**«УТВЕРЖДАЮ»**
Ректор «Astana IT University»
_____ Қ. Қожахмет
«_____» _____ 2019 г.

# МОДЕЛЬ ВЫПУСКНИКА «ASTANA IT UNIVERSITY»

**Бакалавр по образовательной программе**
**6B06301 «Cyber Security» (Кибербезопасность)**

г. Нур-Султан, 2019

**СОДЕРЖАНИЕ**

## ВВЕДЕНИЕ

Разработка компетентностной модели выпускника становится безусловным условием для реализации основных направлений Болонского процесса и требованием современного рынка труда. Компетентностная модель выпускника (бакалавриат) призвана отвечать на вопрос о том, какие профессиональные задачи должен уметь решать специалист определенного ранга (должности), того или иного профиля. Формирование современной модели выпускника вуза, отвечающая запросам стейкхолдеров и всех заинтересованных лиц, является главной стратегической целью «Astana IT University» и обеспечивается необходимыми ресурсами для образовательного процесса, включающее кадровое, учебно-методическое, информационное и материально-техническое обеспечение. Университет ведет целенаправленную кадровую политику и планомерное улучшение материально технической базы университета для обеспечения качества подготовки выпускника - бакалавра, востребованного на рынке труда.

Нормативно-правовая база модели выпускника - бакалавра по специальностям Университета основывается на следующих документах:

- Закон Республики Казахстан «Об образовании» № 319-III от 27 июля 2007 года (с изменениями и дополнениями на 11.07.2017г.)
- Государственная программа развития образования РК на 2011-2020 годы, утвержденная Указом Президента РК № 1118 от 07.12.2011 г.
- ГОСО высшего и послевузовского образования № 604 от 31. 10. 2018 г.
- Правилами «Организация учебного процесса по кредитной технологии обучения» (№ 152 от 20.04.2011г. с изменениями и дополнениями № 563 от 12. 10. 2018)
- Типовые правила деятельности организаций образования, реализующих образовательные программы высшего образования. Постановление Правительства Республики Казахстан от 7 апреля 2017 года № 181. Квалификационный справочник должностей руководителей, специалистов и других служащих, утвержденного приказом Министра труда и социальной защиты населения Республики Казахстан от 21 мая 2012 года № 201-п-м с изменениями от с изменениями от 17.04.2013 г.)

## 1. 6B06301 «Cyber Security» (Кибербезопасность). Развитие и перспективы

Кибербезопасность - это практика защиты компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от вредоносных атак. Это также известно как безопасность информационных технологий или электронная защита информации. Этот термин применяется в различных контекстах, от бизнеса до мобильных компьютеров, и может быть разделен на несколько общих категорий.

Задачи Кибербезопасности включает следующее:

1) Обеспечение защиты информации и объектов информатизации с помощью стандартов и протоколов сетевого взаимодействия.
2) Проведение мониторинга, анализа и сравнения эффективности программно-аппаратных средств защиты информации в операционных системах и сетях.
3) Проведение корректности работы администрирования системы и программно-аппаратных средств защиты.
4) Проведение постоянного мониторинга и контроля защищенности информации, определения угроз, уязвимости, рисков в области безопасности Интернета вещей.
5) Разработка, проектирование и сопровождение средств сетевой безопасности организации.
6) Оценивание уровня безопасности компьютерных систем и сетей организации и подготовка сопроводительной документации.

По данным Бюро статистики труда США, темпы роста занятости в сфере информационной безопасности прогнозируются на уровне 37% в 2012–2022 гг., Что намного быстрее, чем в среднем по всем другим профессиям. А так же, согласно исследованию PwC «Global Economic Crime Survey», киберпреступность заняла второе место по количеству зарегистрированных экономических преступлений после незаконного присвоения активов. Попадание в кибер-атаки может быть очень дорогостоящим занятием для организации. Чтобы уменьшить эти риски, спрос на экспертов по кибербезопасности возрастает.

В данном случае, можно рассмотреть пять отраслей, которые жаждут профессионалов в области кибербезопасности:

- Банковское дело и финансы
- Правительство
- Здравоохранение
- Производство

Для выпускников бакалавриата существует широкий спектр профессий в сфере кибербезопасности. Вот некоторые из областей, в которые вы можете войти после получения степени бакалавра в области кибербезопасности:

- Аналитик информационной безопаности

В целях защиты компьютерных сетей от кибератак, организациям нужны аналитики информационной безопасности, которые могут разрабатывать и внедрять системы ИТ-безопасности, а также разработать лучшие для всей организации передовые практики в области безопасности.

Задача Аналитика информационной безопасности заключаются в следующем:

Мониторинг сетей своей организации на наличие нарушений безопасности и расследование нарушений при их возникновении

Установки и использования программного обеспечение, таких как брандмауэры и программы шифрования данных, для защиты конфиденциальной информации.

Подготовка отчетов, которые документируют нарушения безопасности и степень ущерба, вызванного нарушениями

Проведения тестирования проникновения, когда аналитики имитируют атаки, чтобы найти уязвимости в своих системах, прежде чем их можно будет использовать

Исследование последних тенденции в области безопасности информационных технологий

Разработка стандартов безопасности и лучших практик для их организации

- Тестировщик информационной безопасности

Это специалист, который занимается тестированием программного обеспечения с целью выявления ошибок в его работе и их последующего исправления. Тестирование информационной безопасности - это практика тестирования платформ, сервисов, систем, приложений, устройств и процессов на наличие уязвимостей информационной безопасности.

Некоторые обязанности Тестировщика информационной безопасности включают в себя:

Создание новых тестов для выявления уязвимостей в нескольких системах

Использование тестов физической безопасности и идентифицируйте области, которые нуждаются в физической защите

Найти уязвимости в популярных, распространенных программах, а также в проприетарных приложениях

Определение точки входа для хакеров

Использование социальной инженерии для выявления улучшений в сфере безопасности и образования

Усовершенствование текущих аппаратных и программных обеспечений за счет реализации лучших стандартов безопасности

- Менеджер по управлению инфомрационной безопасностью

Менеджер по управлению информационной безопасностью отвечает за контроль и координацию программы по управлению, рискам и соответствию. Менеджер должен обладать экспертными знаниями в области систем ISO 27001, PCI DSS и NIST 800-53. А также, необходимы практические знания по GDPR, SOC 1 / II, COBIT и другим отраслевым стандартам и правилам.

В задачи Менеджера входит следующее:

обеспечить соответствие требований безопасности бизнес-потребностям, организационной структуре, ролям и обязанностям

проводить измерение эффективности Системы управления информационной безопасностью (СУИБ)

определять задачи и обеспечивать механизмы контроля

определять и сообщать об эффективности мер безопасности и поддерживать усилия по улучшению состояния безопасности организации

руководить группой управления для достижения поставленных целей, оценивать риски развертывания и реализовывать стратегии для обеспечения успешного выполнения программы

## 2. Составные компоненты при формировании модели выпускника образовательной программы

Ключевые компоненты формирования Модели выпускника образовательной программы включают информацию о целях и задачах образовательной программы, объектах, видах и направлениях профессиональной деятельности, компетентностную модель специалиста (Приложение 1), включая дескрипторы, разновидность компетенций в соответствии с образовательной программой, результаты образовательной программы.

### 2.1 Цели Образовательной программы:

Обеспечить практико-ориентированную подготовку высококвалифицированных специалистов в области кибербезопасности предприятий, обладающих общекультурными и профессиональными компетенциями в сфере информационной безопасности, а также создать условия для непрерывного профессионального самосовершенствования, развития социально-личностных компетенций специалистов, расширения социальной мобильности и конкурентоспособности на рынке труда.

### 2.2 Задачи Образовательной программы:

– подготовка нового конкурентоспособного поколения технических специалистов в области радиотехники, электроники и телекоммуникаций для рынка труда, инициативного, умеющего работать в команде, обладающего высокими личностно-профессиональными компетенциями;

– интеграция образовательной и научной деятельности;

– установление партнерства с ведущими вузами ближнего и дальнего зарубежья с целью улучшения качества образования, для поддержки технических и культурных связей;

– расширение связей с заказчиками образовательных услуг, работодателями с целью определения требований к качеству подготовки специалистов, проведению курсов, семинаров, мастер-классов, стажировок, производственных практик.

### 2.3 Общие и профессиональные компетенции

Общими и профессиональными компетенциями, как результатами обучения, являются знания, навыки и умения, полученные по завершению дисциплины или курса и отражающие требования.

*Общие компетенции:*

- Обладать необходимыми знаниями в области информационных технологий и кибербезопасности, и понимать возможность их применения в прикладных областях.
- Знать принципы обработки, анализа и представления данных и уметь использовать их для детализации в различных областях.
- Способность анализировать требования к предметной области, возможности построения или модернизации информационных технологий при обосновании результатов анализа с помощью методов исследования и инструментов моделирования.
- Способность быть компетентным при выборе методов ИКТ и математического моделирования для решения конкретных инженерных задач, способность быть готовым выявить естественнонаучную сущность проблем, возникающих в процессе профессиональной деятельности, и способностью привлечь для ее решения соответствующий математический аппарат.

*Профессиональные компетенции:*

- Способность найти (выбрать) оптимальные решения при создании новых продуктов с учетом требований качества, стоимости, сроков исполнения, конкурентоспособности и экологической безопасности
- Понимание архитектуры информационных систем
- Способность применять теории и методы теоретического и прикладного Кибербезопасности, систем и стратегий управления, управления и использования стандартов информационной безопасности на предприятии
- Способность решать профессиональные задачи на основе истории и философии нововведений, математических методов и моделей для управления IT-инновациями, компьютерных технологий в сфере информационной безопасности
- Способность формировать и развивать коммуникативные умения и компетенции в области организации, планирования и управления производством, способность применять полученные знания для осмысления окружающей экологической действительности, способность обобщать, анализировать, прогнозировать при постановке целей в профессиональной сфере и выбирать пути их достижения с применением научной методологии исследования
- Способность разработать план и программу организации работ по защите информации
- Способность применять теорию и методы математики для построения качественных и количественных моделей объектов и процессов в естественно-научной сфере деятельности, способность выбирать и применять подходящее оборудование, инструменты и методы исследований для решения задач в области кибербезопасности, способность настраивать и налаживать программно-аппаратные комплексы, способность сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем.

**2.4 Матрица соотнесения результатов обучения образовательной программы с формируемыми компетенциями**

| | РО1 | РО2 | РО3 | РО4 | РО5 | РО6 | РО7 | РО8 | РО9 | РО10 | РО11 | РО12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ПК1** | V | | | | | | | | | | | V |
| **ПК 2** | | V | | | | V | V | | | | | |
| **ПК 3** | | V | V | V | V | | | | | | | |
| **ПК 4** | | | | V | V | V | V | | | | | |
| **ПК 5** | | | | V | | | | | | | | |
| **ПК 6** | | | | | V | | | | | | | V |
| **ПК 7** | | | | | | V | V | | | | | V |
| **ПК 8** | | | | | | | | V | V | V | V | V |
| **ПК 9** | | | | | | | | | V | V | V | V |

**2.5Личностные качества менеджера по информационной безопасности**

– Аналитические умения: умение проводить системный анализ информации; систематизировать информацию; сравнивать данные; абстрагировать информацию; проектировать результат.

– Диагностические умения: умение структурировать полученную информацию; осуществлять инновационные и комбинационные процессы, связанные с умением прогнозирования; определять стратегические, тактические и оперативные цели; формулировать и решать профессиональные задачи; выбирать, модифицировать и разрабатывать новые методы работы; использовать позитивный опыт; принимать управленческие решения; диагностировать возможные варианты решений.

– Вербальные и невербальные навыки: умение выстраивать деловые отношения с коллегами; устанавливать сотрудничество с партнёрами; формулировать профессиональные задачи; владеть устной и письменной речью; свободно владеть Европейским языком; схватывать мысль и суть на лету;ориентироваться в том, что уже известно и в том, что ещё не известно; стратегически мыслить и логически предвидеть развитие событий;решать нестандартные проблемы, используя оригинальные приёмы и средства;определять важное в экстремальных ситуациях.

– Прогностические умения: уверенность в собственных действиях в соответствии с оценкой всего происходящего; проявление экстравертности и доминирования, как условие целеустремлённости, управления, моделирования информации, мобилизации энергии, проявления настойчивости, активности, умения выдерживать нагрузку, упорства при выполнении сложных заданий.

– Коррекционные умения: умение осуществлять самоанализа, самокоррекцию; определять траектории саморазвития и самообразования; осмысливать собственные профессиональные и личностные возможности.

**Выводы**

Рыночная экономика Казахстана все больше переходит от стихийных форм организации к плановым. Кибербезопасность по результатам становится ведущей

доктриной управления в бизнесе. Многие компании рассматривают организационную «культуру, как важный регуляторный механизм в организационном окружении». В этой связи изменилось отношение к персоналу компании со стороны работодателей.

Однако профессиональные знания и опыт не есть единственное требование, соответствие которому обеспечивает специалисту вход в компанию. Последнее положение особенно касается молодых выпускников, у которых наличие знаний, приобретенных в университетах, не подтверждено опытом решения производственных или управленческих задач. Отсутствие такого опыта резко понижает преимущества молодых при найме на работу и определении стоимости их труда. Слишком велики риски работодателей. Это с одной стороны. С другой – важным критерием успешного прохождения конкурса на вакансию является оценка личностного потенциала молодого выпускника вуза. Что входит в понятие потенциала, являющегося гарантом инвестиций при формировании кадрового резерва? Что ждут работодатели от молодых специалистов, только что закончивших вуз? Что может сделать неопытных выпускников конкурентоспособными в глазах работодателей?

- Желание использовать молодую энергию, активность, открытость новому, динамичность
- Возможность использовать молодой потенциал за меньшую плату
- Легкая интеграция в организационную культуру предприятия

Не смотря на все это, выпускник должен обладать базовыми знаниями по информационным технологиям, деловому этикету, и др.

Несмотря на признание несомненных преимуществ молодых специалистов, работодатели не торопятся комплектовать ими кадровый состав своих предприятий. Чего же, кроме опыта, молодым выпускникам не хватает, по мнению работодателей?

- В них нет стабильности и надежности. Молодые выпускники, особенно те, которые раньше вообще не работали, быстро меняют свое первое рабочее место, рассматривая его именно как первое и отнюдь не последнее, как место, где можно перебиться первое время. Поэтому работодатели и не торопятся вкладывать деньги, время, усилия в тех, кто быстро может уйти.
- Молодым не хватает ответственности. У тех, кто не имел раньше опыта, нет сформированной привычки ходить на работу и выполнять порученные задачи, соблюдать элементарные нормы делового этикета. Они ориентированы на себя, а не на дело (свободное время и вообще времяпрепровождение важнее, чем суть дела компании).
- Нет умения работать на результат (а это значит, «держать» цель, находить пути преодоления препятствий на пути к ней, проявлять самостоятельность и настойчивость). Не видят взаимосвязей между своей работой и результатом (в том числе, и финансовым) деятельности компании, не видят того, как от порученной им работы зависят другие этапы и звенья работы всего предприятия.
- Нет адекватности в восприятии себя как работника: завышенные ожидания и по зарплате, и по оценке своего труда, и по характеру работы, которую хотят выполнять.

На основе вышесказанного можно сделать вывод, что для работодателей принципиальными моментами в вопросе, принимать или не принимать молодого выпускника на работу, являются, помимо специальных знаний, личностные качества потенциального работника (восприимчивость, динамичность, готовность учиться, готовность начинать с малого). И даже наличие предыдущего опыта, по ответам

работодателей, необходимо как некий «социальный опыт работы», как показатель ответственности и надежности. Что касается высшего образования, то работодатели расценивают его как признак, который априори отличает выпускника вуза от тех, кто высшим образованием не обладает.

Таким образом, работодатели рассматривают в целом молодого выпускника вуза как источник активности, динамичности и современных знаний для предприятия, с одной стороны, а с другой стороны, как тревожное сочетание пониженной ответственности с повышенными амбициями. Работодатели, решая вопрос, принять или не принять молодого выпускника на работу, исходят в принципе из наличия у выпускника одного из двух рыночных преимуществ:

Специальные знания, рыночный спрос на которые высок и которые не могут быть компенсированы личностными качествами (знания в области IT). Специальные знания делают выпускников определенных специальностей априори конкурентоспособными.

Особые личностные качества, которые требуются в рыночной экономике и которые выделяют одного выпускника на фоне целого ряда его же однокурсников (тех, кто обладает теми же знаниями, но не обладает необходимыми качествами). Эти качества могут сделать конкурентоспособными своих носителей, даже если они получили специальность, предложение по которой превышает спрос.

**Приложение 1**

**Компетентностная модель выпускника (бакалавр Кибербезопасность)**