Учреждение образования

«Белорусский Государственный Технологический Университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

Электронный конспект по дисциплине

«Основы защиты информации»

Выполнил:

Студент 2 курса 4 группы

Карленок Юрий

Минск 2019

**Практическое занятие №3**

**Тема «Разработка политики информационной безопасности университета»**

Цель: Разработать проект политики информационной безопасности университета.

**Введение**

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

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:

* проведение профессиональной ориентации, довузовской подготовки и конкурсного отбора учащихся;
* обучение студентов;
* проведение последипломной подготовки и повышения квалификации;
* осуществление подготовки и аттестации научно-педагогических кадров высшей квалификации в соответствии с учебно-научным профилем университета;
* 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:

* 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;
* 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;
* 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.

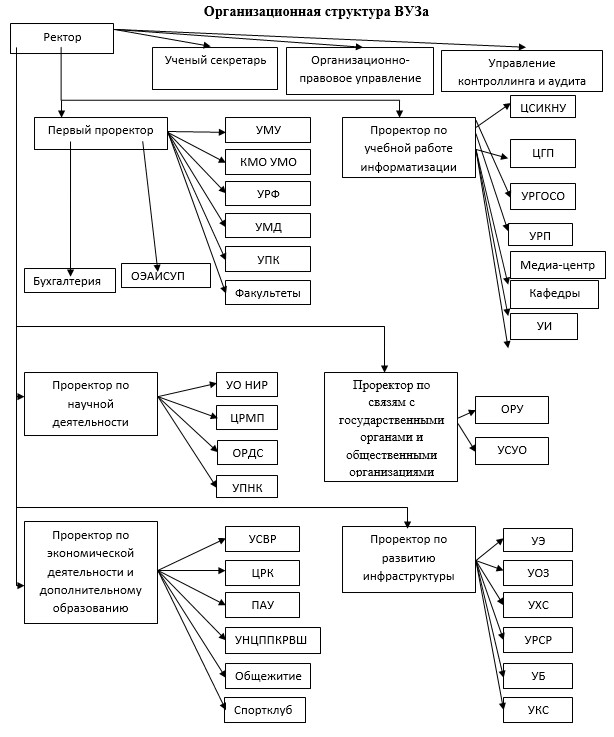


Рисунок 3.1 - Организационная структура ВУЗа

* 1. **Специфика образовательных учреждений**

В современном вузе хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация.

Рост количества преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей учебных заведений и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательного учреждения. Эти составляющие определяют единую политику обеспечения безопасности информации в вузе.

Специфика защиты информации в образовательной системе заключается в том, что вуз – публичное заведение с непостоянной аудиторией, а также место повышенной активности «начинающих киберпреступников».

Основную группу потенциальных нарушителей в вузе составляют студенты, ряд из них имеют достаточно высокий уровень подготовки. Возраст (от 18 до 23 лет) и юношеский максимализм побуждают таких людей блеснуть знаниями перед сокурсниками: устроить вирусную эпидемию, получить административный доступ и «наказать» преподавателя, заблокировать выход в Интернет и т. д. Достаточно вспомнить, что первые компьютерные правонарушения родились именно в вузе (червь Морриса) [4].

Особенности вуза как объекта информатизации связаны также с многопрофильным характером деятельности, обилием форм и методов учебной работы, пространственной распределенностью инфраструктуры (филиалы, представительства). Сюда же можно отнести и многообразие источников финансирования, наличие развитой структуры вспомогательных подразделений и служб (строительная, производственная, хозяйственная деятельность), необходимость адаптации к меняющемуся рынку образовательных услуг, потребность в анализе рынка труда, отсутствие общепринятой формализации деловых процессов, необходимость электронного взаимодействия с вышестоящими организациями, частое изменение статуса сотрудников и обучаемых.

Несколько облегчает проблему то, что вуз представляет собой стабильную, иерархическую по функциям управления систему, обладающую всеми необходимыми условиями жизнедеятельности и действующую на принципах централизованного управления (последнее означает, что в управлении задачами информатизации может активно использоваться административный ресурс).

Указанные выше особенности обусловливают необходимость соблюдения следующих требований:

* комплексная проработка задач информационной безопасности, начиная с концепции и заканчивая сопровождением программно-технических решений;
* привлечение большого числа специалистов, владеющих содержательной частью деловых процессов;
* использование модульной структуры корпоративных приложений, когда каждый модуль покрывает взаимосвязанную группу деловых процедур или информационных сервисов при обеспечении единых требований к безопасности;
* применение обоснованной последовательности этапов в решении задач информационной безопасности;
* документирование разработок на базе разумного применения стандартов, что гарантирует создание успешной системы;
* использование надежных и масштабируемых аппаратно-программных платформ и технологий различного назначения, обеспечивающих необходимый уровень безопасности.

С точки зрения архитектуры в корпоративной информационной среде можно выделить три уровня, для обеспечения безопасного функционирования которых необходимо применять различные подходы:

* оборудование вычислительной сети, каналов и линий передачи данных, рабочих мест пользователей, системы хранения данных;
* операционные системы, сетевые службы и сервисы по управлению доступом к ресурсам, программное обеспечение среднего слоя;
* прикладное программное обеспечение, информационные сервисы и среды, ориентированные на пользователей.

При создании комплексной информационной сети (КИС) необходимо обеспечить межуровневое согласование требований по безопасности к выбираемым решениям или технологиям. Так, на втором уровне архитектура КИС многих вузов представляет собой разрозненные и слабо связанные подсистемы с разными операционными средами, согласованные друг с другом только на уровне закрепления IP-адресов или обмена сообщениями. Причинами плохой системной организации КИС является отсутствие утвержденной архитектуры КИС, наличие нескольких центров ответственности за развитие технологий, которые действуют несогласованно. Проблемы начинаются с нежелания управлять выбором операционных сред в подразделениях, когда ключевые технологические решения полностью децентрализованы, что резко снижает уровень безопасности системы.

Вузы, имеющие четкую стратегию развития информационных технологий, единые требования к информационной инфраструктуре, политику информационной безопасности и утвержденные регламенты на основные компоненты КИС, отличаются, как правило, сильным административным ядром в управлении и высоким авторитетом руководителя ИТ-службы.

В таких вузах могут, конечно, использоваться различные операционные среды или системы среднего слоя, но это обусловлено организационно-техническими или экономическими причинами и не препятствует развертыванию КИС вуза и внедрению унифицированных принципов безопасного доступа к информационным ресурсам.

Состояние развития в вузах третьего уровня архитектуры КИС можно охарактеризовать следующим образом: в основном завершен переход от локальных программных приложений, автоматизирующих отдельный деловой процесс и опирающихся на локальный набор данных, к корпоративным клиент-серверным информационным системам, обеспечивающим доступ пользователей к оперативным базам данных вуза. В том или ином виде решена задача интеграции данных, порожденных различными информационными системами, что позволяет усовершенствовать бизнес-процессы, повысить качество управления и принятия решений.

Если в начале 90-х гг. XX в. был высокий спрос на бухгалтерское программное обеспечение и программное обеспечение управленческого учета (учет кадров, отчетность и т. д.), то в настоящее время этот спрос в большей части удовлетворен. В настоящее время стоит задача обеспечить достоверными данными о деятельности образовательного учреждения не только управленческий персонал, но и каждого преподавателя и студента, т. е. задача эффективного управления данными, циркулирующими в КИС, что, в свою очередь, делает задачу обеспечения информационной безопасности в таких сетях еще более актуальной.

* 1. **Информационная безопасность корпоративных сетей вузов**

Активное внедрение Интернета и новых информационных технологий в образовательный процесс и систему управления вузом создало предпосылки к появлению корпоративных сетей.

Корпоративная сеть вуза – это информационная система, включающая в себя компьютеры, серверы, сетевое оборудование, средства связи и телекоммуникации, систему программного обеспечения, предназначенную для решения задач управления вузом и ведения образовательной деятельности.

Корпоративная сеть обычно объединяет не только структурные подразделения вуза, но и их региональные представительства. Ранее недоступные для вуза, в настоящее время эти сети стали активно внедряться в образовательные структуры в связи с массовым распространением Интернета и его доступностью.

Комплексная информационная безопасность вуза – система сохранения, ограничения и авторизованного доступа к информации, содержащейся на серверах в корпоративных сетях вузов, а также передаваемая по телекоммуникационным каналам связи в системах дистанционного обучения.

В более широком смысле термин «комплексная информационная безопасность вуза» включает в себя два аспекта: систему защиты интеллектуальной информационной собственности вуза от внешних и внутренних агрессивных воздействий и систему управления доступом к информации и защиты от агрессивных информационных пространств. В последнее время, в связи с неконтролируемым массовым развитием Интернета, последний аспект безопасности становится особенно актуальным.

Под термином «информационное пространство» понимается информация, содержащаяся на серверах в корпоративных сетях учебных заведений, учреждений, библиотек и в глобальной сети Интернет, на электронных носителях информации, а также передаваемая по телевизионным каналам связи или по телевидению.

Агрессивное информационное пространство – это информационное пространство, содержание которого может вызвать проявления агрессии у пользователя как сразу же после информационного воздействия, так и через некоторое время (отдаленный эффект).

Проблемы комплексной информационной безопасности корпоративных сетей вузов гораздо шире, разнообразнее и острее, чем в других системах. Это связано со следующими особенностями:

* корпоративная сеть вуза строится обычно на концепции «скудного финансирования» (оборудование, кадры, нелицензионное программное обеспечение);
* как правило, корпоративные сети не имеют стратегических целей развития. Это значит, что топология сетей, их техническое и программное обеспечение рассматриваются с позиций текущих задач;
* в одной корпоративной сети вуза решаются две основные задачи: обеспечение образовательной и научной деятельности и решение задачи управления образовательным и научным процессами. Это означает, что одновременно в этой сети работает несколько автоматизированных систем или подсистем в рамках одной системы управления (АСУ «Студент», АСУ «Кадры», АСУ «Учебный процесс», АСУ «Библиотека», АСУ «НИР», АСУ «Бухгалтерия» и т. д.);
* корпоративные сети гетерогенны как по оборудованию, так и по программному обеспечению в связи с тем, что создавались в течение длительного времени для разных задач;
* планы комплексной информационной безопасности, как правило, либо отсутствуют, либо не соответствуют современным требованиям.

В такой сети возможны как внутренние, так и внешние угрозы безопасности информации:

* попытки несанкционированного администрирования баз данных;
* исследование сетей, несанкционированный запуск программ по аудиту сетей;
* удаление информации, в том числе библиотек;
* запуск игровых программ;
* установка вирусных программ и троянских коней;
* попытки взлома АСУ «ВУЗ»;
* сканирование сетей, в том числе других организаций, через Интернет;
* несанкционированная откачка из Интернета нелицензионного софта и установка его на рабочие станции;
* попытки проникновения в системы бухгалтерского учета;
* поиск «дыр» в OC, firewall, Proxy-серверах;
* попытки несанкционированного удаленного администрирования ОС;
* сканирование портов и т. п.
  1. **Анализ угроз, их источников и рисков**

Источниками возможных угроз информации являются:

* компьютеризированные учебные аудитории, в которых проходит учебный процесс;
* Интернет;
* рабочие станции неквалифицированных в сфере информационной безопасности работников вуза.

Анализ информационных рисков можно разделить на следующие этапы:

* классификация объектов, подлежащих защите, по важности;
* определение привлекательности объектов защиты для взломщиков;
* определение возможных угроз и вероятных каналов доступа на объекты;
* оценка существующих мер безопасности;
* определение уязвимостей в обороне и способов их ликвидации;
* составление ранжированного списка угроз;
* оценка ущерба от несанкционированного доступа, атак в отказе обслуживании, сбоев в работе оборудования. Основные объекты, нуждающиеся в защите от несанкционированного доступа:
* бухгалтерские ЛВС, данные планово-финансового отдела, а также статистические и архивные данные;
* серверы баз данных;
* консоль управления учетными записями;
* www/ftp-серверы;
* ЛВС и серверы исследовательских проектов.

Как правило, связь с Интернетом осуществляется сразу по нескольким линиям связи (оптоволоконная магистраль, спутниковые и радиоканалы). Отдельные каналы предоставляются для связи с другими университетами или для безопасного обмена данными.

Чтобы исключить риски, связанные с утечкой и порчей передаваемой информации, такие сети не должны подключаться к глобальным сетям и общей университетской сети.

Критически важные узлы для обмена данными университета (например, бухгалтерская ЛВС) также должны существовать отдельно.

* 1. **Рубежи защиты**

Первый рубеж обороны от атак извне (Интернет) – роутер (маршрутизатор). Он применяется для связи участков сети друг с другом, а также для более эффективного разделения трафика и использования альтернативных путей между узлами сети. От его настроек зависит функционирование подсетей и связь с глобальными сетями (WAN). Его главная задача в плане безопасности – защита от распределенных атак в отказе обслуживания (DDOS).

Вторым рубежом может служить межсетевой экран (МСЭ): аппаратно-программный комплекс Cisco PIX Firewall.

Затем следует демилитаризованная зона (DMZ). В этой зоне необходимо расположить главный прокси-сервер, dns-сервер, www/ftp, mail-серверы. Прокси-сервер обрабатывает запросы от рабочих станций учебного персонала, серверов, не подключенных напрямую к роутеру, и фильтрует трафик. Политика безопасности на этом уровне должна определяться блокированием нежелательного трафика и его экономией (фильтрация мультимедиаконтента, iso-образов, блокировка страниц нежелательного/нецензурного содержания по ключевым словам). Чтобы не происходило скачивания информации, зараженной вирусами, на этом сервере оправдано размещение антивирусных средств.

Информация от прокси-сервера должна параллельно отсылаться на сервер статистики, где можно посмотреть и проанализировать деятельность пользователей в Интернете. На почтовом сервере обязательно должен присутствовать почтовый антивирус, например Kaspersky AntiVirus for Mail servers.

Так как эти серверы связаны непосредственно с глобальной сетью, аудит программного обеспечения, установленного на них, – первоочередная задача инженера по информационной безопасности вуза. Для экономии средств и гибкости настраивания желательно применять opensource ОС и программное обеспечение.

Одни из самых распространенных ОС – FreeBSD и GNU Linux. Но ничто не мешает использовать и более консервативную Open BSD или даже сверхстабильную ОС реального времени – QNX.

Для централизованного управления антивирусной деятельностью необходим продукт с клиент-серверной архитектурой, такой как Dr.Web Enterprise Suite. Он позволяет централизованно управлять настройками и обновлением антивирусных баз с помощью графической консоли и предоставлять удобочитаемую статистику о вирусной деятельности, если таковая присутствует.

Для большего удобства работников вуза можно организовать доступ к внутренней сети университета с помощью технологии VPN.

Некоторые университеты имеют свой пул дозвона для выхода в Интернет и используют каналы связи учреждения. Во избежание использования этого доступа посторонними лицами в незаконных целях работники учебного заведения не должны разглашать телефон пула, логин, пароль.

Степень защищенности сетей и серверов большинства вузов России оставляет желать лучшего. Причин тому много, но одна из главных – плохая организация мер по разработке и обеспечению политики информационной безопасности и недооценка важности этих мероприятий. Вторая проблема заключается в недостаточном финансировании закупок оборудования и внедрения новых технологий в сфере информационной безопасности.

* 1. **Структура системы комплексной информационной безопасности вуза**

Система комплексной информационной безопасности должна включать в себя выработку следующих политик.

Прежде всего, это финансовая политика развертывания, развития и поддержания в актуальном состоянии корпоративной сети вуза. Она является доминирующей и ее можно разделить на три направления: скудное финансирование, финансирование с разумной достаточностью и приоритетное финансирование.

Вторая политика определяется уровнем организации развертывания и сопровождения корпоративной сети вуза.

Третья политика относится к кадровому составу информационного центра. Для вуза она особенно актуальна в связи с повышенной востребованностью опытных сисадминов.

Политика программного обеспечения в настоящее время – один из затратных факторов развития корпоративной сети. Рациональные подходы к его решению в условия монопольного рынка ОС и программных продуктов MicroSoft – это отдельный вопрос, требующий внимательного рассмотрения.

Политика технического обеспечения, может быть, не вполне актуальна в условиях достаточного финансирования. Но всегда существует проблема обновления устаревшего оборудования.

Наконец, последняя политика связана с формирование морально-этических норм толерантного поведения в информационных системах и разумного ограничения от посещений агрессивных информационных пространств. Недооценка этих направлений будет компенсироваться повышенными финансовыми затратами на сопровождение корпоративных сетей вузов.

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:

* Цель злоумышленника;
* Портрет злоумышленника;
* Направления атаки;
* 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.

**Вывод:** 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.