УДК 681.3.06

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ЭКОНОМИЧЕСКОГО ВУЗА: ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ, ПОДЛЕЖАЩЕЙ ЗАЩИТЕ, И ПОСТРОЕНИЕ МОДЕЛИ ЗЛОУМЫШЛЕННИКА

[1]Замараева О.А., [1]Титов В.А., [1]Кузин Д.О.

[1]ФГБОУ ВПО «Российский экономический университет имени Г.В. Плеханова», Москва, Россия (117997 Российская Федерация, г. Москва, Стремянный пер., 36), e-mail: vtitov213@yandex.ru

Определена степень актуальности проблемы защиты информации в высших учебных заведениях. Указаны основные принципы, необходимые для разработки политики информационной безопасности. Представлены цели, функции и задачи высшего учебного заведения экономического профиля. Предложена организационная структура ВУЗа. Подробно определена информация, подлежащая защите, в соответствии с подразделениями ВУЗа, занимающимися обработкой и хранением информации. Указаны виды хранения защищаемой информации и определен круг лиц, имеющих доступ к защищаемой информации. Дано определение и предложена модель злоумышленника. Приведены основные виды угроз конфиденциальной информации. Рассмотрено понятие внешнего и внутреннего злоумышленника. Проведено построение модели злоумышленника с описанием возможных угроз информации в высшем учебном заведении. Определены категории лиц, которые могут являться нарушителями. Рассмотрены ограничения и внесены предположения о характере действий возможных нарушителей.

Ключевые слова: политика информационной безопасности, модель злоумышленника, виды угроз информации, организационная структура Университета, информация.

DEVELOPMENT OF POLICY OF INFORMATION SECURITY FOR ECONOMIC HIGHER EDUCATION INSTITUTION: DEFINITION OF INFORMATION WHICH IS SUBJECT TO PROTECTION, AND CREATION OF MODEL OF THE MALEFACTOR

[1]Zamaraeva O.A., [1]Titov V.A., [1]Kuzin D.O.

[1]Plekhanov Russian University of Economics, Moscow, Russia (117977 Russian Federation, Moscow, Stremjannyj pereulok, 36), e-mail: vtitov213@yandex.ru

Degree of relevance of a problem of information security in higher educational institutions is defined. The basic principles necessary for development of policy of information security are specified. The purposes, functions and problems of a higher educational institution of an economic profile are presented. The organizational structure of higher education institution is offered. Information which is subject to protection, according to the divisions of higher education institution which are engaged in processing and storage of information is in detail defined. Types of storage of protected information are specified and the circle of people, having access to protected information is defined. Definition is given and the model of the malefactor is offered. Main types of threats of confidential information are given. The concept of the external and internal malefactor is considered. Creation of model of the malefactor with the description of possible threats of information in a higher educational institution is carried out. Categories of persons who can be violators are defined. Restrictions are considered and assumptions of nature of actions of possible violators are brought.

Keywords: policy of information security, model of the malefactor, types of threats of information, organizational structure of University, information.

Введение

В развитии компьютерной техники и программного обеспечения очень важную роль сыграли научные учреждения и высшие учебные заведения. В частности, в ВУЗах разрабатываются, испытываются и внедряются передовые проекты в сфере IT. С ростом киберпреступности защита конфиденциальной информации и научных разработок в учебных учреждениях становится особенно актуальной.

Под политикой информационной безопасности компании понимается «формальное изложение правил поведения лиц, получающих доступ к конфиденциальным данным в корпоративной информационной системе». При этом различают общую стратегическую политику безопасности компании, взаимоувязанную со стратегией развития бизнеса и ИТ-стратегией компании, и частные тактические политики безопасности, детально описывающие правила безопасности при работе с соответствующими ИТ-системами и службами компании.

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами: невозможность миновать защитные средства, усиление самого слабого звена, многообразие защитных средств, минимизация привилегий, разделение обязанностей, невозможность перехода в небезопасное состояние, достаточность всеобщей поддержки мер безопасности, простота в управлении информационной системой.

В первую очередь для разработки политики информационной безопасности ВУЗа экономического профиля необходимо рассмотреть его цель, функции, задачи и структуру.

Цель: университет как государственное высшее учреждение образования и науки определяет главенствующую роль в национальной системе образования, удовлетворяет потребности граждан в приобретении профессиональных знаний и умений в экономической сфере деятельности, в интеллектуальном, культурном и нравственном развитии личности, в удовлетворении потребностей общества в квалифицированных специалистах с высшим экономическим образованием.

Задачи университета:

1) Проведение профессиональной ориентации, довузовской подготовки и конкурсного отбора учащихся;
2) Обучение студентов;
3) Проведение последипломной подготовки и повышения квалификации;
4) Осуществление подготовки и аттестации научно-педагогических кадров высшей квалификации в соответствии с учебно-научным профилем университета;
5) Разработка новых методов и технологий подготовки кадров, обеспечивающих эффективную интеграцию РФ в мировое сообщество.

Университет в соответствии с порядком, установленным действующим законодательством РФ, выполняет следующие функции:

1) Определяет перечень специализаций и специальностей, а также направлений научных исследований по профилю университета во взаимодействии с заинтересованными

ведомствами и министерствами, организациями и предприятиями на основе изучения потребностей народного хозяйства в специалистах.

2) Разрабатывает и реализует целевые программы в области высшего образования, науки и техники в соответствии со своими профилем совместно с заинтересованными ведомствами и министерствами, организациями и предприятиями.

3) Проводит инновационную политику в области технологий обучения, направленную на эффективную реализацию целей высшего, послевузовского профессионального и соответствующего дополнительного образования, развитие творческой активности научно-педагогических работников и студентов.

Ниже представлены расшифровки аббревиатур типовых подразделений высшего учебного заведения:

УМУ - Учебно-методическое управление;

КМО УМО - Координационно-методический отдел УМО;

УПК - Управление приемной комиссии;

УРф - Управление по работе с филиалами;

УМД - Управление международной деятельности;

УРП - Управление по работе с персоналом;

УИ - Управление по информатизации;

ЦСИКНУ - Центр сохранения историко-культурного наследия университета;

УРГОСО - Управление по работе с государственными органами и связям с общественностью;

ЦГП - Центр гуманитарной подготовки;

УО НИР - Управление организации НИР;

ЦРМП - Центр развития молодежного предпринимательства;

УПНК - Управление подготовки научных кадров;

ОРДС - Отдел по работе с диссертационными советами;

УСВР - Управление по социальной и воспитательной работе;

ЦРК - Центр развития карьеры;

УНЦППКРВШ - Учебно-научный центр по переподготовке и повышению квалификации работников высшей школы;

ПАУ - Прогнозно-аналитическое управление;

УОЗ - Управление организации закупок;

УКС - Управление капитального строительства;

УРСР - Управление ремонтно-строительных работ;

УЭ - Управление эксплуатации;

УХС - Управление хозяйственной службы;

УБ - Управление безопасности;

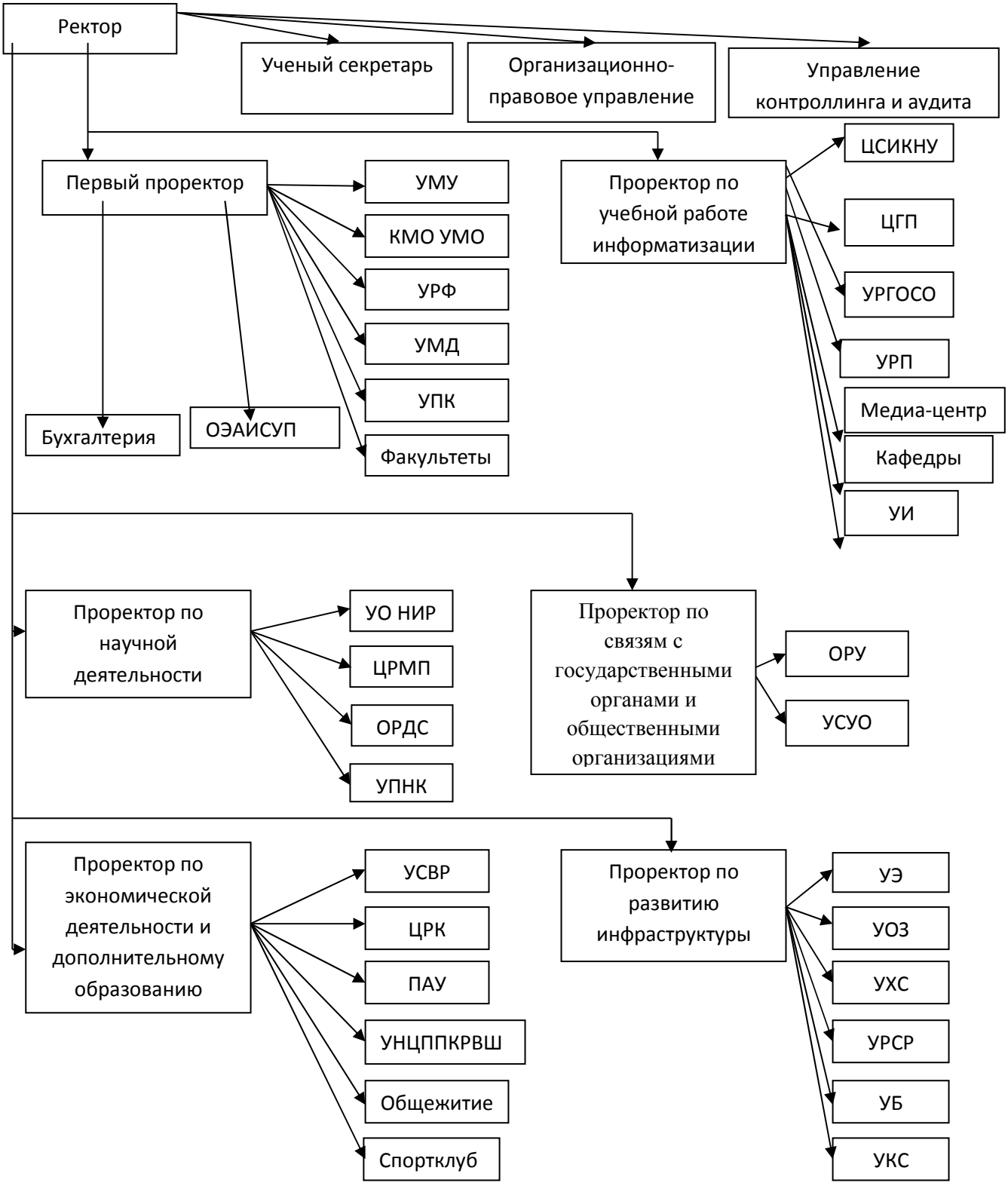
ОРУ - Операционно-расчетное управление;

УСУО - Управление сводного учета и отчетности;

ОПУ – организационно-правовое управление;

УКА – управление контроллинга и аудита.

Организационная структура ВУЗа



На основе анализа деятельности подразделений ВУЗа, а также самого университета в целом, составлен перечень типов информации, наиболее нуждающейся в защите:

- Персональные данные студентов и сотрудников (отдел кадров, бухгалтерия, отдел эксплуатации АИС учебного процесса, факультеты, кафедры);
- Информация об информационных технологиях, корпоративной сети, вычислительной сети, программном обеспечении, разработках в области информационных технологий, информационной системе университета (управление по информатизации);
- Бизнес-идеи студентов и сотрудников;
- Сведения о техническом обслуживании объектов и инженерных сетей (управление эксплуатации);
- Политика безопасности, результаты конфиденциальных совещаний (управление по безопасности).

Подлежащая защите информация хранится как в электронном, так и в бумажном виде на серверах университета, на персональных компьютерах сотрудников отделов и в архиве документов; с информацией работают сотрудники указанных отделов, и, соответственно, только сотрудники отделов имеют доступ к соответствующей информации.

Следующим этапом после определения информации, подлежащей защите, является разработка модели злоумышленника.

Модель злоумышленника — абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Модель злоумышленника включает в себя 4 основных пункта:

1. Цель злоумышленника;
2. Портрет злоумышленника;
3. Направления атаки;
4. Инструменты атаки.

Модель злоумышленника разрабатывается исходя из 4 видов угроз информации:

1. Блокирование.

При блокировании целью злоумышленника является создание условий для отсутствия или ограничения доступа пользователей информационной системы для последующего получения как материальной, так и нематериальной выгоды.

2.Копирование.

При копировании целью злоумышленника является нарушение конфиденциальности информации для последующего оглашения, использования в личных целях или продажи заинтересованным лицам.

3.Модификация.

При модификации целью злоумышленника является изменение информации в системе для причинения ущерба, получения выгоды либо иных личных интересов.

4.Уничтожение.

При уничтожении целью злоумышленника является невозможность восстановления информации ее владельцем для причинения материального и нематериального ущерба.

Для полного описания модели злоумышленника необходимо определить категорию нарушителя: внутренний или внешний злоумышленник.

Внутренним злоумышленником может быть лицо из следующих категорий сотрудников Университета:

- сотрудники факультетов и кафедр;
- сотрудники отдела кадров;
- сотрудники Управления информатизации;
- сотрудники Управления безопасности;
- руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями:

- уволенные сотрудники;
- технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположена информация);
- посетители (приглашенные представители организаций, представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);
- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
- лица, умышленно проникшие в сети университета из внешних (по отношению к ней) сетей телекоммуникации (хакеры).

Сотрудники Управления информатизации и Управления безопасности имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связаны с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или спецслужбами.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные знания и опыт выделяют их среди других источников внешних угроз.

Конкуренты и криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников ВУЗа всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в университете. Наибольшую угрозу представляют криминальные структуры и уволенные сотрудники при взаимодействии с ныне работающими.

Внешние информационные посредники (организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем) представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Конкуренты, криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к защищаемой информации.

Предлагается принять следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия исключают возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей – сотрудников университета по преодолению системы защиты;
- нарушитель скрывает свои несанкционированные действия от других сотрудников ВУЗа;
- несанкционированные действия могут быть следствием ошибок, как сотрудников факультетов, кафедр, так и сотрудников Управления информатизации, а также вследствие несовершенства и недостатков принятой технологии обработки, хранения и передачи информации;
- в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, а также адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

Из вышесказанного следует, что при разработке политики информационной безопасности учреждения, в том числе и ВУЗа, необходимо учитывать модель злоумышленника. Чем адекватнее будет модель, тем более полно будет организована защита конфиденциальных данных. Таким образом, построение модели злоумышленника является существенным звеном в организации политики безопасности информационной безопасности на предприятии.

Список литературы

1. Алексеев Е.Г., Богатырев С.Д. Информатика. Мультимедийный электронный учебник [Электронный ресурс]. — Режим доступа: http://inf.e-alekseev.ru/text/Politics_inf_bezopas.html (дата обращения: 13.04.14).

2. Блинов А.М. Информационная безопасность: Учебное пособие. – Часть 1. – М.: СПбГУЭФ, 2010.
3. Гладких А.А., Дементьев В.Е. Базовые принципы информационной безопасности вычислительных сетей: учебное пособие для студентов. – М.: УлГТУ, 2009.
4. Мордвинов В.А., Фомина А.Б. Защита информации и информационная безопасность. – М.: МГДД(Ю)Т, МИРЭА, ГНИИ ИТТ «Информика», 2003/2004.
5. Петренко С.А., Курбатов В.А. Политики информационной безопасности. – М.: Компания АйТи, 2006.
6. Цуканова О.А., Смирнов С.Б. Экономика защиты информации: Учебное пособие. – М.: СПб ГУИТМО, 2007.

Рецензенты:

Тихомиров Н.П., д.э.н., профессор, заведующий кафедрой Математические методы в экономике ФГБОУ ВПО «Российский экономический университет имени Г.В. Плеханова» Министерства образования и науки РФ, г. Москва.

Татарников О.В., д.т.н., профессор, заведующий кафедрой Высшей математики ФГБОУ ВПО «Российский экономический университет имени Г.В. Плеханова» Министерства образования и науки РФ, г. Москва.