АКАДЕМИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ КАЗАХСТАН

Национальная школа государственной политики

на правах рукописи

Искаков Медет Болатбекулы

ОЦЕНКА РИСКОВ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННОМ АППАРАТЕ

Образовательная программа ««7М04120 – Государственное управление»
по направлению подготовки «7М041 Бизнес и управление»

Магистерский проект на соискание степени
магистра государственного управление

Научный руководитель _____ (подпись) Адалиев Н.К., магистр

Проект допущен к защите: «_____»_____20__г.

Директор Национальной
школы государственной
политики _____ (подпись) Абдыкаликова М.Н., к.п.н.

Нур-Султан, 2022

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ……..……... 3
ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ……... 4
ВВЕДЕНИЕ…… 5
1. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В ГОСУДАРСТВЕННОМ АППАРАТЕ……... 7
2. ТЕКУЩАЯ СИТУАЦИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ…….. 12
3. МИРОВЫЕ ТРЕНДЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ.. 20
4. ИНЦИДЕНТЫ ИБ В ГОСУДАРСТВЕННОМ СЕКТОРЕ…...
5. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ ……. 26
6. ПРЕДЛАГАЕМЫЕ МЕРЫ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ……..…….. 33
ЗАКЛЮЧЕНИЕ…… 39
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ……. 41

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей диисертации использованы ссылки на следующие нормативные документы:

Закон Республики Казахстан. Об информатизации: утвержденный 24 ноября 2015 года, № 418-V.

Постановление Правительства Республики Казахстан. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: утвержденное 20 декабря 2016 года, № 832.

Постановление Правительства Республики Казахстан. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): утвержденное 30 июня 2017 года, № 407.

Постановление Правительства Республики Казахстан. Об утверждении Плана мероприятий по реализации Концепции кибербезопасности («Киберщит Казахстана») до 2022 года: утвержденное 28 октября 2017 года, № 676.

Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан. Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности: утвержденный 3 июня 2019 года, № 111/НҚ.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИБ	– Информационная безопасности
АИК	– Анализ исходного кода
АПК	– Аппаратно-программный комплекс
АСУ ТП	– Автоматизированные системы управления технологическим процессом
ВПО	– Вредоносное Программное обеспечение
ГИК	– Глобальный индекс кибербезопасности
ГО	– Государственные органы
ГП ЦК	– Государственная программа «Цифровой Казахстан»
ГТС	– Акционерное общество «Государственная техническая служба»
ЕШДИ	– Единый шлюз доступа к Интернет
ИКТ	– Информационно-коммуникационные технологии
ИП	– Инвестиционное предложение
ИР	– Интернет-ресурс
ИС	– Информационная система
Испытание	– Испытание на соответствие требованиям информационной безопасности
ИТ	– Информационные технологии
КВОИКИ	–Критически важные объекты информационно-коммуникационной инфраструктуры
ККС	– Консультативный координационный совет по информационной безопасности
Концепция	– Концепция кибербезопасности «Киберщит Казахстана»
МОЗ	– Мониторинг обеспечения защиты
МОБФ	– Мониторинг обеспечения безопасного функционирования
МОИБ	– Мониторинг обеспечения информационной безопасности
МРИ	– Мониторинг реагирования на инциденты
МЦРИАП	– Министерство цифрового развития, инноваций и аэрокосмической промышленности
НКЦИБ	– Национальный координационный центр информационной безопасности
ОИ	– Объект информатизации
ОИ ЭП	– Объект информатизации «электронного правительства»
ООН	– Организация Объединенных Наций

ПО	– Программное обеспечение
РК	– Республика Казахстан
СЗИ	– Средства защиты информации
СНГ	– Содружество независимых государств
ФЭО	– Финансово-экономическое обоснование
ЦГО	– Центральные государственные органы
ЭИР	– Электронные информационные ресурсы

ВВЕДЕНИЕ

Общая характеристика работы.

В рамках данного магистерского проекта проводилось изучение основных рисков информационной безопасности существующих в государственном аппарате, ключевые аспекты способствующие возникновению данных рисков, анализ и их оценка, а также выработка мер, существенно способствующих их снижению и минимизации.

Актуальность и проблема исследования.

Информационная безопасность в общепринятом значении - это защита конфиденциальности, целостности и доступности информации.

Известно, что текущая тенденция скоростного развития цифровой сферы и ИКТ повышает прозрачность, улучшает подотчетность и противодействие коррупции, и в целом повышает эффективность деятельности государственных структуры. Учитывая, что на текущий момент мир стремительно движется к «инновационному» будущему, с повсеместным применением интеллектуальных цифровых решений, в государственном секторе это влечет за собой автоматизацию и совершенствование многих производственных процессов. При этом наряду с этим, уровень киберугроз и уязвимостей также непрерывно растет. С этой целью, для минимизации фактов несанкционированного доступа, защиты информации, содержащихся в объектах информатизации «электронного правительства» от утечки и предотвращения возможности злонамеренных действий, к решению вопросов информационной безопасности необходимо подходить комплексно.

Постоянные вызовы и тренд современности сигнализируют необходимость развития сетевых технологий и мощности применяемых технологичных оборудований, расширение информационного пространства и несомненно достижения высокого уровня обеспечения ИБ и реагирования на угрозы и инциденты. Зачастую, темп развития цифровизации может на порядок опережать всевозможные предпринимаемые меры информационной безопасности.

Таким образом, необходимо понимать, что обеспечение информационной безопасности должно идти параллельно или опережать развитие сферы цифровизации и ИКТ в государственном аппарате. По этой причине возникает существенная необходимость в комплексной оценке существующих в государственных органах рисков ИБ и разработке новых методов, способных вынести состояние защищенности и уровень информационной безопасности на качественно новый уровень.

Целью проведенного исследования является разработка мер по повышению уровня информационной безопасности в государственном секторе, с целью обеспечения безопасной инфраструктуры для деятельности государства, а также повышения уровня доверия общества и бизнеса к государству.

Задачи проекта.

Для достижения цели исследования необходимо решение поставленных задач:

1) проведение анализа состояния защищенности объектов информатизации «электронного правительства»;
2) изучение и оценка компетентности ответственных специалистов за информационную безопасность в государственных органах;
3) изучение и проведение анализа предпринимаемых мер в случае возникновения инцидентов информационной безопасности;
4) оценка осведомленности государственных служащих основополагающими принципами кибербезопасности;
5) выработка мер способствующих минимизировать риски ИБ и негативные факторы связанные с ними, а также максимизировать положительное их влияние.

Объектом магистерского исследования являются государственные органы.

Методы исследования: проведение испытаний на основании заполняемой анкеты-опросник о характеристиках ОИ ЭП на соответствие ее требованиям ИБ, изучение информационно-коммуникационной инфраструктуры государственных органов на предмет исполнения требований НПА и стандартов в области ИБ, действующих на территории РК,.

Гипотеза и ожидаемые результаты: по результатам реализации предложенных мер по минимизации рисков информационной безопасности в рамках решения задач обеспечения информационной безопасности и общественного правопорядка будет достигнуто следующее:

1) снижение рисков и угроз ИБ в государственном секторе;
2) повышение уровня общественного доверия и безопасности граждан;
3) эффективное предотвращение, выявление и реагирование на современные угрозы;
4) развитие кадрового потенциала в области информационной безопасности.

Практическая значимость. Реализация предлагаемых в данной магистерской работе мер по снижению рисков и угроз информационной безопасности в государственном секторе поспособствуют повышению защищенности используемых в государственных органах объектов информатизации. Так или иначе мероприятия в комплексе нацелены на оказание содействия в решении задач обеспечения общественного правопорядка и национальной безопасности.

1. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В ГОСУДАРСТВЕННОМ АППАРАТЕ

Настоящее время характеризуется очередным этапом научно-технической революции, высоким уровнем развития информационно--телекоммуникационных технологий и их интенсивным использованием населением, бизнесом, общественными и государственными органами в различных целях. На государственном уровне внедрены и продолжают внедряться такие инструменты как «электронное правительство» и Единая система электронного документооборота. Таким образом, наблюдается постепенный переход в электронный вид всей осуществляемой деятельности государственных органов. В государственных органах увеличивается объем информации, существующей только в цифровом виде. Этому способствуют внедряемые и эксплуатируемые объекты информатизации «электронного правительства», аппаратно-программные комплексы и информационные системы.

Развитие информационно-коммуникационных технологий неразрывно связано с наступившей эпохой «Четвертой промышленной революции» (Индустрия 4.0), характерными чертами которой являются полностью автоматизированные производства, с управлением всеми процессами в режиме реального времени и с учетом меняющихся внешних условий.

Основными ключевыми технологиями «Индустрии 4.0» несомненно являются:

- облачные вычисления;
- большие даные;
- робототехника, искусственный интеллект и машинное обучение;
- кибербезопасность;
- виртуальная и дополненная реальность;
- нтернет вещей;
- квантовые вычисления.

Вышеуказанные направления в совокупности приводит страны к переходу в эпоху «Индустрии 4.0» и обеспечивает новый уровень эффективности производства.

Немаловажным является и то, что пандемия короновируса COVID-19 оставляя за собой след крупного экономического ущерба, также способствует введению новых цифровых технологий в общество и экономику во всем мире.

Таким образом, развитие цифровых технологий в сегодняшнем мире меняет ранее устоявшиеся механизмы и принципы работы сфер государственного управления, экономики и общественной жизни. Цифровые технологии трансформируют финансовую среду, изменяя способы оказания платежных, сберегательных, кредитных услуг, а также субъектов, оказывающих эти услуги. Таким образом, это является основным фактором развития бизнеса и его конкурентоспособности. Спрос на внедрение новых инструментов информационных технологий в различных сферах неминуемо

растет, а для некоторых сфер цифровизация и вовсе становится безальтернативной. А виртуальное и удаленное взаимодействие и вовсе становится повседневностью.

Следует отметить, что высокие темпы развития информационно-коммуникационных технологий в Казахстане отмечены международными экспертами ООН, Международного союза электросвязи и Всемирного экономического форума.

Так, в отчете ООН по индексу развития «электронного правительства», оценивающий возможность государственного сектора в странах использования информационных технологий для предоставления государственных услуг, опубликованном в 2020 году, Казахстан занимает 29 место среди 193 стран мира.

В сегодняшнем мобильном и цифровом мире потребители ожидают, что у них будет доступ к цифровым услугам в любое время и в любом месте. Естественно, это относится ко всем аспектам их жизни, включая взаимодействие с правительственными учреждениями.

Организации государственного сектора вынуждены делать предоставление услуг гражданам более доступным и удобным, обеспечивая тот же уровень обслуживания, как тот, который пользователи обычно встречают в банках и магазинах. Мобильные устройства, социальные сети и другие инновационные технологии увеличивают ожидания граждан в отношении обслуживания клиентов в самых разных сферах. Как потребители, они привыкли к совершению покупок в одном месте и к быстрому и удобному обслуживанию. Соответственно, как граждане и налогоплательщики, они ожидают такого же быстрого доступа к информации и скорости обслуживания от государственного сектора.

Сегодняшние граждане, хорошо знакомые с цифровыми технологиями, ожидают, что услуги будут доступны тогда, когда они потребуются, причем по всем каналам. От простых процессов вроде получения адресной справки до замены водительского удостоверения или паспорта, и до получения помощи в качестве опекуна или лица, недавно потерявшего работу, - граждане все активнее требуют замены процедур, осуществляемых при личном визите, онлайн-процедурами для простых операций, а также упрощения и совершенствования обслуживания с помощью более сложных и требующих сложных согласований взаимодействий и услуг.

Граждане все в большей мере ждут персонализированных и предиктивных услуг, учитывающих события жизни или известные даты для принятия решений и оказания услуг в реальном времени. Это может быть напоминание о том, что пора обновить разрешение на парковку, о наступлении срока уплаты налога или о том, что пора записать ребенка в школу. Предприятия торговли и другие коммерческие организации используют анализ, управляемый данными, для улучшения обслуживания клиентов. Этот подход можно применять и для правительственных учреждений.

Цифровая трансформация страны является частью реформы государственного управления. В государственном секторе развитию и

повсеместному внедрению информационных технологий разумеется способствует реализация мероприятий Государственной программы «Цифровой Казахстан», основными целями которого являются форсирование развития всех отраслей жизнедеятельности Республики Казахстан и повышение уровня жизни населения.

Так например, одним из направлений Государственной программы «Цифровой Казахстан» является развитие проактивного государства, а именно создание открытого и эффективного государства, обеспечивающего население и бизнес качественными государственными услугами в соответствии с их нуждами, когда гражданину страны не нужно будет стоять в очередях для получения государственных услуг. Правительство будет отслеживать жизненные ситуации гражданина и выполнять необходимые процессы. А гражданину только нужно будет подтверждать удаленно.

Основные принципы развития электронного правительства заложены в следующих современных потребностях: внедрение омниканальности, проактивность государственных услуг, удобство и простота использования, эффективное оказание электронных услуг, открытость, единое информационное пространство.

В результате выполнения мероприятий Государственной программы «Цифровой Казахстан» выгодополучателями будут являться гражданское общество, бизнес и, следовательно, общество и государство в целом. Гражданское общество получит повышение качества государственных услуг, бизнес-сообщество получит сокращение времени, и, следовательно, издержек, существующих при получении государственных услуг и контактах с государственными структурами.

Соответственно проекты, что указаны в программе направлены:

– на развитие цифировизации в стране во всех отраслях и информационно-коммуникационного пространства;

– на создание новых возможностей и условий для бизнеса и государства в целом;

– на формирование и развитие цифровой грамотности у населения, тем самым увеличение спроса на специалистов в сфере информационных технологий и как следствие повышение уровня образования;

– на увеличение количества госуслуг, при этом параллельно улучшая качество оказываемых услуг, позволющих в значительной степени снизить нагрузку с работников государственных органов и организаций ;

В недалеком будущем взаимодействие человека и государства изменится. Государство отойдет от предоставления точечных услуг и сервисов посредством объектов информатизации «электронного правительства» и перейдет к предоставлению комплексных решений жизненных ситуаций человека посредством единой цифровой платформы, основанное на едином массиве данных и алгоритмах работы с ними. Благодаря использованию современных технологий граждане будут защищены от действий злоумышленников.

Таким образом, внедрение единой цифровой платформы позволит перевести взаимодействия государства с гражданами и бизнесом от «традиционной» сервисоцентричной модели к новой человекоцентричной модели, что является необходимым условием для улучшения качества жизни граждан, обеспечения устойчивого роста экономики Казахстана, укрепления его глобальной конкурентоспособности, оптимизации роли и функций государства и ликвидации коррупции. В рамках человекоцентричной модели государственного управления государство, вместо отдельных потребностей гражданина, будет удовлетворять целый набор потребностей гражданина в зависимости от жизненной ситуации.

В ходе цифровой трансформации происходит строительство новой экосистемы ИТ государства. При этом, с точки зрения инфраструктуры, вся идея цифровой трансформации со всеми вышеупомянутыми особенностями зависит от наличия необходимой и достаточной цифровой инфраструктуры. Без наличия Центров обработки данных, соответствующих стандартам и требованиям, необходимым для бесперебойной и защищенной работы государственного управления, без подключенных широких каналов связи и других инфраструктурных и коммуникационных элементов запуск цифровой трансформации и полноценная работа единой цифровой платформы невозможна.

Процесс реинжиниринга системы и процессов государственного управления и переход к цифровым процессам предоставит следующее:

– автоматизируются полностью и вообще перестанут требовать человеческого участия;

– уровни организационной иерархии уйдут;

– скорость обработки информации изменится от недель и дней до секунд, что потребует от государственного аппарата пересмотра регламентов, численности, процедур и навыков государственных служащих.

Цифровая трансформация в Казахстане с переходом на платформенную модель государственного управления должна принести следующие выгоды:

1. для граждан:

– новый уровень качества государственных сервисов;

– повышение уровня безопасности пользовательских данных;

– реализация принципа «невидимого государства»;

2. для бизнеса:

– возможность интеграции коммерческих услуг с государством;

– снижение издержек на взаимодействие с государством;

– доступ на рынок государственного IT заказов;

3. для государства:

– технологический суверенитет;

– управление государством на основе данных и снижение коррупции;

– новый уровень кибербезопасности.

Перед Правительством Республики Казахстан стоит амбициозная экономическая задача: к 2050 году войти в тридцатку самых развитых стран

мира. Приведенная в Стратегии «Казахстан-2050» формулировка этой задачи логически выражается в повышении доходов на душу населения до уровня, достаточного чтобы с учетом оценок роста мировой экономики и сравнимых стран, к 2050 году войти в рейтинг тридцати наиболее «богатых» стран мира.

Экономический рост в сегодняшних условиях уже невозможен без использования информационных и коммуникационных технологий, особенно в связи с распространением их применения практически в любых сферах экономической деятельности и созданием возможностей для социально-экономического развития. Глобализация, трансформация потребительского поведения, мобильность, доступность информации — все это тренды нашего времени. Цифровые технологии радикально меняют глобальную экономическую систему. Формирование эффективной цифровой экономики раскроет новый потенциал и возможности для создания и развития бизнеса, поможет в наращивании инвестиций и повышении уровня человеческих и финансовых ресурсов.

В условиях формированного развития экономических и технологических составляющих в мире национальная система государственного управления сталкивается с различными сложными задачами, однако не способна оперативно порой и вовсе решить возникаемые задачи. Вопрос совершенствования системы государственного управления и повышения уровня информационной безопасности в контексте цифровой трансформации становится более актуальным, в частности, в связи с массовым использованием онлайн-продуктов.

2. ТЕКУЩАЯ СИТУАЦИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ

Необходимо признать, что текущая тенденция скоростного развития отрасли ИКТ и цифровой сферы повышает прозрачность, улучшает подотчетность и противодействие коррупции, и в целом повышает эффективность деятельности государственных органов. Учитывая, что на текущий момент мир стремительно движется к «инновационному» будущему, с повсеместным применением интеллектуальных цифровых решений, в государственном секторе это влечет за собой автоматизацию и совершенствование многих производственных процессов.

Цифровые технологии превращаются в ключевой фактор конкурентоспособности бизнеса. Однако при этом пропорционально увеличивается активность киберпреступников и кибератак во всех сферах деятельности, в связи с чем возрастает значимость кибербезопасности. Новые реалии постоянно требуют увеличения мощности информационно-коммуникационных технологий, скоростных параметров сетей, ставят новые потребности в достижении высокого уровня информационной безопасности.

Однако, зачастую, темп развития цифровизации может на порядок опережать всевозможные предпринимаемые меры информационной безопасности. Уровень киберугроз и уязвимостей также непрерывно растет. С этой целью, для минимизации фактов несанкционированного доступа, защиты информации, содержащихся в объектах информатизации «электронного правительства» от утечки и предотвращения возможности злонамеренных действий, к решению вопросов информационной безопасности необходимо подходить комплексно.

Таким образом, необходимо понимать, что обеспечение информационной безопасности должно идти параллельно с развитием сферы информационно-коммуникационных технологий и цифровизации. Соответственно возникает необходимость в комплексной оценке существующих в государственных органах рисков информационной безопасности и разработке новых методов, способных вынести состояние защищенности и уровень информационной безопасности на качественно новый уровень.

Как известно информационная безопасность в общепринятом значении - это защита конфиденциальности, целостности и доступности информации. Современные IT-технологии могут быть использованы в целях подрыва суверенитета, нарушения территориальной целостности государств и осуществления других действий против мира, безопасности и стабильности. В силу своей общедоступности и возможности анонимного использования ИКТ применяются в террористических и экстремистских целях, в том числе для пропаганды терроризма и экстремизма.

Стремительно растет количество киберпреступлений в различных сферах жизнедеятельности в особенности в банковской отрасли, что является источником рисков возникновения угроз информационной безопасности и как следствие экономической безопасности государства. Несанкционированный доступ киберпреступников влечет за собой компроментацию персональных данных нарушая права современного общества на неприкосновенность личной жизни.

Прослеживается тенденция использования отдельными государствами своего технологического доминирования для монополизации рынка IT-технологий, ограничения доступа других стран к передовым технологиям, а также для усиления их технологической зависимости от стран, доминирующих в сфере информатизации.

Казахстан в свою очередь осуществляет собственную политику в целях укрепления позиции в информационной безопасности на государственном уровне.

В целях реализации Указа Президента Республики Казахстан, утвержденного 15 февраля 2017 года «О мерах по реализации Послания Главы государства народу Казахстана от 31 января 2017 года «Третья модернизация Казахстана: глобальная конкурентоспособность» успешно реализуется Концепция кибербезопасности «Киберщит Казахстана», призванная реализовать комплекс мер, которые направлены на поддержку информационной безопасности пользователей сети и казахстанского сегмента

Интернета в целом. Концепция призвана обепечить осуществление государственной политики в сфере защиты объектов информацтизации, информационно-коммуникационного пространства и как следствие персональных данных содержащихся в информационных ресурсах государственных органов, посредством обеспечения безопасности используемых информационных технологий.

Концепция бесспорно призвана обеспечить общий подход к обеспечению информационной безопасности информационных систем государственных органов а также информационного пространства в целом, в том числе данных о граждах РК. В рамках Коценпции требуется создание механизма, позволяющий заблаговременно предупредить, обнаружить и предотвратить инциденты информационной безопасности, в том числе и во внештатных ситуациях.

Посредством данной Концепции будет достигнута реализация мер, направленных на повышение уровня защищенности объектов информатизации и информационно-коммуникационной пространства, предотвращающих возникновение различных инцидентов информационной безопасности в условиях цифровой трансформации и развития отрасли информационных технологий.

Дополнительно в период с 2018 по 2022 год в Казахстане осуществлялась реализация и исполнение Государственной программы «Цифровой Казахстан».

Государственная программа «Цифровой Казахстан» приоритетным направлением ставит усиление мер по развитию внутренней и внешней экономики страны посредством внедрения и повсеместным использованием IT-продуктов. При этом, важно отметить, что вопросы кибербезопасности не остались в стороне – так как выдвинуты вопросы по реагированию на инциденты информационной безопасности в казахстанском сегменте сети Интернет.

Одним из важнейших показателей развития кибербезопасности является международный рейтинг, составляемый Международным союзом электросвязи ООН – Глобальный индекс кибербезопасности.

Государственная программа «Цифровой Казахстан» в качестве одного из показателей включала в себя достижение Казахстаном в 2022 году уровня 0,810 в ГИК. Показатель перевыполнен в 2020 году, когда составил 0,931.

Согласно актуальным результатам ГИК, опубликованным в 2021 году Республика Казахстан занимает 31 место из 182 участников. При этом в отчете за 2020 год Казахстан занимал 40 место, в 2019 – 83 место, а еще ранее не входил и в топ-100 рейтинга. Среди стран СНГ Казахстан занимает 2 место после России. По мнению экспертов, Казахстан выделился техническими, законодательными и кооперативными мерами, нацеленными на создание и укрепление технических институтов, вовлеченных в обеспечение информационной безопасности, а также потенциалом развития и сотрудничества с другими государствами. В этой связи, важно отметить существенную роль Концепции и ГП ЦК в достижении высоких позиций в ГИК.

В соответствии с существующим законодательством и нормативными правовыми актами предусмотрены различные меры обеспечения информационной безопасности.

1. Так, например, ИС ГО или организаций квазигосударственного сектора и негосударственные ИС, предназначенные для формирования государственных электронных информационных ресурсов, создаются, эксплуатируются и развиваются при условии успешного прохождения испытаний на соответствие требованиям ИБ. С этой целью созданы испытательные лаборатории в сфере информационной безопасности осуществляющие данный вид деятельности. Испытания в свою очередь непосредственно включают в себя работы по оценке соответствия объектов испытаний требованиям технической документации, НПА и действующих на территории РК стандартов в сфере ИБ и проводятся в среде штатной эксплуатации.

2. Также, в 2018 году в стране начал функционировать Национальный координационный центр информационной безопасности при акционерном обществе «Государственная техническая служба», который обеспечивает защиту информационных ресурсов и объектов информатизации ГО и КВОИКИ от кибератак и является главным элементом в системе обеспечения информационной безопасности в масштабе страны. Создавался он в качестве субъекта, координирующего вопросы информационной безопасности (в большей части по реагированию на инциденты ИБ).

Таким образом, являясь технологическим ядром системы обеспечения безопасности информационного пространства Республики Казахстан акционерное общество «Государственная техническая служба» реализует ряд функций, закрепленных статье 7-4 Закона «Об информатизации», направленных на координацию по вопросам мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации «электронного правительства», казахстанского сегмента Интернета, а также критически важных объектов информационно-коммуникационной инфраструктуры, реагирования на инциденты информационной безопасности и повышение уровня информационной безопасности объектов информатизации «электронного правительства» в целом.

3. Посредством системы мониторинга обеспечения информационной безопасности НКЦИБ осуществляется Мониторинг обеспечения информационной безопасности объектов информатизации «электронного правительства». Основной целью МОИБ является контроль за реализацией владельцами ОИ ЭП технических и других мероприятий по обеспечению ИБ посредством выявления угроз и инцидентов информационной безопасности.

Мониторинг обеспечения информационной безопасности включает следующие виды работ:

1) МРИ ИБ;
2) МОЗ;
3) МОБФ.

4. Кроме того, в отношении объектов информатизации государственных органов осуществляется МСИБ, основной целью которого является мониторинг за состоянием ОИ с целью обнаружения инцидентов ИБ. В рамках данного вида деятельности осуществляется:

1) установка источников событий ИБ в информационно-коммуникационной инфраструктуре ГО;

2) техническое сопровождение источников событий, инцидентов и угроз ИБ в информационно-коммуникационной платформе и инфраструкте ГО и организаций квазигосударственного сектора;

3) отслеживание событий информационной безопасности объектов, с целью обнаружения инцидентов информационной безопасности и последующего на них реагирования.

В рамках данного вида деятельности проведены работы по оснащению центральных государственных органов продвинутыми средствами защиты информации, в связи с чем достигнута высокая степень защиты информационно-коммуникационной инфраструктуры центральных исполнительных органов.

5. НКЦИБ агрегирует всю актуальную информацию о кибератаках и угрозах из информационного поля с оперативных центров информационной безопасности.

В этом контексте, одним из немаловажных требований к владельцам КВОИКИ или объектов информатизации «электронного правительства» согласно нынешнего законодательства является создание и обеспечение функционирования ОЦИБ в своей структуре или приобретение услуги ОЦИБ у других лиц, осуществляющие деятельность по идентификации, оценке, нейтрализации, отражению и профилактике угроз ИБ ИКИ государственных органов и организаций квазигосударственного сектора.

6. Для поддержания соответствующего уровня защищенности государственных ЭИР, ИС и ИКИ Республики Казахстан от внешних и внутренних угроз 4 июня 2019 года был организован ККС по информационной безопасности в состав которых входят специалисты технического направления ГО и организаций.

Основной целью ККС является создание, поддержание и развитие условий, необходимых и достаточных для межотраслевой координации по вопросам МОИБ, МОЗ, МОБФ объектов информатизации «электронного правительства», казахстанского сегмента Интернета, а такжи КВОИКИ, реагирования на инциденты ИБ с проведением совместных мероприятий по обеспечению ИБ.

Основными задачами ККС является:

1) разработка различных мер и методов, способных обозначить основные направления для государственных органов и организаций в сфере информатизации в части реагирования на угрозы и инциденты а также выработка практических мер способных повлиять на улучшение состояния обеспечения ИБ;

2) выработка мероприятий для государственны органов и организациц по противодействию современным угрозам, выявлению, реагированию и расследованию угроз и инцидентов ИБ в казахстанском сегмента Интернета;

3) оказание взаимной помощи в решении организационных, технических и нормативно-правовых вопросов, связанных с предотвращением угроз ИБ и чрезвычайных ситуаций, оперативным реагированием на них и ликвидацией последствий;

4) формирование практических механизмов совместного реагирования на угрозы ИБ;

5) органиция и проведение совместных тренировок и учений государственных органов и организаций по реагированию на угрозы и инциденты ИБ;

6) организация проведения семинаров и конференцций с участием представителей государственных органов и организаций по вопросам реагирования на угрозы и инциденты ИБ;

7) внедрение передового опыта в сфере информатизации в части реагирования на угрозы и инциденты ИБ;

Таким образом, Совет выполняет следующие функции:

1) участие в выраоьтке государственной политики в сфере информатизации в части реагирования на угрозы и инциденты ИБ;

2) изучение зарубежной практики реагирования на угрозы и инциденты ИБ;

3) оценка и выработка мер по совершенствованию деятельности государственных органов и организаций в сфере информатизации в части реагирования на угрозы и инциденты ИБ;

4) оказание содействия собственникам, владельцам и пользователям объектов информатизации в решении вопросов по безопасному использованию информационно-коммуникационных технологий;

5) выработка мер и механизмов взаимного обмена информацией и мерами по вопросам идентификации, обнаружения и предотвращения инцидентов ИБ между государственными органами и организациями;

6) содействие в выявлении и устранении причин возникновения угроз и инцидентов ИБ;

7) оказание содействия в осуществлении международного сотрудничества в сфере информатизации, взаимодействии с международными профильными организациями по вопросам угроз и инцидентов ИБ и реагированию на них;

8) координация основных задач связанных с МОИБ, МОЗ и МОБФ объектов информатизации «электронного правительства», казахстанского сегмента Интернета, а такжи КВОИКИ, реагирования и оперативное предотварщение угроз и инцидентов ИБ с проведением совместных мероприятий по обеспечению ИБ, в порядке определенном действующим на территории РК законодательством.

В рамках совета проводится ознакомление с текущим состоянием ИБ в ГО и организациях квазигосударственного сектора, обмен опытом и в отношении выработки мер по взаимному обмену между государственными органами оперативной и иной информацией касательно реагирования на инциденты и угрозы ИБ. Помимо этого ККС позволяет обсудить вопросы улучшения взаимодействия ГО и организаций в сфере ИБ. Более того, в рамках ККС вырабатываются конкретные рекомендации для государственных органов по повышению эффективности работы и формированию механизмов совместного реагирования на угрозы ИБ.

7. Также, для защиты интернет-ресурсов государственных органов используется оборудование ЕШДИ, который представляет из себя АПК призванных защищать сети телекоммуникаций при доступе к Интернету или сетям связи, имеющим выход в сеть интернет. ЕШДИ представляет из себя своеобразный фильтр, очищающий трафик от разного рода атак и не допускает их воздействия на ИКИ государственных органов а также на информационные ресурсы.

Таким образом, подключение локальных, ведомственных и корпоративных сетей телекоммуникаций государственных органов, органов местного самоуправления, государственных юридических лиц, субъектов квазигосударственного сектора, а также собственников или владельцев критически важных объектов информационно-коммуникационной инфраструктуры к Интернету осуществляется операторами связи через единый шлюз доступа к Интернету.

ЕШДИ включает в себя:

– систему предотвращения вторжений, предназначенную для обнаружения и блокировки сетевых атак;

– систему межсетевого экранирования на уровне приложений, позволяющую определять и контролировать запросы, формируемые различного рода программным обеспечением, в том числе, и вредоносным;

– межсетевой экран защиты веб-приложений, позволяющий фиксировать и блокировать атаки на веб-приложения, направленные на получение несанкционированного доступа к данным и их модификации;

– сетевую «песочницу», предназначенную для обнаружения сложных целевых атак в изолированной защищенной среде («песочнице»);

– веб-фильтрацию, позволяющую ограничивать доступ пользователей телекоммуникационных сетей, подключенных к сегменту Интернет через ЕШДИ, к ИР посредством их категоризации;

– средство мониторинга несанкционированных изменений веб-страниц, позволяющее автоматическое выявление модификации и искажение веб-страниц ИР злоумышленниками, а также восстанавливать интернет-ресурсы до исходного состояния.

В настоящее время к ЕШДИ подключены операторы связи, имеющие собственные каналы связи:

1. АО «Казахтелеком»;

2. АО «Astel»;
3. АО «Jusan Mobile»;
4. АО «Транстелеком»;
5. ТОО «TNS-plus»;
6. ТОО «SMARTNET»;
7. ТОО «КаР-Тел»;
8. ТОО «Мобайл Телеком-Сервис»;
9. АО «Казтелепорт»;
10. ТОО «NLS ASTANA»;
11. АО «Алма Телекоммуникейшнс Казахстан»
12. ТОО «KAZOPTICLINK»

На сегодняшний день более чем 200 интернет-ресурсов обеспечены защитой средствами *Единого шлюза доступа к Интернет.*

Так, Акционерным общество «Государственная техническая служба», стоящим на страже кибербезопасности нашей страны приводится следующая статистика в государственных органах:

- в 2021 году с использованием *ЕШДИ* было заблокировано порядка 82,3 млн. атак, более 1,4 млн из которых были направлены на ИР государственных органов , из них атаки на «Портал электронного правительства составили более 15 тыс. В результате глубокого экспертного анализа данных экспертами ГТС выявлено более 114 тыс. угроз информационной безопасности.

8. Немаловажным является и то, что с целью осуществления государственной политики в сфере информационной безопасности и защиты персональных данных был создан уполномоченный орган – МЦРИАП РК - осуществляющий регулятивные, реализационные и контрольные функции области обеспечения ИБ в сфере информатизации, в сфере обеспечения защищенности обрабатываемых в ЭИР персональных данных, а также электронного документа и электронной цифровой подписи на предмет соблюдения законодательства Республики Казахстан об электронном документе и электронной цифровой подписи. Уполномоченным органом проводятся профилактический контроль и внеплановые проверки, которые позволяют выявлять несоответствия требованиям информационной безопасности в деятельности государственных органов, критически важных объектов информационно-коммуникационной инфраструктуры и организаций. Более того, в случае обнаружения фактов незаконного сбора или утечки персональных данных, а также нарушения правил использования электронно-цифровой подписи, граждане имеют возможность обратиться в уполномоченный орган для принятия ими соответствующих мер в отношении нарушителей.

3. МИРОВЫЕ ТРЕНДЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Мир информационных технологий не стоит на месте и изменяется каждый день. Вместе с ним меняются и угрозы кибербезопасности.

Так например, статистика Всемирного экономического форума говорит о том, что ущерб нанесенный инцидентами в сфере ИБ экономике глобально составил в 2020 году 2,5 трлн. Долларов. В 2022 году данные показатели могут выйти за отметку в 8 трлн. долларов

Согласно исследованию Cybersecurity Ventures ожидается, что киберпреступность будет до 5 раз прибыльнее, чем глобальные транснациональные преступления вместе взятые.

Во всем мире отмечается тренд на увеличение числа кибератак на критическую инфраструктуру, которые приводят к серьезным последствиям.

Основные мировые тренды в сфере кибербезопасности связаны с появлением новых угроз, созданием технологий и бизнес-моделей:

1. Атаки вирусов-вымогателей (ransomware).

Вирусы-вымогатели или как их еще называют "шифровальщики" проникают в локальную сеть организации и шифруют пользовательские данные (часто при этом предварительно копируя их на удаленный сервер злоумышленников), после чего требуют выкуп за дешифрование данных. Жертвой подобной атаки может стать компания в любой отрасли. В дальнейшем подобные атаки будут только набирать обороты, особенно учитывая распространение RaaS (Ransomware-as-a-Service), модели, при которой операторы шифровальщика предоставляют злоумышленникам всю необходимую инфраструктуру и инструменты для проведения атак.

2. Атаки на цепочку поставок (supply-chain attacks).

При подобном типе атаки злоумышленники встраивают свой вредоносный код (бэкдор) в компонент программного обеспечения или обновления, разрабатываемый субподрядчиками или же взламывают менее защищенные организации, задействованные в общем масштабном процессе. Так, атака на платформу компании SolarWinds вызвала огромный резонанс: хакеры взломали 9 правительственных агентств США и примерно 100 известных коммерческих компаний с помощью зараженной платформы компании.

3. Развитие концепции XDR (extended detection response).

XDR осуществляет обнаружение угроз и реагирование на них за счет консолидации информации о безопасности и управления событиями. XDR - это единый центр сбора, нормализации, анализа, корреляции данных, расширенного расследования и реагирования с применением максимально возможной автоматизации.

4. Модель «нулевого доверия» (zero trust).

Модель «нулевого доверия», одна из популярных концепций, в своем определении означает модель безопасности подразумевающий полное отсутствие доверенных зон. В рамках этой модели потенциальные источники

атаки, в том числе различные устройства и приложения а также учетные данные подвергаются постоянной проверке тогда когда запрашивается доступ к какому-то ресурсу.

5. Безопасность при удаленной работе (remote workforce security).

Согласно отчету Gartner, 65% сотрудников теперь могут работать из дома и не менее 35% намерены продолжать работу в таком режиме даже после пандемии. От организаций потребуется полная смена инструментов безопасности, подходящих для современного удаленного рабочего пространства. Руководители служб безопасности также должны пересмотреть политики защиты данных, резервного копирования и аварийного восстановления.

4. ИНЦИДЕНТЫ ИБ В ГОСУДАРСТВЕННОМ СЕКТОРЕ

Обеспечение безопасности киберпространства и защита информационнокоммуникационной инфраструктуры - важнейшая задача государства в современном цифровом мире. Именно поэтому информационная безопасность является неотъемлемой частью национальной безопасности. По поручению Первого Президента Республики Казахстан с 2017 года в стране начата реализация Концепции кибербезопасности "Киберщит Казахстана".

В 2021 году зафиксирован рост интереса к квазигосударственному сектору Казахстана со стороны злоумышленников. По сравнению с 2020 годом, в 2021 году количество уникальных IP-адресов зарубежных стран, с которых были зафиксированы вредоносные запросы на квазигосударственный сектор, выросло в 2,2 раза и составило 264 тысячи. 264 (в 2020 году число уникальных IP-адресов, с которых фиксировались вредоносные запросы на объекты информатизации квазигосударственного сектора составило 120 тыс., в 2021 это число составило 264 тыс.).

Из всех 27 тысяч инцидентов ИБ, зарегистрированных в 2021 году, количество инцидентов ИБ в государственном секторе (государственные и местные исполнительные органы) составляет 23 тысяч. Количество компьютерных вирусов (вредоносного программного обеспечения) из числа всех инцидентов ИБ в государственном секторе составляет 80%. Компьютерные вирусы фиксировались в государственном секторе более 20 тысяч раз.

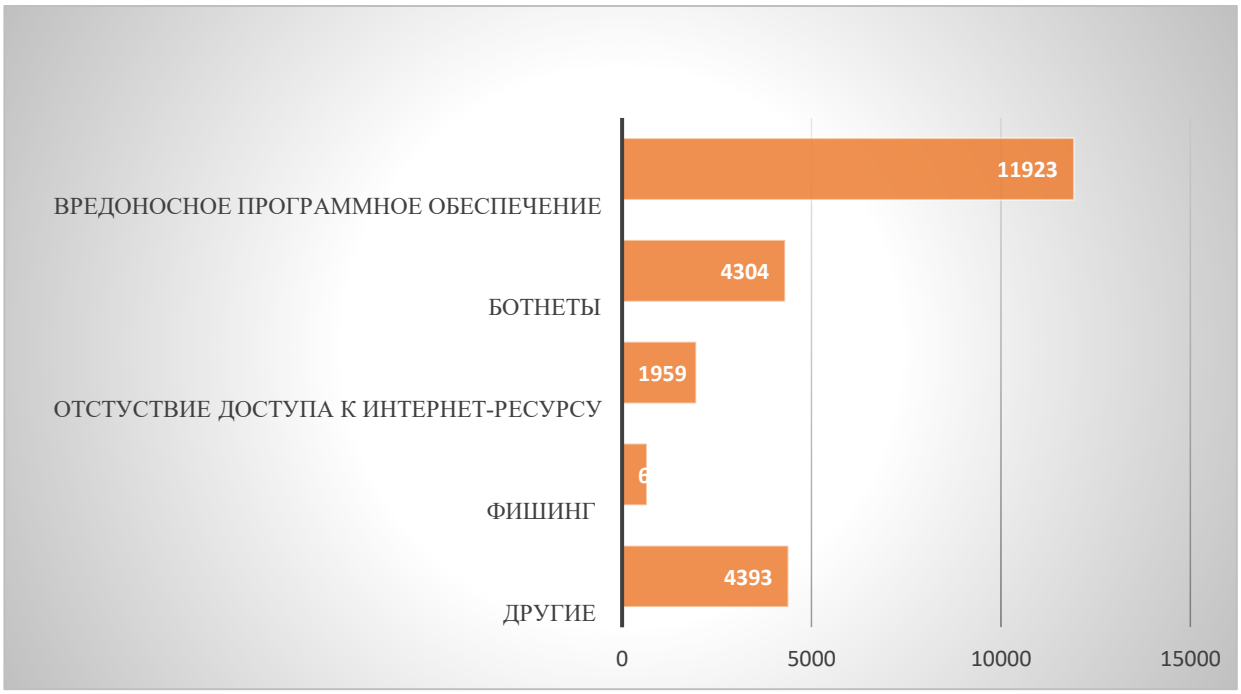

Рисунок 1- Статистика инцидентов за 2021 год

Одними из самых распространенных киберинцидентов в государственном секторе являются:

1) Фишинговые атаки

Организации в Казахстане по-прежнему сталкиваются с большим объемом и широким спектром фишинговых атак, главная угроза – письма с вредоносным вложением. При фишинговой атаке (phishing — от англ. fishing, что значит «рыбалка») злоумышленники стараются заманить в свои сети как можно больше людей, чтобы украсть логины и пароли, данные банковских карт, конфиденциальную корпоративную информацию или же заразить устройства пользователей вредоносным ПО.

Сегодня фишинг — один из самых распространенных в мире видов киберпреступлений, с помощью которого чаще всего похищают аккаунты и банковскую информацию. Большое количество фишинговых атак осуществляется с использованием мошеннических интернет-ресурсов, которые маскируются под легитимные. Подобные атаки представляют собой рассылку ссылок на мошеннические сайты, имитирующие интернет-ресурсы государственных органов, банков второго уровня (далее - БВУ), популярных компаний, соцсетей, интернет-магазинов и т.д.

Злоумышленники рассчитывают на то, что пользователь не заметит подделки и укажет на странице личные данные: реквизиты банковской карты, логин и пароль, номер телефона. Чаще всего злоумышленники создают фишинговые сайты для проведения мошеннических действий путем сбора персональных данных граждан

2) DDoS – атаки (Distributed Denial of Service)

Атаки типа «распределенный отказ в обслуживании» – это действия, направленные на перегрузку трафиком, когда на атакуемый ресурс отправляется большое количество злонамеренных запросов, из-за чего полностью «забиваются» все каналы сервера или вся полоса пропускания. При этом передача легитимного трафика на сервер затрудняется или становится невозможной.

В результате атаки нарушается или полностью блокируется обслуживание законных пользователей, сетей, систем и иных ресурсов. Так или иначе по итогам воздействия атаки серверные оборудования, на котором развернуты интернет-ресурсы, приходится пропускать непосильный и превышающий объем запросов, в большинстве своем ложные. Таким образом, интернет-ресурс из-за большой нагрузки становится просто напросто недоступным для добросовестных пользователей данных ресурсов.

Вышеупомянутые запросы приходят с различных сетей и потому предотварить данный вид мошенничества киберпреступников совершенно сложно и требует существенной работы над заражением. Так, защита включает такие мероприятия, как фильтрация и блэкхолинг, устранение уязвимостей сервера, наращивание ресурсов, построение распределённых систем, которые продолжат обслуживать пользователей интернет-ресурсов, уклонение или увод непосредственной цели атаки от других связанных ресурсов, маскировка IP-адреса.

3) Ботнет - это сеть компьютеров, удаленно управляемая злоумышленниками.

Самым активным в ГО страны стал знаменитый ботнет AAEH - полиморфный загрузчик с более чем 2 миллионами уникальных образцов. После установки он трансформируется каждые несколько часов и быстро распространяется по сетям, съемным дискам (USB / CD / DVD) и через файлы архивов ZIP и RAR. Система, зараженная AAEH, может использоваться для распространения вредоносного ПО, сбора учетных данных пользователей для онлайн-сервисов, включая банковские услуги, и вымогательства денег у пользователей путем шифрования файлов с последующим требованием оплаты. AAEH использовался для загрузки других семейств вредоносного ПО, таких как Zeus, Cryptolocker, ZeroAccess и Cutwail.

4) APT-группировки

Advanced Persistent Threat переводится как развитая устойчивая угроза. APT-группировками принято обозначать злоумышленника, в распоряжении которого имеются специальные знания, соответствующий инструментарии и значительные ресурсы, которые в совокупности позволяют осуществлять целенаправленные кибератаки.

Особенностью целенаправленных атак (APT) является наличие у злоумышленников определенной жертвы, зачастую это крупная компания или государственная организация. Целенаправленные атаки хорошо спланированы и содержат несколько этапов. Результатом атаки может стать закрепление злоумышленников в инфраструктуре жертвы и скрытый сбор данных на протяжении многих месяцев.

В марте 2021 года специалисты по безопасности из компании SentinelOne обнаружили вредоносную атаку на РК с применением ВПО, написанного на Delphi, называемого Delphocy, также известны как APT28 и FancyBear. В качестве приманок использовались документы Word, якобы созданные АО "Казхром". Было обнаружено 6 используемых Delphocy документов Word, которые содержали VBA-скрипт, который файл заменял и доставлял в формате PE.

5) Атаки на автоматизированные системы управления технологическим процессом.

Очень часто целью злоумышленников является получение контроля над автоматизированной системой управления технологическим процессом (в английской терминологии SCADA). АСУ ТП представляет из себя техническое решение на базе различных программных средств и предназначенные для автоматизации управления каким-либо технологическим процессом. Возможна связь с основной автоматизированной системой управления предприятия. В основном атаки направлены не на вывод из строя оборудования или осуществление аварий: по большей части это разведка, глубокое закрепление и длительное присутствие в инфраструктуре атакуемых объектов.

Казахстан занимает 15 место в антирейтинге стран по числу компьютеров АСУ ТП, на которых заблокировано вредоносное ПО (по данным Kaspersky). Согласно исследованию, опубликованному Kaspersky ICS CERT, основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, съемные носители и электронная почта.

В Казахстане совершаются определенные шаги в сторону защиты АСУ ТП. Например, в Перечень КВОИКИ входит 40 объектов автоматизированной системы управления технологическим процессом.

Стоит отметить, что нарушение или прекращение работы АСУ ТП может привести к чрезвычайной ситуации техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или для жизнедеятельности населения, проживающего на соответствующей территории, в том числе таких значимых производственных объектов промышленности как теплоснабжение, электро и газоснабжение, водоснабжение, области здравоохранения, обеспечения связи, сферы банковской деятельшншости, транспортной инфраструктуры, производств гидротехнических сооружений, осуществления правоохранительной деятельности и конечно же электронного правительства.

6) Шифровальщики

Шифровальщиками (Ransomeware) или как их называют иначе программами-вымогателями принято называть вредоносное ПО, цель которого шифрование данных жертвы с последующим получением выкупа за дешифрование данных. Согласно статистике злоумышленники в среднем требуют выкуп в размере 300 долларов для расшифровки данных.

5. АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ

Проблемы кибербезопасности становятся ежедневной угрозой, в том числе и для государственного аппарата. Организациям, которые сталкиваются с нарушениями информационной безопасности, необходимо выделять средства на исправление различных уязвимостей, расследования произошедших инцидентов, а также на повышение как осведомленности сотрудников в вопросах обеспечения кибербезопасности, так и их квалификации.

В то время как компании затрачивают средства на обеспечение безопасности, злоумышленники продолжают «оттачивать свое мастерство», подготавливая эксплойты для использования данной уязвимости. Рекомендуется уделять больше внимания на сокращение времени, затрачиваемого на исправление уязвимости, найти эффективные гибкие и адаптированные инструменты безопасности и действовать быстрее злоумышленников, пытающихся проникнуть в систему

С учетом существующих вызовов и задач, а также на основе мировых практик можно выделить следующие ключевые процессы информационной безопасности, которые позволяют эффективно предотвращать, выявлять и реагировать на современные угрозы:

Таблица 1 - ключевые процессы информационной безопасности

Направления информационной безопасности	**Процессы информационной безопасности**
Политики ИБ	Разработка политик ИБ
	Пересмотр политик ИБ
Организация ИБ	Организация внутренних аудитов
	Оценка рисков ИБ
	Анализ со стороны руководства
	ИБ в управлении проектами и др.
Безопасность персонала	Проверка работника перед трудоустройством
	Дисциплинарный процесс
	Осведомленность, образование и обучение в сфере ИБ и др.
Управление активами	Инвентаризация активов
	Контроль использования активов
	Классификация информации
	Управление съемными носителями информации и др.

Продолжение таблицы 1

Управление доступом	Управление доступом к сетям и сетевым службам
	Управление привилегированными правами доступа
	Пересмотр прав доступа пользователей
	Безопасные процедуры входа в систему и др.
Криптография	Политики использования криптографических методов защиты
	Управление криптографическими ключами
Физическая защита от угроз природного характера	Защита офисов, помещений и оборудования
	Защита от внешних угроз и угроз природного характера
	Обслуживание оборудования
	Безопасная утилизация или повторное использование оборудования и др.
Безопасность производственной деятельности	Управление изменениями
	Защита от вредоносного кода
	Резервное копирование
	Управление уязвимостями и инцидентами ИБ
	Регистрация событий и инцидентов
Приобретение, создание, развитие и сопровождение систем	Безопасная разработка
	Управления изменениями в системе
	Принципы разработки защищенных систем
	Тестирование защищенности системы и др.
Безопасность обмена информацией	Безопасность сетевых сервисов
	Разделение в сетях
	Политики и процедуры передачи информации
	Безопасность прикладных сервисов в общедоступных сетях и др.
КБ в отношениях с поставщиками	Политика ИБ в отношениях с поставщиками

Продолжение таблицы 1

КБ в отношениях с поставщиками	Включение безопасности в договора с поставщиками
	Управление изменения услуг поставщика
	Мониторинг и пересмотр услуг поставщика и др.
Управление инцид ентами	Мониторинг и реагирование (раскрывается в разделе SOC)
	Извлечение уроков из инцидентов ИБ и др.
КБ в управлении непрерывностью бизнеса	Планирование непрерывности ИБ
	Обеспечение непрерывности ИБ
	Проверка, пересмотр и оценка непрерывности КБ
Соответствие требованиям регуляторов	Определение применимого законодательства и договорных требований
	Независимый пересмотр (аудит) ИБ
	Соответствие политикам безопасности и стандартам
	Проверка соответствия техническим требованиям и др.

В соответствие с Законом Республики Казахстан, утвержденного 24 ноября 2015 года «Об информатизации», постановлением Правительства Республики Казахстан, утвержденного 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности», СТ РК ISO/IEC 27005-2013 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности» с целью обеспечения информационной безопасности необходимо государственным органам разрабатывать Методику оценки рисков информационной безопасности.

Методика предназначена для определения актуальности и экономической целесообразности используемых систем защиты информации, а также определения соответствия принимаемых мер по информационной безопасности к требованиям нормативно-технических документов в области информационной безопасности. Анализ рисков информационной безопасности необходим для понимания видов угроз и уязвимости, прогнозирования их наступления и развития, выстраивания системы защиты и необходимого инвестирования на реализацию.

Риск – это ущерб или негативное событие, которое может быть нанесено организации или физическому лицу и может в последствии привести к компроментации, потере или недоступности информации.

Реализация риска может привести к негативным последствиям и зависит от составляющих как стоимость данных и защищенность объекта, в которой обрабатывается информация.

Процесс управления рисками ИБ состоит их следующих основных этапов:

1) идентификация рисков ИБ;
2) оценка рисков ИБ;
3) обработка рисков ИБ;
4) мониторинг рисков ИБ.

Анализ рисков можно условно разделить на:

1) Качественный, который выявляет виды рисков, факторы возникновения;
2) Количественный, определяет размеры риска на основании качественной оценки рисков.

Основными задачами качественного анализа рисков информационной безопасности являются:

– идентификация и оценка информационных активов государственного органа в целях определения требований по конфиденциальности, целостности, доступности или иных требований по информационной безопасности, предъявляемых к информации и информационным активам.

– выявление и определение источников угроз информационной безопасности в отношении бизнес-процессов государственного органа и оценка их влияния на риски;

– определение процессов и мер по обеспечению ИБ, которые противодействуют угрозам или снимают их возможности по влиянию на риски и оценка их эффективности;

– выявление и определение уязвимостей в обеспечении информационной безопасности в реализации процессов и мер по обеспечению ИБ.

Алгоритм оценки рисков информационной безопасности **изучен на базе одного из государственных органов** в ходе проводимых испытаний на соответствие требованиям ИБ.

Таким образом, методом исследования была анкета-опросник о характеристиках объекта испытаний заполненный государственным органом.

Так, в данной анкете-опросник государственный орган отражает следующую информацию:

1) Наименование;
2) Краткая аннотация на объект испытаний;
3) Классификация: класс прикладного программного обеспечения, схема классификации;

4) Архитектура объекта испытаний: функциональная схема объекта испытаний (при необходимости) с указанием компонентов, модулей объекта испытаний и их IP-адресов, связей между компонентами или модулями и направления информационных потоков, точки подключения интеграционного взаимодействия с другими объектами информатизации, точки подключения пользователей, мест и технологий хранения данных, применяемого резервного оборудования, разъяснения применяемых терминов и аббревиатур;

5) Функциональная схема;

6) Схема сети передачи данных;

7) Информация о серверном оборудовании;

8) Информация о сетевом оборудовании;

9) Местонахождение серверного и сетевого оборудования;

10) Характеристика резервного серверного оборудования;

11) Характеристики резервного сетевого оборудования;

12) Местонахождение резервного серверного и сетевого оборудования;

13) Структура сети объекта испытаний;

14) Информация по рабочим станциям администраторов;

15) Информация о пользователях прикладного программного обеспечения, в том числе с применением мобильных и интернет приложений;

16) Информация об интеграционном взаимодействии объекта испытаний, в том числе, планируемые;

17) Исходные коды прикладного ПО;

18) Исходные коды и исполняемые файлы используемых библиотек и программных(ой) платформ(ы);

19) Документирование испытываемого объекта

На основании изучения документирования испытываемого объекта было выявлено следующее.

Активы в государственном органе сгруппированы по следующим типам для обеспечения полного учета активов:

- информационные активы: база данных, файлы данных, системная документация, руководства пользователя, учетные материалы, процедуры эксплуатации или поддержки (обслуживания), планы по обеспечению непрерывности функционирования информационного обеспечения, процедуры действий при сбоях, архивированная информация;
- физические активы: серверное оборудование, компьютерное оборудование, виртуальные машины, телекоммуникационное оборудование, лицензии, сменные носители информации и другое оборудование;
- активы программного обеспечения: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты;
- услуги: вычислительные услуги, услуги связи, общие коммунальные услуги и другие услуги;
- персонал: люди, их квалификации, способности и опыт;
- нематериальные активы: репутация и имидж организации.

По итогам определения активов, было проведения работа по оценке ценности каждого из активов, на основании того какой ущерб будет нанесен государственному органу в случае потери безопасности, компроментации и нарушения целостности активов. Также во внимание брались и затраты направленные на создание, развитие и сопровождение того или иног

Для определения ценности актива использованы следующие уровни:

− «высокий» (1) уровень подразумевает, что в результате потери свойств безопасности актива ГО будет нанесен значительный ущерб;

− «средний» (2) уровень подразумевает, что в результате потери свойств безопасности актива ГО будет нанесен существенный ущерб;

− «низкий» (3) уровень подразумевает, что в результате потери свойств безопасности актива, ГО будет нанесен незначительный ущерб.

Активы в реестре информационных активов ГО были сформированы таким образом, чтобы наблюдалась сортировка по по значимости. Самые значимые - находились начале реестра, менее значимые - ниже.

Для определения наиболее значимых рисков проведена количественная оценка рисков в соответствии с таблицами 1 и 2, которая определяет вероятность возникновения рисков и влияние последствия рисков.

Таблица 2 - вероятность возникновения рисков

Балл	Вероятность	Качественная характеристика	Количественная характеристика
5	Крайне высокая	Вероятность реализации риска крайне высокая. Существует история многократной реализации данного риска.	Не менее 1 раза в месяц
4	Высокая	Вероятность реализации риска крайне высокая. Существует история многократной реализации данного риска.	Не менее 1 раза в месяц
3	Средняя	Риск может реализоваться. Существует история реализации данного риска.	Не менее 1 раза в месяц
2	Низкая	Вероятность реализации риска низкая. Риск никогда не реализовывался ранее.	Не менее 1 раза в год
1	Крайне низкая	Вероятность реализации риска крайне низкая. Риск никогда не реализовывался ранее.	Не менее 1 раза в год

Таблица 3 - Влияние последствия рисков

Балл	Степень влияния	Описание
5	Критическое	В случае реализации риска, компания практически не сможет полностью восстановиться от последствий, связанных с данным риском
4	Существенное	Последствия от реализации риска очень значительные, но могут быть исправлены до определенной степени
3	Среднее	Последствия от реализации риска очень значительные, но могут быть исправлены до определенной степены
2	Низкое	Последствия от реализации риска не значительные
1	Крайне незначительное	Отсутствие каких-либо последствий в случае реализации риска

На основании результатов процессов идентификации и анализа принимаются решения по обработке рисков информационной безопасности.

Применяются следующие варианты обработки рисков ИБ:

– Снижение (корректировка) риска – уровень возникновения риска необходимо снизить и обеспечить использование таких мер управления рисками способных в дальнейшем остаточный риск перенести на допустимый уровень, например внедрив средства защиты информации и т.д.;

– Сохранение риска – без принятия каких-либо действий; способных снизить риск;

– Избежание риска – предотвращение действий, споособствующий возникновению конкретного риска. Сюда же можно отнести воздействие на источник угрозы, которое может изменить условия, вызывающие риск;

– Перенос (разделение) риска – перенос риска к тем, кто наиболее лучшим образом может осуществлять управление идентифицированным риском.

Таким образом, в рамках рассматриваемого примера на основе одного из ГО определены следующие риски ИБ:

– Риск выхода из строя серверного и телекоммуникационного оборудования;

– Риск по возникновению кибератак;

– Риск потери конфиденциальности данных;

– Получение доступа других лиц к служебной информации ограниченного распространения;

– Риск нарушения конфиденциальности и целостности информации, хранящейся в эксплуатируемых ИС;

– Риск несанкционированного удаления, утечки информации или искажения по причине воздействия вредоносных программ (вирусы, «черви» и т.п.);

– Риск утечки информации ограниченного распространения путем выноса из здания носителя информации;

– Риск несвоевременного обнаружения и реагирования на инциденты/события ИБ;

– Риск возникновения значительных неисправностей оборудования;

– Риск утечки исходного кода программного обеспечения.

6. ПРЕДЛАГАЕМЫЕ МЕРЫ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках проводимой цифровизации государственными органами вопросам обеспечения информационной безопасности порой внимание уделяется по остаточному принципу. Указанное негативно отражается при рассмотрении вопроса ввода ОИ ЭП в промышленную эксплуатацию с многочисленными уязвимостями и нарушениями, что в результате приводит к неэффективному расходованию бюджетных средств.

По различным оценкам среднее время выявления инцидента составляет 100 дней, что является достаточным для закрепления злоумышленника в информационно-коммуникационной инфраструктуре и последующих действий. Специалисты, обеспечивающие информационную безопасность, не всегда обладают навыками практического реагирования на угрозы и события информационной безопасности и зачастую имеют общее представление о мерах, которые необходимо предпринять после выявления инцидента.

Не проводятся регулярные тренинги, имитирующие кибератаки, которые могли бы продемонстрировать актуальные тенденции информационной безопасности и векторы атак злоумышленников. Это, наряду с нерелевантными настройками мониторинга информационной безопасности может привести к невозможности расследования инцидента или значительно его затруднить.

Новые технологические решения требуют больших инвестиций в развитие имеющихся навыков сотрудников государственных органов, наращивании их знаний и привитию культуры при работе с инструментами информационных технологий.

В этой связи в рамках данной исследовательской работы как одна из мер, способных улучшить состояние ИБ в государственном аппарате предлагается **создание и функционирование киберполигона.**

С целью повышения уровня информационной безопасности требуется развитие практических навыков кадрового состава сотрудников в сфере информационной безопасности. Мировой опыт показывает наличие и успешность внедрения платформ для проведения обучения ответственных за информационную безопасность. Создание киберполигона позволит организовать функционирование и осуществление деятельности Центра компетенции по информационной безопасности для обучения и тренировки студентов ВУЗов, специалистов и экспертов различных направлений, в том числе и руководящий состав.

Отрабатывая на практике методы противодействия кибератакам и реагирования на инциденты, сотрудники подразделений по информационной безопасности повышают свою готовность противодействовать реальным кибератакам. Обучение на базе киберполигона позволит IT-специалистам и сотрудникам служб кибербезопасности подготовиться к современным цифровым вызовам.

Таким образом, повышение уровня обеспечения ИБ Республики Казахстан путем внедрения площадки по обучению и повышению

квалификации для сотрудников, различных организаций и студентов ВУЗов РК является основным назначением Киберполигона.

Признанием эффективности киберполигона стало мероприятие «Cyberpolygon», проведенное в 2020 и 2021 годах при поддержке Центра кибербезопасности Глобального экономического форума и Интерпола. В онлайн-тренингах приняли участие представители более сотни компаний и нескольких десятков международных организаций.

Таблица 4 - Алгоритм разработки киберполигона

1	Внесение изменений в нормативные правовые акты *(Определить единого оператора по созданию и сопровождению киберполигона)*
2	Разработка ИП и ФЭО
3	Инициация проекта
4	Определение/набор проектной команды, создание рабочей группы по реализации проекта
5	Разработка плана мероприятий
6	Разработка технического задания
7	Приобретение серверного и телекоммуникационного оборудования
8	Написание исходного кода Киберполигона
9	Развертывание и конфигурация оборудование в Центре обработке данных
10	Обучение проектной команды
11	Функциональное и нагрузочное тестирование платформы
12	Ввод платформы Киберполигона в опытную эксплуатацию и проведение испытаний
13	Ввод платформы Киберполигона в промышленную эксплуатацию

Описание технологического процесса

Система обучения в Киберполигоне должен состоять из нескольких курсов, таких как основы кибербезопасности, старший специалист кибербезопасности, специалист по тестированию на возможность проникновения, специалист по сетевой криминалистике и киберразведка. На основании договорных отношений по проведению обучения по вышеуказанным курсам будет предоставлена возможность обучать сотрудников информационных технологий организаций и студентов Высших учебных заведений РК. По завершению обучения по каждому из курсов будет выдаваться сертификат.

Технические, информационные и математические средства и методы, используемые на практике

В настоящее время в Республике Казахстан отсутствует оптимизированная процедура обучения и повышения квалификации сотрудников. На практике деятельность осуществляется на основе договорных отношений с поставщиками услуг по обучению, что приводит к значительным финансовым и временным затратам для организаций.

При этом необходимо отметить, что в настоящее время на территории РК аналога такого решения как Киберполигон не имеется.

Сведения о существующей практике контроля и управления

На сегодняшний день государственный орган осуществляет обучение и повышение квалификации сотрудников путем заключения договоров с поставщиками услуг по обучению. В виду того, что на обучение необходимы финансовые средства количество обучаемых ограничено, что влечет за собой отсутствие возможности быстрого включения в процесс работы новоприбывших сотрудников. В следствие чего при действующей системе процесс обучения сотрудников и ввода в процесс работы занимает значительных временных, трудовых и финансовых ресурсов. Киберполигон позволит оптимизировать работу по проведению обучения и позволит значительно повысить скорость обнаружения и предотвращения инцидентов ИБ.

При этом, необходимо учесть, что в организациях отмечается острая нехватка квалифицированных кадров в сфере ИБ либо их слабые практические знания и понимание различных процессов в ИБ, что приводит к увеличению времени отработки и устранению инцидентов ИБ.

Эксплуатация киберполигона должна проводится в помещениях, не подверженных каким-либо вредным воздействиям и удовлетворяющих требованиям по установке средств вычислительной техники. Температурно-влажностный режим помещений, в которых установлен комплекс технических средств, практически не зависит от характеристик окружающей среды (для всех климатических условий Казахстана), отсутствуют технологические опасности и вредности (взрыво- и пожароопасность, агрессивные среды и т.п.). В связи с этим какие-либо особые требования к выбору.

Информационная инфраструктура Киберполигона должна быть построена с учетом следующих основных принципов:

– комплексное решение вопросов информационной безопасности;
– отказоустойчивости;
– открытость к развитию и адаптивность, включающая возможность в дальнейшем расширения состава предоставляемых Киберполигоном услуг путем внедрения дополнительной функциональности.

Киберполигон должен предоставлять предоставлять следующие возможности:

1) моделировать внештатные ситуации, связанные с возникновением угроз ИБ, для того что наработать навыки по отработке инцидентов информационной безопасности, расследовании компьютерных инцидентов и внедрению мер по исключению и предотвращению атак.

2) проведение обучений, тренировок студентов ВУЗов, специалистов и экспертов различных направлений, в том числе и руководящий состав а также организация различных кибертурниров.

3) тестирование ПО, оборудования, информационных элементов на реализацию функций ИБ, защищенность инфраструктуры и отсутствие уязвимостей, а также ложных срабатываний.

4) тестирование СЗИ на соответствие выдвигаемым требованиям по мощностям и функциональным возможностям, защищенность и наличие различных уязвимостей, способных нанести вред системе.

Учитывая вышеизложенное, наличие собственных платформ как киберполигон приведет к:

1) системному развитию кадрового потенциала Республики Казахстан в области информационной безопасности в выявлении угроз, расследовании инцидентов и рисков ИБ, разработка мер способных предотвратить реализацию угрозы наступления инцидента;

2) повышению уровня защищенности информационно-коммуникационной инфраструктуры ГО, аппаратно-программных комлпексов и применяемых в ГО программных обеспечений, а также сетей телекоммуникаций аппаратного обеспечения информационной, в том числе объектов КВОИКИ.

3) улучшению и оптимизации основы методического обеспечения, включающий описание процедур и процессов обеспечения информационной безопасности ГО в Республике Казахстан.

4) обеспечение взаимообмена и обучение лучшим практикам обеспечения ИБ между государственными органами и организациями, а также субъектами квазигосударственного сектора в Республике Казахстан.

5) развитию деятельности в области обучения в сфере ИБ, в том числе, предоставлению услуг коммерческим компаниям Республики Казахстан и компаниям государств Центральной Азии;

6) повышению рейтинга в глобальном рейтинге кибербезопасности, так одним из вопросов при оценке страны является наличие национальных отраслевых образовательных программ/тренингов/курсов для сотрудников. Киберполигон позволит учебным заведениям, осуществляющим теоретическую подготовку специалистов по направлению противодействие киберпреступности получать практические знания и навыки в области кибербезопасности;

7) развитию навыков, как теоритических так и практических, нацеленных на защиту от угроз ИБ, реагированию на компьютерных атаки и инциденты у специалистов, студентов, а также руководителей профильного направления.

8) повышению скорости исследований;

9) поиску и привлечению талантливых отечественных специалистов. Это будет достигнуто благодаря широкому охвату целевой аудитории и выявлению людей с наибольшим потенциалом развития;

10) обеспечению возможности для студентов и заинтересованных специалистов в определении направлений развития своих навыков по актуальным тематикам, связанным с информационной безопасностью. Это позволит расширить круг потенциальных специалистов в этой сфере.

11) уменьшению расходов на курсы обучения в сфере ИБ в связи с некоммерческой составляющей платформы.

ЗАКЛЮЧЕНИЕ

Основными векторами направлений в области государственного управления в мире являются дебюрократизации, уменьшение количества работников за счет автоматизации многих процедур и облегчению операционной деятельности, повсеместная оптимизация всех бизнес-процессов, развитие цифровой грамотности населения и в особенности работников государственных учреждений, развитие у работников компетенций и наращивание их навыков. При решение этих задач цифровизация является одним из основных факторов. Очевидно, что применение высокотехнологичных решений несомненно вызывает положительный эффект при противодействии коррупции за улучшения прозрачности процедур.

По мере развития цифровой отрасли в ближайшие годы резко возрастет потребность в обеспечении конфиденциальности и безопасности в виду непрерывного роста киберугроз и уязвимостей.

В рамках данной исследовательской работы проведен анализ состояния ИБ в государственных органах, наиболее распространенные риски ИБ и возникаемые угрозы и инциденты.

В контексте изучения состояния ИБ в ГО выявлено то, что Казахстан осуществляет собственную политику в целях укрепления информационной безопасности на национальном уровне. Так, согласно статистике ГИК, который оценивает уровень информационной безопасности государств, Казахстан в 2020 году занимает 31 место, и второе место среди стран СНГ. Однако, работу по улучшению состояния ИБ необходимо продолжать и дальше, а также предпринимать действия по усилению мер по обеспечению информационной безопасности и защите персональных данных, путем повышения стандартов ИБ и внедрению различных мер с учетом развития цифрового мира.

Наряду с предпринимаемыми мерами по обеспечению информационной безопасности в ходе исследования было выявлено, что на текущий момент в стране остро ощущается нехватка квалифицированных кадров, способных вынести ИБ в стране на новый уровень и которые имеют высокий уровень практических знаний в сфере в сфере информационной безопасности. Вышеуказанные проблемы несомненно связаны со слабой преподавательской системой в средних и высших учебных заведениях.

В виду этого необходимо отметить особую важность реализации киберполигона, который позволит моделировать ситуации любого уровня и сложности, что позволяет получить объективную оценку навыков и лучше подготовить персонал в случае возникновения нештатных ситуаций, создающих реальную угрозу.

Создание и внедрение киберполигона в широком смысле будет способствовать системному развитию кадрового потенциала в области информационной безопасности в расследовании компьютерных инцидентов, анализе существущих рисков ИБ, изучении критических событий, оптимизации бизнес-процессов и процедур IT а также касаемых обеспечения ИБ и взаимодействия между подразделениями, формировании мер, способных

отразить или предотвратить компьютерные атаки, и конечне же развитию практических навыков с целью защиты от несанкционированных доступов и других угроз ИБ у студентов и специалистов различных направлений, в том числе и руководителей.

Наличие собственных платформ позволит обеспечить развитие деятельности в области обучения в сфере ИБ, системное развитие кадрового потенциала в области ИБ, формирование практических навыков защиты от угроз ИБ, привлечение талантливых отечественных специалистов, повышение уровня защищенности программного и аппаратного обеспечения информационной и промышленной автоматизированной инфраструктуры РК, повышение рейтинга в глобальном рейтинге кибербезопасности, а также уменьшение расходов на курсы обучения в сфере ИБ в связи с некоммерческой составляющей платформы.

Тенденция на широкое использование цифровых технологий в системе государственного управления и бизнесе, а также дальнейшее развитие инфраструктуры должна обеспечить стране необходимый уровень инновационного и экономического потенциала. Однако по мере развития цифровой отрасли возникает также непрерывный рост киберугроз и уязвимостей. Злоумышленники наращивают свой потенциал и находят новые способы взлома. Таким образом, для борьбы с нарастающими киберугрозами необходимо расширение арсенала технических средств, развитие профессиональных навыков и создание эффективных процессов по обеспечению ИБ.

СПИСОК ЛИТЕРАТУРЫ

Закон Республики Казахстан. Об информатизации: утв. 24 ноября 2015 года, № 418-V.

Постановление Правительства Республики Казахстан. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: утв. 20 декабря 2016 года, № 832.

Постановление Правительства Республики Казахстан. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): утв. 30 июня 2017 года, № 407.

Постановление Правительства Республики Казахстан. Об утверждении Плана мероприятий по реализации Концепции кибербезопасности («Киберщит Казахстана») до 2022 года: утв. 28 октября 2017 года, № 676.

Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан. Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности: утв. 3 июня 2019 года, № 111/НҚ.

СТ РК ИСО/МЭК 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации».

СТ РК ИСО/МЭК 27005-2013 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».

Казахстан улучшил позиции в Глобальном индексе кибербезопасности// https://profit.kz/news/61580/Kazahstan-uluchshil-pozicii-v-Globalnom-indekse-kiberbezopasnosti/

Сайт Службы реагирования на компьютерные инциденты// https://www.cert.gov.kz/

Сайт Комитета по информационной безопасности МЦРИАП РК// https://www.gov.kz/memleket/entities/infsecurity?lang=ru.

Приложение 1

Аналитическая записка

Автор проекта: Искаков Медет Болатбекулы
Научный руководитель: Адалиев Нурлан Каиржанович

Идея проекта	Оценка рисков системы информационной безопасности в государственном аппарате
Проблемная ситуация (кейс)	Цифровая трансформация государства является частью реформы государственного управления. Текущая тенденция стремительного развития отрасли информационно-коммуникационных технологий цифровой среды повышает прозрачность, улучшает подотчетность и противодействие коррупции и в целом повышает эффективность деятельности государственных органов автоматизируя многие процессы. Новые реалии диктуют постоянное развитие цифровизации. Таким образом, цифровые технологии превращаются в ключевой фактор конкурентноспособности. Вместе с тем пропорционально увеличивается актвность киберпреступников и кибератак во всех сферах деятельности. Проблемы кибербезопасности становятся ежедневной угрозой, в том числе и для государственного аппарата. В рамках проводимой цифровизации государственными органами вопросам обеспечения информационной безопасности порой внимание уделяется по остаточному принципу.Темп развития цифровизации может на порядок опережать всевозможные предпринимаемые меры информационной безопасности. Уровень киберугроз и уязвимостей также непрерывно растет. Для минимизации фактов несанкционированного доступа, защиты информации, содержащихся в объектах информатизации «электронного правительства» от утечки и предотвращения возможности злонамеренных действий, к решению вопросов информационной безопасности необходимо уделять особое внимание. В этой связи возникает необходимость в комплексной оценке существующих в

	государственных органах рисков информационной безопасности и разработке дополнительных мер по снижению рисков информационной безопасности.
Имеющиеся решения данной проблемы	Казахстан осуществляет собственную политику в целях укрепления информационной безопасности на национальном уровне. Так например, утверждена Концепция кибербезопасности «Киберщит Казахстана», призванная реализовать комплекс мер, которые направлены на поддержку информационной безопасности пользователей сети и казахстанского сегмента Интернета в целом. Также в период с 2018 по 2022 год в Казахстане реализовывалась Государственная программа «Цифровой Казахстан». Помимо этого существуют нормативные правовые акты, регламентирующие требования при создании, развитии, сопровождении и эксплуатации объектов информатизации государственных органов. Помимо этого, с целью обеспечения ИБ на уровне страны предпринимаются следующие меры: 1. Перед процедурой ввода в промышленную эксплуатацию объектов информатизации проводится испытание на соответствие требованиям ИБ; 2. В 2018 году в стране начал функционировать Национальный координационный центр информационной безопасности при акционерном обществе «Государственная техническая служба», который обеспечивает защиту информационных ресурсов и объектов информатизации ГО и КВОИКИ от кибератак и является главным элементом в системе обеспечения информационной безопасности в масштабе страны. 3. Осуществляется МОИБ объектов информатизации «электронного правительства», основной целью которого является контроль за реализацией владельцами ОИ ЭП технических и других мероприятий по обеспечению ИБ посредством выявления угроз и инцидентов информационной безопасности. 4. Осуществляется МСИБ, основной целью которого является мониторинг за состоянием ОИ с целью обнаружения инцидентов ИБ; 5. Обеспечивается создание и функционирование

	собственного ОЦИБ в своей структуре или приобретение услуги ОЦИБ у других лиц, осуществляющие деятельность по идентификации, оценке, нейтрализации, отражению и профилактике угроз ИБ ИКИ государственных органов и организаций квазигосударственного сектора; 6. Для поддержания соответствующего уровня защищенности государственных ЭИР, ИС и ИКИ Республики Казахстан от внешних и внутренних угроз 4 июня 2019 года был организован ККС по информационной безопасности в состав которых входят специалисты технического направления ГО и организаций; Для защиты интернет-ресурсов государственных органов используется оборудование ЕШДИ, который представляет из себя АПК призванных защищать сети телекоммуникаций при доступе к Интернету или сетям связи, имеющим выход в сеть интернет. ЕШДИ представляет из себя своеобразный фильтр, очищающий трафик от разного рода атак и не допускает их воздействия на ИКИ государственных органов а также на информационные ресурсы. 7. С целью осуществления государственной политики в сфере информационной безопасности и защиты персональных данных создан уполномоченный орган осуществляющий регулятивные, реализационные и контрольные функции области обеспечения информационной безопасности.
Предлагаемое решение данной проблемы	Наряду с предпринимаемыми мерами по обеспечению информационной безопасности предлагается создание киберполигона для повышения практических навыков работников в сфере IT и информационной безопасности. Основное назначение Киберполигона - повышение уровня обеспечения информационной безопасности Республики Казахстан путем внедрения площадки по обучению и повышению квалификации для сотрудников, различных организаций и студентов ВУЗ РК. Мировой опыт показывает наличие и успешность внедрения платформ для проведения обучения ответственных за информационную безопасность.

	Создание киберполигона позволит организовать функционирование и осуществление деятельности Центра компетенции по информационной безопасности для обучения студентов, специалистов и разных профилей, в том числе и руководителей в области ИБ и IT передовым методам обеспечения ИБ. Отрабатывая на практике методы противодействия кибератакам и реагирования на инциденты, сотрудники подразделений по информационной безопасности повышают свою готовность противодействовать реальным кибератакам. Обучение на базе киберполигона позволит IT-специалистам и сотрудникам служб кибербезопасности подготовиться к современным цифровым вызовам.
Ожидаемый результат	Наличие собственных платформ как киберполигон приведет к: 1) снижению рисков и угроз ИБ в государственном секторе; 2) повышению уровня общественного доверия и безопасности граждан; 3) эффективному предотвращению, выявлению и реагированию на современные угрозы; 4) развитие кадрового потенциала в области информационной безопасности; 5) повышению уровня защищенности информационно-коммуникационной инфраструктуры ГО, аппаратно-программных комлпексов и применяемых в ГО программных обеспечений, а также сетей телекоммуникаций аппаратного обеспечения информационной, в том числе объектов КВОИКИ; 6) улучшению и оптимизации основы методического обеспечения, включающий описание процедур и процессов обеспечения информационной безопасности ГО в Республике Казахстан; 7) обеспечение взаимообмена и обучение лучшим практикам обеспечения ИБ между государственными органами и организациями, а также субъектами квазигосударственного сектора в Республике Казахстан; 8) развитию деятельности в области обучения в сфере ИБ, в том числе, предоставлению услуг

	коммерческим компаниям Республики Казахстан и компаниям государств Центральной Азии; 9) повышению рейтинга в глобальном рейтинге кибербезопасности, так одним из вопросов при оценке страны является наличие национальных отраслевых образовательных программ/тренингов/курсов для сотрудников. Киберполигон позволит учебным заведениям, осуществляющим теоретическую подготовку специалистов по направлению противодействие киберпреступности получать практические знания и навыки в области кибербезопасности; 10)развитию навыков, как теоритических так и практических, нацеленных на защиту от угроз ИБ, реагированию на компьютерных атаки и инциденты у специалистов, студентов, а также руководителей профильного направления; 11)повышению скорости исследований; 12)поиску и привлечению талантливых отечественных специалистов. Это будет достигнуто благодаря широкому охвату целевой аудитории и выявлению людей с наибольшим потенциалом развития; 13)обеспечению возможности для студентов и заинтересованных специалистов в определении направлений развития своих навыков по актуальным тематикам, связанным с информационной безопасностью. Это позволит расширить круг потенциальных специалистов в этой сфере; 14)уменьшению расходов на курсы обучения в сфере ИБ в связи с некоммерческой составляющей платформы.
Литература	Закон Республики Казахстан. Об информатизации: утв. 24 ноября 2015 года, № 418-V. Постановление Правительства Республики Казахстан. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: утв. 20 декабря 2016 года, № 832. Постановление Правительства Республики Казахстан. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): утв. 30 июня 2017 года, № 407. Постановление Правительства Республики Казахстан. Об утверждении Плана мероприятий по

	реализации Концепции кибербезопасности («Киберщит Казахстана») до 2022 года: утв. 28 октября 2017 года, № 676. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан. Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности: утв. 3 июня 2019 года, № 111/НҚ. СТ РК ИСО/МЭК 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации». СТ РК ИСО/МЭК 27005-2013 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности». Казахстан улучшил позиции в Глобальном индексе кибербезопасности// https://profit.kz/news/61580/Kazahstan-uluchshil-pozicii-v-Globalnom-indekse-kiberbezopasnosti/ Сайт Службы реагирования на компьютерные инциденты// https://www.cert.gov.kz/ Сайт Комитета по информационной безопасности Министерства цифрового развития инноваций и аэрокосмической промышленности// https://www.gov.kz/memleket/entities/infsecurity?lang=ru