УДК-004.056.53:005.922.1

[1]Т.Ж. Мазаков , [2]А. Бадигулов

[1] Институт информационных и вычислительных технологий МОН РК , г. Алматы, Республика Казахстан
[2] Казахский национальный университет имени аль-Фараби , г. Алматы, Республика Казахстан
[1]E-mail: tmazakov@mail.ru

Инсайдер - внутренний источник возникновения угрозы информационной безопасности

Для любой большой компании одна из основных угроз информационной безопасности - это инсайдеры. Как утверждают эксперты по защите информации, 80 являются внутренними. Серьезный ущерб безопасности компании может нанести сотрудник, имеющий полный доступ к финансовой или другой информации и недовольный политикой руководства. В данной статье рассмотрены проблемы организации защиты информации, именно от этого, т.е. от внутренних утечек. Авторами дано определение инсайдера, как источника возникновения угрозы информационной безопасности, их типы. Существует несколько способов защиты от инсайдерства. Прежде всего, надо выявить инсайдера, для этого в статье предложены различные психологические методы обнаружения инсайдеров. Описаны психологические типы сотрудников склонных к инсайдерству и способы их выявления. Следующий этап - это предотвращение угрозы со стороны инсайдера. Для этого существуют ряд технических методов по обнаружению действий злоумышленников, они также рассмотрены в статье. Таким образом, при решении задачи противодействия инсайдерам нужно для начала оценить риски и применить комплекс организационных и технических средств.
Ключевые слова: информационная безопасность, защита информации, инсайдер, психотип, утечка информации, конфиденциальная информация, несанкционированный доступ.

T. Mazakov, A. Badigulov,

Insider - internal source of information security threats

For any large company is one of the major threats to information security - it's insiders. According to experts on the protection of information, 80Serious damage to the company's security can do, having full access to the financial or other information, and dissatisfied with the policy manual. This article describes the problems of the organization of information security, it is from this, that by internal leakage. The authors give the definition of an insider as the source of a threat to information security, their types. There are several ways to protect against insiders. First of all, it is necessary to identify the insider, this article proposed various psychological methods to detect insiders. Describes the psychological types of employees are prone to insiders and ways of detecting them. The next step - is to prevent threats from insiders. For this, there are a number of technical methods to detect malicious activity, they are also considered in the article. Thus, when solving the problem of counteraction insiders need to begin to assess the risks and apply a set of organizational and technical means.
Key words: Information security, insider, psychology type, leaked of information , confidential information, unauthorized access.

Т.Ж. Мазаков, А. Бадигулов,

Инсайдер - ақпараттық қауіпсіздік қауіп-қатерін тудыратын ішкі қайнар көз

Кез келген үлкен компания үшін ақпараттық қауіпсіздігіне негізгі қауіп төндіруші - инсайдерлер болып табылады. Ақпараттарды қорғау бойынша сарапшылардық айтуынша ақпараттық қауіпсіздік инциденттерінің 80 инциденттер болып табылады. Компания қауіпсіздігіне қаржылық және басқадай ақпараттарға толық қол жетімділігі бар, басшылық саясатын ұнатпайтын қызметкер айтарлықтай зиян келтіруі мүмкін. Бұл мақалада ақпараттарды нақ осындай, ақпараттардың өз ішінде қолды болуынан қорғауды ұйымдастыру проблемалары қарастырылған. Авторлар инсайдерге ақпараттық қауіпсіздікке қауіп төндіретін көздер ретінде анықтама беріп, олардың типтерін келтірілген. Инсайделіктен қорғаудың бірнеше тәсілі бар. Ең алдымен инсайдерді анықтап алу керек, ол үшін мақалада инсайдерлерді анықтаудың бірнеше психологиялық әдістері ұсынылған. Инсайдерлікке бейім қызметкерлердің психологиялық типтері және оларды анықтау тәсілдері сипатталған. Келесі кезең - ол инсайдержағынан болатын қауіпті болдырмау. Бұл үшін қастық ойлаушының әрекеттерін анықтаудың бірқатар техникалық әдістері бар, олар осы мақалада қарастырылған. Осылайша, инсайдерлерге қарсы тұру есептерін шешуде ең алдымен қатерлерді бағалап алып және содан кейін ұйымдық және техникалық құралдар кешенін қолдану керек.

Түйін сөздер: ақпараттық қауіпсіздік, ақпаратты қорғау, инсайдер, психотип, ақпараттық кемуі, құпия ақпарат, рұқсат берілмеген.

Введение

Поступательное развитие современного информационного общества базируется на новейших технологиях, новых методах и современных подходах. Развитие общества - это его динамический состояние, при котором осуществляется его трансформация в новое состояние, с новыми возможностями. Общество может развиваться позитивно, если она адекватно реагирует на возникающие угрозы. Соответственно, проблемы обеспечения информационной безопасности являются одним из приоритетных в обеспечении безопасности в целом. Информационную безопасность принято рассматривать в двух аспектах, в техническом и социально-политическом. Технический аспект подразумевает обеспечение защиты национальных информационных ресурсов, информационных систем, информационно-телекоммуникационной инфраструктуры от неавторизованного доступа, неправомерного использования, раскрытия, нарушения, изменения, прочтения, проверки, записи или уничтожения для обеспечения целостности, конфиденциальности и доступности информации. Социально-политический аспект заключается в защите национального информационного пространства и систем распространения массовой информации от целенаправленного негативного информационного и организационного воздействия, могущего причинить ущерб национальным интересам Республики Казахстан [1]. Общество в рамках государства, являясь по своей структуре системой имеет свои подсистемы - ячейки (семья, коллектив, объединения и т.д.). Так обеспечение безопасности информационного общества зависит от безопасности ее "элементов человека. Таким образом, любое действие человека в обществе, влияет на безопасность общества в целом. Если за действия или бездействия человека, которые создают общественно опасное деяние, Уголовным кодексом РК предусмотрены различные виды наказания. То в рамках информационного пространства, при взаимодействии человека с информационной системой не всегда есть возможность юридически квалифицировать его деяния, по причине не унифицированности законодательства в сфере обеспечения информационной безопасности. Необходимо отметить, что правовое обеспечение информационной сферы

не достаточно адекватно регулирует безопасное использование киберпространства. В настоящее время, недостаточно проработаны механизмы, регулирующие информационные правоотношения. Текущее состояние правового обеспечения противодействия информационным преступлениям также характеризуется недостаточной согласованностью используемых правовых механизмов и не адекватной деятельности субъектов, обеспечивающих информационную безопасность. Современные разработки "High Tech"в сфере обеспечения информационной безопасности позволяет адекватно реагировать появляющимся информационным угрозам на техническом уровне. Однако, правовые механизмы их применения, в большинстве случаев законодательно не отрегулированы. Возникающие проблемы в обеспечении информационной безопасности необходимо рассматривать комплексно. При организации защиты информационных систем от угроз, необходимо поддерживать баланс между "легитимностью "достаточностью мер защиты"и доступностью самой информационной системы пользователю. Под угрозой безопасности информации, принято понимать потенциально существующую опасность случайного или преднамеренного нарушения безопасности информации, обусловленной особенностями ее хранения и обработки. Источник возникновения опасности может быть внешним и внутренним. Ярким примером внешнего преднамеренного источника опасности является "хакер". Хакер - лицо, совершающее различного рода незаконные действия с информационными ресурсами: несанкционированное проникновение в чужие компьютерные сети и получение из них информации, незаконное снятие защиты с программных продуктов и их копирование, создание и распространение компьютерных "вирусов"и т.п. В средствах массовой информации, периодично всплывают сообщения о том, что "хакеры"осуществили взлом сети той или иной организации. В настоящее время, средства и методы защиты информации от внешнего воздействия позволяют своевременно обнаружить угрозу и локализовать их. Актуальным вопросом в обеспечении информационной безопасности является защита информации от внутренних утечек конфиденциальной информации. Утечка информации, это неконтролируемое распространение информации за пределы организации или круга лиц, которым она доверена, в результате ее разглашения, несанкционированного доступа к информации. Утечка информации бывает случайной и умышленной. По результатам исследования аналитического Центра InfoWatch за первое полугодие 2013 в мире зафиксировано, обнародовано в СМИ и выявлено 496 случаев утечки. Необходимо отметить, что исследование охватывает незначительное (не более 1-5) число от реальных утечек, произошедших в мире [2]. При этом доля злонамеренных утечек превышает долю случайных. Злонамеренная утечка, эта утечка организованная лицом - "инсайдером имеющим правомерный доступ к информации. Инсайдер (англ. insider, от inside - внутри) - лицо, имеющее в силу своего служебного или семейного положения доступ к конфиденциальной информации о делах государственных или коммерческих организаций. В эту группу включаются также лица, добывающие конфиденциальную информацию о деятельности организации и использующие ее в целях личного обогащения [3]. Инсайдеры - это технически грамотные люди, поскольку для того, чтобы получить доступ к информации, имеющей значение для организации, нужно иметь представление о том, как эта информация защищается от тех сотрудников, которые не должны её видеть. Но в настоящее время не обязательно быть настоящим хакером для того, чтобы украсть конфиденциальные документы из системы, в которую есть официальный доступ. Просто необходимо умело пользоваться уже разра-

ботанными методами взлома. Следует отметить, что многие государственные организации не уделяют достаточного внимания защите внутренних конфиденциальных данных. Хотя, утечка государственных секретов может привести к непоправимым последствиям, чем утрата коммерческой конфиденциальной информации. Представители National Reconnaissance Office (подразделение разведки США) отмечают, что государственные и коммерческие организации оставляют без должного внимания вопросы организации защиты от внутренних угроз. По данным National Reconnaissance Office, ими в борьбе с инсайдерами применяются такие меры, как составление специфичных профилей, которые описывают типовые действия инсайдеров. Данный подход используется ФБР для розыска преступников. NRO считает, что борьбу с инсайдерами следует начинать с классификации данных и рисков связанных с утечкой конфиденциальной информации [4]. Имея в распоряжении психологический портрет злоумышленника, служба внутренней безопасности организации имеет возможность повысить эффективность работы по выявлению и пресечению нарушителя. Так ряд специалистов по обеспечению информационной безопасности предлагают для классификации возможных нарушителей руководствоваться идеями швейцарский психолог К. Юнга. В первой половине XX века, ученный высказал мысль о том, что поведение человека не является случайным, а поддается предсказанию, и, следовательно, классификации. По мнению психолога, различия в поведении определяются базовыми психическими функциями, свойственными человеку на протяжении всей его жизни. В своей работе "Психологические типы"Карл Юнг выделил различные психологические типы людей в соответствии с разными индивидуальными способами восприятия и оценки информации. В частности, им предложено три пары полярных шкал, описывающих психические процессы восприятия и переработки информации (экстраверсия - интроверсия, сенсорика - интуиция, мышление - эмоции). На основе идеи Юнга, специалист в области информационной безопасности А. Дрозд в своей статье "Выявление инсайдеров путем анализа психотипов работников: мысли и немного практики"определил какие психотипы соответствуют тем и иным профессиям. К примеру: психотип ESTP - экстравертированная (E), предпочитающая получать информацию об окружающем мире при помощи своих органов чувств (S), ориентированная на мышление (T), склонная занимать созерцательную позицию (P) личность, предпочтение в высказывании своего собственного мнения относительно вопроса, при этом исключение доводов других (J) - соответствуют сотрудникам занимающих определенные ключевые и руководящие должности [5] . К примеру, по данным Метатека новости, бывшие сотрудники AMD перед уходом в NVIDIA скопировали на флеш-диск более 100 тыс. файлов с конфиденциальной информацией, принадлежащей AMD. После обнаружения утечки специалисты AMD выяснили, что вся операция была заранее спланирована. Инсайдеры решили покинуть AMD, прихватив с собой коммерческие секреты компании, для чего проникли на защищенные компьютеры и в течение шести месяцев собирали информацию. В числе сотрудников, обвиняемых в краже данных, упоминают Роберта Фельдштейна, бывшего вице-президента AMD по стратегическому развитию [6]. Так, сотруднику с психолотипом ESTP присущи такие негативные характеристики, как склонность к активному отрицанию этики в бизнесе, достижение цели любыми средствами, склонность к криминальному риску, игнорирование правовых барьеров. Проанализировав все типы с точки зрения этических и деловых качеств, среди них можно выделить наиболее склонные к совершению инсайда. В психологии существуют и дру-

гие методы по определению психотипов людей такие, как "Индикатор типов Майерс-Бриггс"(MBTI), "Определитель темперамента"(Keirsey Temperament Sorter) Д.Кирси и др. В рамках реализации технических средств, для выявления действий инсайдеров, необходимо внедрять системы, позволяющие в автоматическом режиме следить и реагировать на действия пользователей. В политике безопасности организации необходимо закрепить принцип регистрации всех действий с конфиденциальной информацией. Записи в журналах регистрации позволяют определить круг лиц, через которых могла произойти утечка, и при проведении расследовании инцидента привлечь к ответственности нарушителя. Наиболее удобной в использовании является система регистрации видео изображения на экране пользователя. Такая система наглядно покажет, что делал каждый сотрудник в определенные моменты времени. Недостатком технических средств защиты от утечки конфиденциальной информации, является обнаружения действий инсайдера через некоторое определенное время. Для эффективного противодействия инсайдерам, необходимо использовать в комплексе весь спектр возможных аналитических, психологических, административных и технических мер и методов.

Литература

[1] Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 "О Концепции информационной безопасности Республики Казахстан до 2016 года http://www.ru.government.kz/docs/u110000017420111114.htm

[2] Глобальное исследование утечек конфиденциальной информации в I полугодии 2013 года. Аналитический Центр InfoWatch, www.infowatch.ru/analytics.

[3] Экономический словарь. Инсайдер , http://abc.informbureau.com.

[4] Журнал "Homeland Defense Journal www.homelanddefensejournal.com.

[5] А. Дрозд Выявление инсайдеров путем анализа психотипов работников: мысли и немного практики, http://daily.sec.ru/

[6] Статья "Сотрудники AMD ушли в NVIDIA, украв секреты компании http://metateka.com/archive/17.01.13

References

[1] Ukaz Prezidenta Respubliki Kazakhstan ot 14 noyabrya 2011 goda № 174 "O Kontseptsii informatsionnoy bezopasnosti Respubliki Kazakhstan do 2016 goda http://www.ru.government.kz/docs/u110000017420111114.htm. Sovmestimoe sostoyanie

[2] Globalnoe issledovanie utechek konfindentsialnoi infomatsii v I polugodii 2013 goda. Analiticheskii Tsentr InfoWatch, www.infowatch.ru/analytics.

[3] Ekonomicheskii slovar. Insaider, http://abc.informbureau.com.

[4] Zhurnal "Homeland Defense Journal"// www.homelanddefensejournal.com.

[5] Drozd, Vyyavlenie insaiderov putem analiza psihotipov rabotnikov: mysli I nemnogo praktiki // http://daily.sec.ru/.

[6] Statya "Sotrudniki AMD ushli v NVIDIA, ukrav sekrety kompanii http://metateka.com/archive/17.01.13.