряют ноутбуки с конфиденциальной информацией, умышленно или неумышленно копируют и выносят данные за пределы офисов, пересылают посредством сторонних мессенджеров информацию, предназначенную исключительно для внутреннего использования. Инсайдер (англ. insider) - член какой-либо группы людей, имеющей доступ к информации, недоступной широкой публике. Зачастую именно инсайдеры виновны в том, что информация выходит за пределы группы. Можно при заключении трудового договора указать условие о неконкуренции? В пункте 9 статьи 1 Трудового кодекса содержится термин: «условие о неконкуренции - условия договора о неконкуренции, ограничивающие право работника на осуществление действий, способных нанести ущерб работодателю», согласно 29 статье Трудового кодекса РК по соглашению сторон между работодателем и работником может заключаться договор о неконкуренции, которым предусматривается обязательство работника не осуществлять действий, способных нанести ущерб работодателю [7]. Так же в договоре о неконкуренции устанавливаются ограничения и условия их принятия, а также может устанавливаться компенсация на период действия этого условия. Но зачастую и это не останавливает инсайдеров. Так как же решать проблемы утечки информаций? Полностью ограничивать доступ к данным нельзя, так как от этого пострадает производство. Существуют несколько путей решения этой проблемы, и в этом докладе мы постараемся рассказать о некоторых из них.

Как решить все вопросы безопасности, не ограничивая при этом сотрудников в функциональности и давая компании возможность активно развиваться? Решение всех этих задач предложила компания Cisco, представив платформу Cisco Identity Services Engine (ISE). Платформа Cisco ISE позволяет внедрить в компаниях концепцию BYOD, а также организовать наиболее безопасный доступ к ресурсам центра обработки данных. Кроме того, она позволяет управлять процессами идентификации и контроля доступа, давая возможность обеспечить соблюдение всех норм безопасности в организации. Как отмечают представители Cisco, платформа работает с учетом контекста местоположения и на основе идентификации. Она собирает информацию о сети, пользователях и устройствах в режиме реального времени. Затем она использует эту информацию для принятия упреждающих решений по управлению, обеспечивая применение политик в пределах всей сетевой инфраструктуры.

Если же говорить о финансовой стороне вопроса, проект по внедрению Cisco Identity Services Engine окупается в течение одного-полутора лет. «Причем, такие кейсы, как автоматизация гостевого доступа, могут окупаться еще быстрее, - отмечает Владимир Илибман, эксперт по продуктам безопасности Cisco. Основные статьи получения выгоды: уменьшение затрат на инфраструктуру; уменьшение затрат на подключение мобильных устройств; уменьшение затрат на службу поддержки; уменьшение рисков, связанных с инцидентами безопасности, внутренними вирусными эпидемиями и заражениями. Подчеркну, в чем состоит окупаемость [8].

Также надежным средством ограничения доступа и защиты документов является Active Directory Rights Management Services, которое с помощью маркировки документов не допускает неправомерного их использования. Служащие, работающие с информацией, теперь могут указывать тех, кому разрешено использовать документ. Также они могут определять действия, которые разрешено производить с документом. Например, они могут предоставить права на открытие, внесение изменений, печать, пересылку документа, а также на выполнение ряда других действий.

Одним из наиболее распространённых способов защиты в Казахстане это специальные DLP-решения (Data Loss Prevention). DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Такую защиту предоставляет компания InfoWatch с продуктом InfoWatch Traffic Monitor 5.0, которая заполнили большую часть Казахстанского рынка в области обеспечения безопасности сферы предпринимательства. «InfoWatch Traffic Monitor 5.0 - это огромный шаг в развитии DLP-систем в целом. Если раньше данные системы использовались преимущественно для задач информационной безопасности, то теперь с их помощью можно эффективно решать задачи бизнеса. Наше решение помогает бизнесу получить уверенность в безопасности ценных и конфиденциальных данных, дает понимание всех внутренних и внешних потоков информации в организации, позволяет выявить сговоры, злоумышленников, лиц занимающихся промышленным шпионажем, помогает осуществлять бизнес-разведку с целью контроля деятельности персонала и определения степени их лояльности к компании.»: говорит Евгений Симонов, руководитель направления по развитию бизнеса InfoWatch в Центральной Азии. Около 70% заказчиков данной продукций находится в государственном сегменте. Это объясняется тем, что государственные организации используют крайне чувствительную информацию, утечка которой критична. Приблизительно 20% заказчиков - это финансовый сектор, и оставшиеся 10% - это достаточно разнородные компании из промышленной и нефтяной отрасли. Сейчас среди заказчиков InfoWatch - крупнейшие казахстанские компании из различных отраслей, среди которых Служба охраны Президента Республики Казахстан, Министерство нефти и газа Республики Казахстан, Министерство здравоохранения Республики Казахстан, Администрация Президента Республики Казахстан, АО «Нурбанк» и многие другие [9].

Для обеспечения информационной безопасности своего бизнеса, предприниматели должны во-первых, защищать свои документы от всех видов утечки посредством установления специальных программ и обращаясь в специальные организаций предоставляющие информационную безопасность. Во вторых нанимать высокообразованных работников и заключать с ними договор о неконкуренции, в соответствии с нормами трудового законодательства. Законодатель же для поддержки предпринимательства и обеспечения безопасности в сфере охраны информации, должны ужесточить санкций за преступления в сфере инсайдерской деятельности.

Список использованных источников:

1. Закон Республики Казахстан от 6 января 2012 г. № 527-IV «О национальной безопасности Республики Казахстан» (с изменениями по состоянию на 10.07.2012 г.) // Казахстанская правда. - 2012 г. - 17 янв. - № 19-20 (26838-26839).
2. Информационная безопасность. Официальный сайт Комитета национальной безопасности Республики Казахстан // knb.kz/
3. Кодекс Республики Казахстан от 29 октября 2015 года № 375-V «Предпринимательский кодекс Республики Казахстан» (с изменениями и дополнениями от 14.01.2016 г.)
4. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 24.11.2015 г.)
5. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 30.12.2015)
6. Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года № 235-V (с изменениями и дополнениями по состоянию на 22.01.2016 г.)
7. Трудовой кодекс Республики Казахстан от 23 ноября 2015 года № 414-V
8. Статья: «Cisco Identity Services Engine — надежность и мобильность вашей корпоративной сети» // http://profit.kz/articles/7174/Cisco-Identity-Services-Engine-nadezhnost-i-mobilnost-vashej-korporativnoj-seti/
9. Статья «ИТ-безопасность коммерческой информации» // http://efsol.ru/promo/data-protection.html

УДК 338.1

РОЛЬ ОБРАЗОВАНИЯ И НАУКИ В ФОРМИРОВАНИИ НАЦИОНАЛЬНОГО ЧЕЛОВЕЧЕСКОГО КАПИТАЛА: ОРГАНИЗАЦИОННЫЕ И ПРАВОВЫЕ ВОПРОСЫ

Жангалиев Нурбек Наурызбаевич
astananurbek@mail.ru
Магистрант 2 курса,
Евразийский Национальный Университет им. Л.Н. Гумилева, г. Астана
Научный руководитель – Б. Алтынбасов

На сегодняшний день актуальным является вопрос формирования механизма инвестирования в человеческий капитал. В целом современные тенденции развития и формирования общественной модели развития позволяют сделать вывод о том, что именно инвестирование человеческого капитала, формирование баланса в социальной сфере будет стимулировать развитие всех сфер деятельности государства. Первоначально под человеческим капиталом понималась лишь совокупность инвестиций в человека, повышающая его способность к труду - образование и профессиональные навыки. В дальнейшем понятие человеческого капитала существенно расширилось. На современном этапе указанное понятие включают в него потребительские расходы - затраты семей на питание, одежду, жилища, образование, здравоохранение, культуру, а также расходы государства на эти цели [1, с. 36]. То есть, сегодня человеческий капитал - это своего рода