МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**Аналитическая записка к документу «Good Practice. Information security 2019/2020»**

Выполнил: Деспотащвили Илья

Группа: 191-351

**Список терминов и сокращений**

ИБ – информационная безопасность.

Толерантность к риску – уровень риска, который организация может принять на собственное удержание для достижения операционных и финансовых целей.

ПО – программное обеспечение.

**Введение.**

Рассматриваемый в данной работе документ разработан компанией DNB и представляет собой практическое руководство по осуществлению мероприятий по обеспечению целостности, конфиденциальности и безопасности электронной обработки данных.

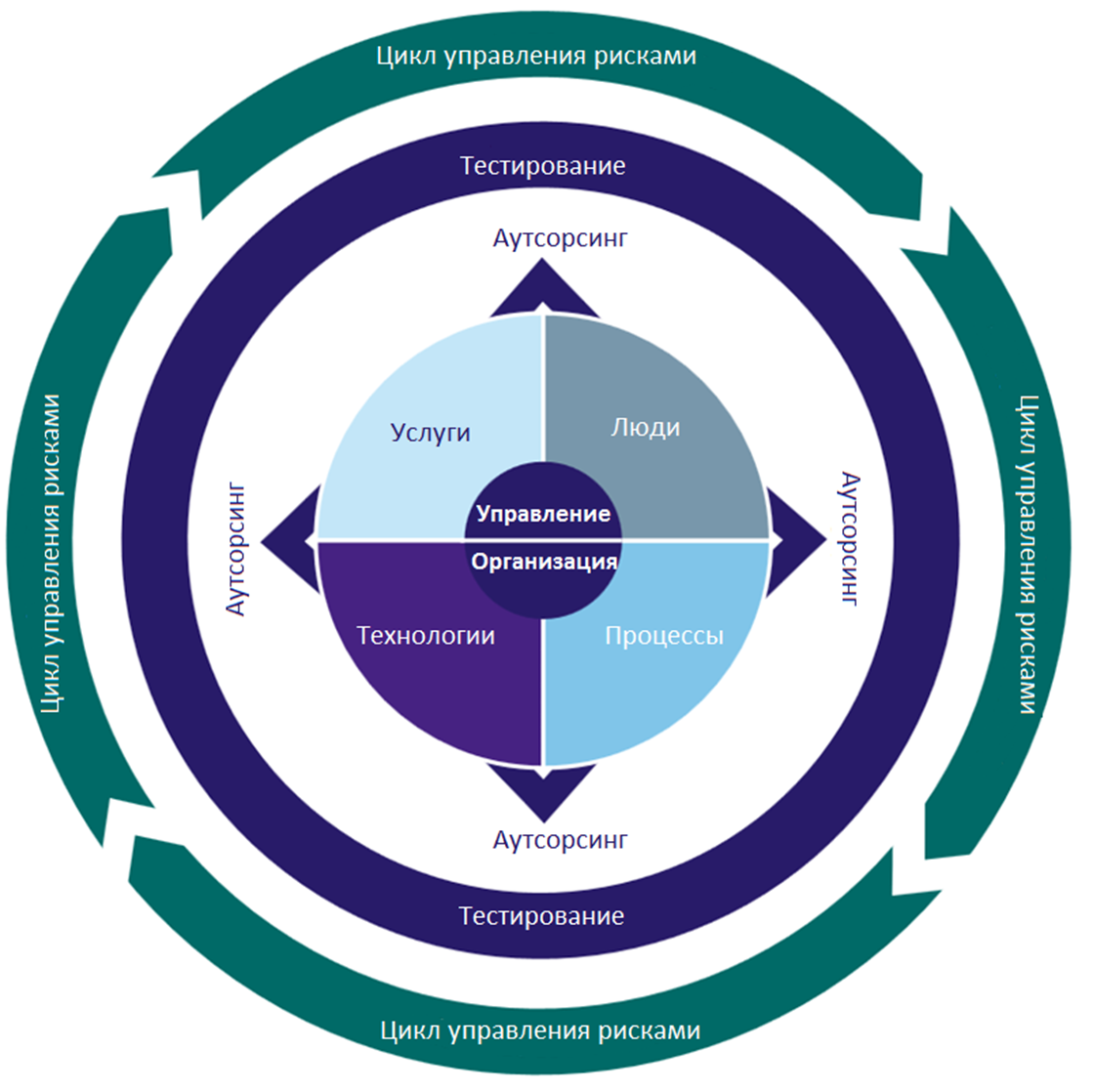
На основе анализа рисков организации осуществляют меры контроля, направленные на управление их информационной безопасностью. Эти меры контроля должны соответствовать характеру, масштабу и сложности рисков, связанных с деятельностью организации и сложностью его организационного состава. Эти меры контроля не ограничиваются технологическими решениями, они также обращаются к человеческим действиям, процессам и к физической безопасности.

Кроме того, учитывая меняющиеся риски ИБ, организации оценивают наличие и эффективность мер контроля и при необходимости улучшают и заменяют их.

Кроме того, организации гарантируют, что они контролируют информационную безопасность в отношении деятельности по аутсорсингу, и проверяют свою устойчивость к киберугрозам.

Рассматриваемый документ включает в себя модель зрелости, используемую для оценки уровней управления рисками ИБ в организациях, которые аудирует компания DNB.

Документ базируется на следующей модели:



Рассмотрим каждый элемент подробнее.

**Управление.** Управление - это стратегическое, тактическое и оперативное управление информационной безопасностью и кибербезопасностью в соответствии со стратегией организации, толерантности к риску и применимыми законодательными и нормативными требованиями. Учитываются характер, размер и сложность организации.

В отношении данного элемента проверяется, разработала ли организация политику ИБ, как она реализуется и поддерживается в актуальном состоянии, а также переводится ли она в комплексный план информационной безопасности с четким распределением задач и обязанностей и формальными линиями отчетности. Также проверяется, каким образом данная политика преобразована в различные меры.

Меры контроля – 1.1, 1.2, 2.1, 2.2, 3.1, 3.2.

**Организация.** Организация - это распределение обязанностей и ответственности в отношении информационной безопасности внутри организации. Распределение должно быть четким и недвусмысленным, а любые связанные с ним действия должны соответствовать стратегии организации, её толерантности к риску и применимым законодательным и нормативным требованиям.

Для данного элемента проверяется действующая документация и формализация ролей и обязанностей по управлению рисками и функциями информационной безопасности.

Также проверяется четкое распределение бизнес-владельцев данных и информационных систем, которые использует организация. Проверяется управление правами доступа организации к данным и информационным системам в соответствии с принципом разделения обязанностей в соответствии со структурой внутреннего контроля организации.

Меры контроля – 5.1, 5.2, 6.1, 7.1.

**Люди.** Данный элемент означает, что все сотрудники, внешний персонал и поставщики услуг ознакомлены с политикой ИБ организации и осведомлены о своих обязанностях по соблюдению ИБ, а также о том, что они работают в соответствии с этой политикой и допустимой степенью риска организации.

Для данного элемента проверяется способность организации обучать персонал и поддерживать его уровень знаний, которые соответствуют её целям и профилю рисков. Ожидается, что организация будет инвестировать в образование и обучение сотрудников, чтобы постоянно обновлять знания своего персонала в области ИБ.

Меры контроля – 8.1, 8.2, 8.3, 8.4, 8.5, 9.1, 9.2, 9.3.

**Процессы.** Процессы - это обеспечение надежного оперативного управления. Процессы необходимы для контроля рисков, связанных с информационной безопасностью.

Для данного элемента важно, чтобы организация разработала план обеспечения непрерывности ИТ и постоянно обновляла этот план. Цель плана - ограничить влияние серьезного сбоя на ключевые функции и процессы организации и обеспечить непрерывность её работы во время сбоев или кибератак. Проверяется, существует ли в организации формальная политика управления инцидентами, включая процедуру эскалации и критерии эскалации. Об инцидентах кибербезопасности необходимо сообщать в соответствующие органы в соответствии с применимыми законами и нормативными актами.

Меры контроля – 10.1, 10.2, 10.3, 10.4, 10.5, 11.1, 11.2, 11.3, 11.4, 12.1, 12.2, 12.3, 13.1, 13.2, 15.1, 15.2, 16.1, 16.2, 16.3, 16.4, 16.5, 17.1, 17.2.

**Технологии.** Технологии - это принятие технических мер для контроля и обеспечения информационной безопасности.

Здесь проверяется, применяются ли меры технического контроля, гарантирующие высокий уровень информационной безопасности, и что анализ рисков организации учитывает текущие киберугрозы.

Организация должна реализовывать превентивные, обнаруживающие и корректирующие меры для защиты своих ИТ-систем от кибератак, таких как вирусы, вредоносное ПО, шпионское ПО и DDoS-атаки.

Меры контроля – 18.1, 18.2, 18.3, 18.4, 18.5, 19.1, 19.2, 19.3, 20.1.

**Объекты.** Элемент «Объекты» - это обеспечение физической безопасности доступа к данным, например меры по ограничению доступа в офисные здания и дата-центры.

Для элемента «Объекты» проверяется, разработала и внедрила ли организация политику, которая регулярно обновляется и соответствует профилю риска организации в отношении следующих аспектов:

1. физическая безопасность офисных зданий, территорий и важных мест ИТ-инфраструктуры, таких как центры обработки данных и серверные комнаты.
2. доступ к зданиям и местам, которые имеют решающее значение для операционных процессов организации.

Меры контроля – 21.1, 21.2.

**Аутсорсинг.** Аутсорсинг - это использование услуг третьих сторон для управления важными операционными процессами, такими как ИТ, управление активами и клиентами, финансовое администрирование.

В случае передачи деятельности на аутсорсинг, организация по-прежнему несет полную ответственность за информационную безопасность и кибербезопасность. Для элемента «Аутсорсинг» проверяется, есть ли в организации процесс, обеспечивающий, по крайней мере, следующее:

* Организация заключила соглашения с поставщиком услуг об обеспечении соблюдения политики информационной безопасности организации и, если применимо, о выполнении плана информационной безопасности. То же самое применимо и в том случае, если эти работы выполняются на субподряде.
* Организация получает отчеты об уровне услуг (SLR) и / или отчеты о гарантиях, на основе которых можно отслеживать соглашения.
* Организация вмешивается, когда ее допустимые уровни риска превышаются (см. Цикл управления рисками).

Меры контроля – 14.1, 14.2, 16.3.

**Тестирование.** Тестирование безопасности обеспечивают эффективное улучшение информационной безопасности организации на постоянной основе. Тесты безопасности могут применяться к различным элементам модели. Тесты могут использоваться для выявления слабых мест в инфраструктуре организации (Технологии), а также в человеческом поведении и человеческих действиях (Люди) или в доступе к зданиям (Объекты).

Для данного элемента контролируется, чтобы организация определяла тесты безопасности, которые необходимо выполнить, а также их объем и глубину на основе анализа рисков и текущих киберугроз. Характер и частота тестирования зависят от профиля риска организации.

Также проверяется, удостоверилась ли организация, что сторона, проводящая данные тесты, имеет соответствующие знания и опыт, а также имеет сертификат.

Меры контроля – 22.1.

**Цикл управления рисками.** Цикл управления рисками применяется ко всем элементам модели. Организация должна выявлять и анализировать соответствующие риски ИБ на регулярной основе. На основе анализа рисков организация определяет свои дальнейшие действия, принимает меры по снижению рисков и (временно) принимает остаточные риски.

Для данного элемента проверяется следующее:

* Внедрила ли организация Систему управления ИТ-рисками для обеспечения контроля над рисками ИБ.
* Использует ли организация единое определение информационной безопасности в своей структуре управления ИТ-рисками на основе рыночных стандартов, таких как NIST, ISO и COBIT, и что они единообразно используются во всех документах и отчетах организации.
* Проводит ли организация периодические оценки рисков на основе качественных и количественных методов, с помощью которых анализируются текущие киберугрозы и определяется их приоритетность.
* Разработала ли организация план действий по устранению неприемлемых рисков, в котором излагаются меры реагирования на риски. План действий по рискам должен быть одобрен руководством и соответствовать характеру и масштабу любых остаточных рисков.

Меры контроля – 4.1, 4.2, 4.3.

**Модель зрелости.**

Организации, находящиеся под контролем DNB, должны периодически проводить самооценки, которые измеряют уровни операционной зрелости организаций.

Цель самооценки - установить, находится ли их контроль над информационной безопасностью на требуемом уровне. Для определения этого уровня мы используем модель зрелости.

Для каждого из вышеперечисленных элементов модели используются определенные меры контроля, которые перечислены в документе. Общее их количество – 58. Это соответствует уровню зрелости не менее 3.

При выполнении самооценки организация должна принять во внимание определения из таблицы ниже.

|  |  |  |
| --- | --- | --- |
| **№** | **Определение уровня зрелости** | **Пояснительные критерии** |
| 0 | **Не существует** - этому элементу управления не уделяется внимание. |  |
| 1 | **Начальный** - элемент управления (частично) определен, но выполняется непоследовательно. Реализация / выполнение контроля сильно зависит от людей | * Контроль отсутствует или ограничен. * Отсутствие контроля или выполнение специального контроля. * Контроль не / частично задокументирован. * Реализация / исполнение зависит от отдельных лиц |
| 2 | **Повторяемый, но интуитивно понятный** - управление на месте и выполняется структурированно и последовательно, но неформальным образом. | Реализация контроля основана на неформальном, но стандартизированном подходе. Этот подход не полностью задокументирован. |
| 3 | **Определенный** - контроль документируется и выполняется структурированным и формальным образом. Выполнение контроля может быть доказано и проверено. | * Контроль определяется на основе оценки риска. * Управление документировано и формализовано. * Обязанности и задачи четко распределены. * План, наличие и эффективность работы очевидны. * Операционная эффективность контроля периодически проверяется. * Оценка операционной эффективности средств контроля основана на оценке риска и демонстрирует, что контроль эффективен в течение более длительного периода времени (> 6 месяцев). * О реализации контроля сообщается руководству. |
| 4 | **Управляемый и измеримый** - периодически оценивается эффективность контроля. При необходимости этот элемент управления улучшается или заменяется другим элементом (ами). Оценка оформляется документально. | * Периодическая (контрольная) оценка и наблюдение. * Оценки оформляются документально. * Формализованы задачи и обязанности по переоценке средств контроля. * Периодичность оценки зависит от профиля риска организации и проводится не реже одного раза в год. * При оценке учитываются производственные происшествия. * Результаты оценки сообщаются руководству. |
| 5 | **Непрерывное совершенствование** - контроль встроен в целостную структуру управления рисками организации, которая обеспечивает непрерывный и эффективный контроль и решение проблем с рисками. Внешние данные и сравнительный анализ используются для поддержки постоянного поиска улучшений. Сотрудники активно участвуют в повышении эффективности средств контроля. | * Непрерывная оценка средств контроля с целью постоянного повышения их эффективности. * Использование результатов самооценки, анализа пробелов и анализа первопричин. * Средства контроля сравниваются на основе внешних данных и являются «лучшей практикой» по сравнению с другими организациями. |

Далее в данном документе перечисляются определенные меры контроля для каждого элемента модели, приведенной выше.

**Меры контроля.**

**1.1 План информационной безопасности**

* Организация разработала свою политику информационной безопасности в соответствии с международно признанными стандартами, такими как ISO 27001 и структура кибербезопасности NIST.
* Политика информационной безопасности включает превентивные, детективные, корректирующие и подавляющие меры.
* Политика информационной безопасности учреждения описывает как технические меры ИТ, так и процедурные меры в операционных процессах.
* Организация обновляет свою политику информационной безопасности с фиксированной частотой, которая соответствует характеру и размеру организации (например, каждые два года), и увеличивает частоту, когда это необходимо, например, в случае слияний и поглощений, крупного аутсорсинга или новых киберугроз.
* Благодаря программам повышения осведомленности сотрудники организации знакомятся с политикой информационной безопасности и знают свои роли и обязанности в этом отношении.

**1.2 Управление ИТ-политиками**

* Организация описала и/или настроила рабочие процессы ИТ так, чтобы гарантировать правильное выполнение этих рабочих процессов и процедур ИТ.
* Процедуры основаны на международно признанных стандартах, таких как ITIL, BISL и PRINCE II.
* Организация обновляет свои рабочие процессы и процедуры ИТ с фиксированной периодичностью, соответствующей характеру и размеру организации, и увеличивает частоту, когда это необходимо. Если возникают новые киберугрозы или интенсивность киберугроз возрастает, учреждение оценивает необходимость ужесточения рабочих процессов и процедур ИТ.
* Организация проверяет, в какой степени его сотрудники соблюдают рабочие процессы ИТ и насколько они осведомлены о том, что надлежащее выполнение их действий способствует информационной безопасности и устойчивости к киберугрозам.

**2.1 Модель информационной архитектуры предприятия**

* Информационная архитектура учреждения разъясняет, как ИТ-системы и сбор данных поддерживают операционную стратегию и процессы учреждения.
* Информационная архитектура учреждения основана на международно признанных стандартах, таких как TOGAF и DYA.
* Организация разработала видение, показывающее, как его ИТ-системы и организационная структура будут развиваться в поддержку его среднесрочной и долгосрочной операционной стратегии, включая обзор ключевых зависимостей от третьих сторон / партнеров.
* Организация применяет архитектурные принципы, направленные на обеспечение простого, гибкого, надежного и безопасного предоставления информации уполномоченному персоналу, клиентам и третьим сторонам.

**2.2 Схема классификации данных**

* Организация создала таблицу классификации данных на основе рисков, в которой все ИТ-системы и данные классифицируются по таким категориям, как высокий / средний / низкий риск и общедоступные / конфиденциальные / секретные.
* Организация принимает меры, основанные на этой классификации.
* Организация отслеживает расположение центров обработки данных, в которых хранятся её критически важные для бизнеса данные. Организация проверяет, что эти центры обработки данных соответствуют её политике информационной безопасности.
* Организация использует программное обеспечение DLP для активного отслеживания исходящего трафика конфиденциальных данных через сеть учреждения и отслеживания того, соответствует ли он классификации данных.

**3.1 Мониторинг будущих тенденций и правил**

* Сотрудники активны на интернет-форумах и / или подписаны на информационные бюллетени по кибербезопасности.
* Организация является членом профессиональных или других отраслевых ассоциаций, которые обмениваются знаниями и опытом в области ИБ, например ISAC.
* Организация заключила договорные соглашения со своими ключевыми партнерами по аутсорсингу о сотрудничестве и обмене информацией в области информационной безопасности.

**3.2 Технологические стандарты**

* Организация работает по общепринятым техническим стандартам в области информационной безопасности (ISO 27001, структура кибербезопасности NIST и / или SANS). Они адаптированы к характеру и размеру организации.
* Сотрудников информируют о необходимости работать в соответствии с установленными стандартами, и они осведомлены о стандартах, относящихся к их работе.
* Новые ИТ-системы и изменения существующих ИТ-систем соответствуют установленным стандартам.
* Организация следит за соблюдением установленных стандартов.

**4.1 Структура управления ИТ-рисками**

* Организация разрабатывает и поддерживает структуру управления ИТ-рисками.
* Структура управления ИТ-рисками соответствует общей концепции управления рисками организации.
* Организация рассматривает риски информационной безопасности в своей концепции управления ИТ-рисками.
* Организация установила допустимые уровни риска в отношении информационной безопасности.

**4.2 Оценка риска**

* Организация периодически проводит анализ ИТ-рисков на основе качественных и количественных методов.
* Текущие киберугрозы включены в анализ ИТ-рисков.
* Об остаточных рисках сообщается для (временного) утверждения руководству, которое имеет отношение к характеру и масштабу этих остаточных рисков.
* Принятые остаточные риски периодически переоцениваются для принятия, если они выходят за пределы допустимых для организации пределов риска.

**4.3 Ведение и мониторинг плана действий по рискам**

* Организация составляет план действий в отношении неприемлемых рисков с подробным описанием мер реагирования организации на риски.
* План действий по рискам описывает любые остаточные риски и включает компенсирующие меры.
* Остаточные риски ИБ являются частью плана действий организации.
* План действий по рискам утверждается на уровне управления, который соответствует характеру и масштабу остаточных рисков.
* План действий по рискам актуален, и последующие действия отслеживаются.

**5.1 Ответственность за риск, безопасность и комплаенс**

* Конечная ответственность за управление рисками информационной безопасности лежит на высшем уровне управления организации.
* Обязанности и ответственность функций управления рисками и информационной безопасности формализованы и задокументированы.
* Сотрудники организации осознают, что они несут ответственность за соблюдение процессов и процедур безопасности.

**5.2 Управление информационной безопасностью**

* Для управления рисками информационной безопасности учреждение разработало цикл PDCA («Планируй - Выполняй - Проверяй - Действуй»).
* Выполнение цикла основано на рисках, согласовано с целями учреждения и в соответствии с пределами допустимого риска учреждения.

**6.1 Владение данными и системой**

* Организация четко распределила права собственности на данные и информационные системы, которые она использует в своем оперативном управлении.
* Данные и информационные системы классифицируются соответствующим владельцем системы. Меры борьбы установлены в соответствии с этой классификацией (см. 2.2).

**7.1 Разделение обязанностей**

* Учреждение установило формальную матрицу разделения обязанностей.
* Подробное разделение обязанностей основывается на анализе рисков, внедряется и утверждается высшим руководством учреждения
* Организация периодически оценивает реализацию разделения обязанностей в своих ИТ-системах. Промежуточная оценка проводится после серьезных изменений в ИТ-системах.
* Организация ограничивает количество учетных записей с высокими привилегиями до минимума. Такой подход предотвратит небезопасные комбинации ролей и прав доступа и связанные с ними риски.
* Учреждение применяет двухфакторную аутентификацию для учетных записей с высокими привилегиями доступа (например, учетных записей администратора).
* Организация не разрешает использование общих учетных записей, кроме как с особого разрешения высшего руководства.

**8.1 Набор и удержание персонала**

* Организация набирает персонал, обладающий знаниями в области информационной безопасности, что соответствует ее целям и профилю рисков.
* Организация инвестирует в образование и обучение, чтобы постоянно обновлять знания своих сотрудников в области информационной безопасности.

**8.2 Компетенции персонала**

* Знания и компетенции в области информационной безопасности сотрудников и лиц, определяющих политику ИБ, соответствуют целям организации (цифровым).
* Регулярно проводятся оценки для определения степени, в которой знания и компетенции сотрудников и политиков в области информационной безопасности соответствуют целям организации.

**8.3 Зависимость от людей**

* Организация провела инвентаризацию процессов / действий, которые имеют решающее значение для ее бизнес-операций, если они зависят от ограниченного числа сотрудников.
* На основе анализа рисков организация определила, где зависимость от отдельных лиц превышает допустимую степень риска.
* Организация приняла меры по ограничению чрезмерной зависимости от отдельных лиц до предела толерантности к риску.

**8.4 Процедуры проверки персонала**

* Перед назначением сотрудники проходят проверку на основе профиля рисков, связанных с их работой.
* Они также регулярно проходят эту проверку во время работы.
* Вышесказанное относится как к постоянным, так и к временным сотрудникам.

**8.5 Смена работы и увольнение**

* Если персонал меняет должность, то права ИТ-системы меняются как можно быстрее. Если сотрудники больше не имеют права доступа на новую должность, права немедленно аннулируются.
* При увольнении с работы система прав и права на процессы немедленно отменяются. Также должно быть уделено должное внимание правам доступа к системам / услугам, которые не входят в компетенцию учреждения, например, интернет-порталам или облачным приложениям, на которые сотрудник (бывший) подписан через учреждение.

**9.1 Передача знаний конечным пользователям**

* Сотрудники обладают знаниями и опытом для правильного использования ИТ-приложений и систем в соответствии с процедурами и рабочими инструкциями организации.
* Сотрудники знают, как информационные технологии поддерживают критически важные бизнес-процессы, и знают о технологических рисках, связанных с информационной безопасностью. Сотрудники применяют эти знания в своей повседневной деятельности.

**9.2 Передача знаний производственному и вспомогательному персоналу**

* ИТ-сотрудники обладают знаниями и опытом для разработки, приобретения, внедрения и администрирования приложений и систем в соответствии с процедурами и рабочими инструкциями учреждения.
* ИТ-сотрудники знают, как информационные технологии поддерживают критически важные бизнес-процессы, и знают о технологических рисках, связанных с информационной безопасностью. ИТ-сотрудники применяют эти знания в своей повседневной деятельности.
* ИТ-сотрудники активно используют свои специализированные знания для выявления рисков информационной безопасности и киберугроз, а также для принятия соответствующих мер по управлению ими.

**9.3 Осведомленность сотрудников**

* Существуют руководящие принципы и кодексы поведения, касающиеся информационной безопасности. С ними знакомы сотрудники на всех уровнях учреждения.
* Повышение осведомленности о безопасности является частью политики информационной безопасности, которая также устанавливает программу повышения осведомленности о безопасности с явным вниманием к рискам кибербезопасности.
* Базовые знания об информационной безопасности и киберугрозах широко распространены среди руководства учреждения и исполнительного руководства.
* Руководство и сотрудники знают, как действовать, когда они подозревают наличие инцидентов в области информационной безопасности.

**10.1 Изменение стандартов и процедур**

* Изменения в ИТ-приложениях, ИТ-инфраструктуре, ИТ-процессах и критических системных учреждениях следуют стандартизированному и контролируемому пути.
* В отношении рассмотрения и утверждения запросов на изменение изложены обязанности и ответственность.
* Изменения, включающие исправления безопасности, являются приоритетными.
* Воздействие и риски от изменений в информационной безопасности оцениваются до внедрения изменения.
* Эксперты по безопасности участвуют в рассмотрении изменений, влияющих на меры защиты информации.
* Изменения в критических системах и инфраструктуре не запрашиваются, не утверждаются и не выполняются одним и тем же лицом (разделение обязанностей).
* Изменения регистрируются (в контрольном журнале) и оцениваются.

**10.2 Оценка воздействия, приоритезация и авторизация**

* Оценивается влияние запросов на изменение на операционные ИТ-системы.
* В процессе принятия решений по запросам на изменение принимаются во внимание последствия для информационной безопасности.

**10.3 Тестовая среда**

* Установлены и соблюдаются критерии защиты данных для тестирования.
* Доступ к тестовым и производственным ИТ-системам строго разделен.
* У организации есть среда, в которой можно проверить эффективность мер безопасности.

**10.4 Тестирование изменений**

* Изменения в ИТ-инфраструктуре и ИТ-приложениях тестируются перед использованием.
* Тестирование проводится в соответствии с планом тестирования, который устанавливает критерии приемлемости для информационной безопасности и производительности ИТ.
* На основе оценки рисков измененные ИТ-системы сканируются на предмет их уязвимости к киберугрозам.

**10.5 Продвижение в производство**

* Есть управляемая передача изменений в производственных системах.
* Организация использует систему документооборота для контролируемой передачи и регистрации изменений в производственной среде.
* Наиболее важные стороны, вовлеченные в системные изменения, такие как пользователи, владелец системы, функциональные и технические администраторы, участвуют в процессе утверждения изменений.
* На основе анализа рисков учреждение определяет, требуется ли новая система или модифицированная система, работающая параллельно с унаследованной системой. Если изменения рискованные, у организации есть запасной план.

**11.1 Планы обеспечения непрерывности ИТ**

* Организация подготовила план непрерывности, чтобы ограничить влияние серьезного сбоя на ключевые операционные функции и процессы.
* Доступны альтернативные варианты обработки и восстановления для всех критически важных ИТ-сервисов.
* План обеспечения непрерывности ИТ учитывает непрерывность мер кибербезопасности и бесперебойное продолжение функций информационной безопасности во время сбоев и кибератак.
* План обеспечения непрерывности ИТ направлен на устойчивость к DDoS-атакам.

**11.2 Тестирование плана обеспечения непрерывности ИТ**

* Проводится регулярное тестирование плана обеспечения непрерывности ИТ для обеспечения эффективного восстановления ИТ-систем, устранения недостатков и сохранения актуальности плана.
* Проводится тестирование устойчивости к DDoS-атакам и другим кибератакам, влияющим на доступность.
* Тестирование мер непрерывности охватывает всю цепочку систем и приложений, поддерживающих критически важные бизнес-процессы.

**11.3 Внешнее хранилище резервных копий**

* Организация имеет более одного места для хранения данных, необходимых для надежного оперативного управления.
* Профиль риска мест должен быть таким, чтобы ни одно бедствие не могло затронуть оба места одновременно.
* Содержание резервной копии определяется владельцами бизнес-процессов и ИТ-персоналом.
* Учреждение регулярно оценивает полноту и правильность данных.
* Управление данными в различных местах (резервное копирование, зеркалирование данных) осуществляется в соответствии с политикой классификации данных учреждения.
* Проводится тестирование и обновление совместимости аппаратного и программного обеспечения для восстановления архивных данных и периодически архивируемых данных.

**11.4 Резервное копирование и восстановление**

* В организации созданы и внедрены процедуры резервного копирования и восстановления ИТ-систем, ИТ-приложений, данных и документации.
* Организация приняла меры для обнаружения и снижения вероятности киберугроз, направленных на резервное копирование.

**12.1 Условия хранения**

* У организации есть политика в отношении хранения и архивирования данных. Она периодически обновляется и проверяется.
* В организации определены и внедрены процедуры хранения и архивирования данных в соответствии с бизнес-целями.
* При хранении данных учитываются законодательные требования в отношении сроков хранения данных.

**12.2 Утилизация**

* В организации определены и внедрены процедуры, обеспечивающие выполнение бизнес-требований по защите конфиденциальных данных и программного обеспечения при удалении или передаче данных и оборудования.

**12.3 Требования безопасности для управления данными**

* Организация определила и внедрила политику и процедуры для безопасного получения, обработки, хранения и предоставления данных в соответствии с политикой организации.

**13.1 Репозиторий конфигурации и базовый план**

* Организация осуществляет всесторонний надзор за ИТ-активами, от которых зависят ее бизнес-процессы.
* Организация имеет представление о конфигурации (параметрах) ИТ-активов.
* Организация оценивает рекомендации поставщиков по безопасному проектированию ИТ-инфраструктуры и ИТ-приложений и устанавливает и документирует, как она безопасно конфигурирует свои ИТ-активы (базовые параметры).

**13.2 Идентификация и обслуживание элементов конфигурации**

* Изменения в базе данных управления конфигурацией (CMDB) (см. Контрольную меру 13.1) производятся контролируемым образом. Это означает, что любые изменения согласовываются и регистрируются. В организации описана процедура управления конфигурацией
* CMDB интегрирована с процедурами управления изменениями, управления инцидентами и управления проблемами.

**14.1 Мониторинг и отчетность о достижениях уровня обслуживания**

* Организация согласовала конкретные количественные и качественные критерии эффективности со своими поставщиками услуг, которые сообщают об этом организации.
* Отчеты поставщиков услуг анализируются для выявления как положительных, так и отрицательных тенденций и изменений как для конкретных, так и для общих услуг учреждения. Об этих тенденциях и изменениях информируется ответственное линейное руководство.

**14.2 Управление рисками поставщика**

* Выявлены и уменьшены риски, связанные с непрерывным и надежным предоставлением услуг поставщиками услуг.
* Контракты составляются в соответствии с отраслевыми стандартами и соответствуют всем требованиям законодательства.
* Управление рисками организации оценивает постоянную доступность критически важных услуг, предоставляемых поставщиками услуг, варианты отката для альтернативных способов продолжения услуг, предоставляемых поставщиками услуг, и соответствие стандартам в области информационной безопасности.

**15.1 Определение инцидента безопасности**

* Организация применяет четкое определение инцидентов безопасности, которое известно всем заинтересованным сторонам в учреждении.
* В процессе управления инцидентами, инциденты кибербезопасности классифицируются и определяются индивидуально, чтобы обеспечить быстрое реагирование на такие инциденты и наличие необходимых знаний.
* В организации установлены процедуры, касающиеся сообщения об инцидентах кибербезопасности, реагирования на кибербезопасность и ограничения любого ущерба, причиненного в результате инцидентов.
* Об инцидентах, связанных с кибербезопасностью, сообщается руководству в соответствии с применимыми правилами.

**15.2 Эскалация инцидента**

* В организации действует формальная политика управления инцидентами, включая процедуру эскалации и критерии эскалации.
* Процедура эскалации основана на согласованных уровнях обслуживания для инцидентов, которые не могут быть немедленно разрешены.
* Категоризация и приоритезация происходит на основе анализа воздействия, определенных критериев и уровней обслуживания.
* Существует обучение реагированию на инциденты информационной безопасности.
* О серьезных инцидентах сообщается руководству.
* В организации осведомлены о процедурах эскалации, и они соблюдаются.
* То, как разрешаются инциденты, регулярно анализируется для улучшения процессов и ИТ-систем.

**16.1 Тестирование, наблюдение и мониторинг безопасности**

* В организации приняты и задокументированы меры безопасности. Эти меры тестируются и периодически оцениваются, поэтому они продолжают соответствовать установленным базовым требованиям безопасности.
* В ИТ-системах осуществляется мониторинг необычных действий, исключения отмечаются и отслеживаются.

**16.2 Мониторинг системы внутреннего контроля**

* Организация управляет ИТ-рисками и рисками в области информационной безопасности. С этой целью организация создала систему внутреннего контроля ИТ, которая включает политику информационной безопасности, стандарты, процедуры, (ключевые) средства контроля и общие средства контроля ИТ в соответствии с целями организации.
* Организация регулярно оценивает структуру, наличие и эффективность системы внутреннего контроля.

**16.3 Внутренний контроль у третьих лиц**

* При подготовке контрактов организация уделяет внимание тому, как поставщик услуг продолжает соблюдать договорные обязательства, законы и постановления, а также механизмы отчетности и мониторинга.
* Организация формирует мнение о мерах внутреннего контроля у своих поставщиков услуг и любых субподрядчиков.
* Поставщик услуг соблюдает законодательные или договорные положения.
* Организация заключила договор о том, что аутсорсинг не будет препятствовать надзору по всей цепочке.

**16.4 Оценка соответствия внешним требованиям**

* Организация регулярно оценивает, соответствуют ли его ИТ-политика и процедуры законам и постановлениям.

**16.5 Независимое заверение**

* Организация получает регулярные периодические заверения о том, как функционируют средства контроля ИТ. Сюда входит гарантия эффективности мер внутреннего контроля в области информационной безопасности.
* Результаты этой независимой оценки представляются руководству организации.

**17.1 Управление идентификацией и доступом**

* Доступ к информационным системам и данным организации можно отследить до уникально идентифицируемых людей (внутренних, внешних и инсорсинговых) или до ИТ-служб (таких как сценарии и пакетные задания) с однозначно идентифицируемым владельцем.
* Организация создала, утвердила и установила доступ к информационным системам (матрицы авторизации SOLL) на основе необходимого разделения функций и бизнес-правил (см. Контрольную меру 7.1).
* Настройка безопасности логического доступа (матрицы авторизации SOLL) регулярно оценивается.
* Доступ к информационным системам и данным учреждения контролируется и отслеживается в ИТ-инфраструктуре и ИТ-приложениях в соответствии с согласованными матрицами авторизации SOLL.
* Права доступа в ИТ-системах (IST) регулярно сравниваются с матрицами авторизации SOLL.

**17.2 Управление учетной записью пользователя**

* Предоставление, изменение или аннулирование прав доступа к информационным системам и данным основано на формализованных этапах, на которых одобрение предоставляется владельцами соответствующих бизнес-процессов, информационных систем и данных.
* Разделение обязанностей или принцип «четырех глаз» не позволяют одному человеку выполнить вышеупомянутые шаги.
* Все действия, связанные с предоставлением, изменением или отменой прав доступа, могут быть отслежены людьми.
* Права доступа людей, увольняющихся с работы в организации, удаляются или блокируются как можно быстрее.

**18.1 Защита и доступность ресурсов инфраструктуры**

* Меры контроля в компонентах ИТ-инфраструктуры настроены таким образом, чтобы гарантировать высокий уровень доступности, конфиденциальности и целостности.
* Ответственность за разработку и внедрение этих мер контроля четко определена.
* Разработка и реализация этих мер контроля отслеживаются и оцениваются.

**18.2 Обслуживание инфраструктуры**

* Техническое обслуживание ИТ-инфраструктуры носит структурный и плановый характер в соответствии с процедурами управления изменениями в организации.
* Организация классифицировала компоненты инфраструктуры, сделав различие между критическими и менее важными компонентами.
* При расстановке приоритетов и проведении технического обслуживания ИТ-инфраструктуры учитывается классификация компонентов инфраструктуры.
* Решения для устранения уязвимостей в ИТ-инфраструктуре, такие как исправления, влияют на приоритизацию деятельности по обслуживанию ИТ-инфраструктуры.
* Должны соблюдаться процессы управления изменениями и должно рассматриваться управление исправлениями для критических и менее критических уязвимостей. Это основано на анализе рисков, который является частью процесса управления изменениями (оценка рисков изменений - CRA).
* В CRA уделяется особое внимание киберугрозам. Они влияют на расстановку приоритетов и внедрение изменений.
* Повышенное внимание учреждения к качеству обслуживания клиентов и времени выхода на рынок не ведет к откладыванию мер безопасности инфраструктуры и инвестиций в технологии.

**18.3 Управление криптографическими ключами**

* Ключи шифрования управляются определенным способом. Организация установила политику и процедуры в отношении создания, изменения, отзыва, уничтожения, распространения, сертификации, хранения, установки, использования и архивирования ключей шифрования.
* Выявляются риски модификации и раскрытия ключей во время этих процессов и принимаются меры по их снижению.
* Организация осознает риски кибератак, направленных на изменение и перехват ключей шифрования, и приняла соответствующие меры для управления этим.

**18.4 Сетевая безопасность**

* Организация применяет современные технические меры безопасности (такие как межсетевые экраны, сегментация сети и обнаружение вторжений) и связанные с ними процессы управления, чтобы ограничить доступ к ИТ-инфраструктуре для уполномоченного персонала, ИТ-службам и обмену информацией между сетями.
* Авторизация для администраторов ИТ-инфраструктуры, включая администраторов сети, надежно настроена (см. Меры контроля 17.1 и 17.2).

**18.5 Обмен конфиденциальными данными**

* В организации действует политика, устанавливающая правила обмена конфиденциальной информацией.
* В организации есть средства, позволяющие обмениваться конфиденциальной информацией по защищенным каналам.

**19.1 Предотвращение, обнаружение и исправление вредоносных программ**

* Организация внедрила превентивные, обнаруживающие и корректирующие меры для защиты своих ИТ-систем от киберугроз, таких как вирусы, вредоносное ПО, черви, криптовалюта, шпионское ПО, криптоджекинг.

**19.2 Управление уязвимостями**

* Наиболее важные ИТ-активы определяются на основе анализа рисков.
* На основе анализа угроз и сканирования уязвимостей организация регулярно выполняет проверки ИТ-активов, чтобы установить, существуют ли кибер-уязвимости, и определяет их влияние на свои процессы.
* Действия по снижению риска определяются для тех угроз, которые выходят за рамки допустимого риска организации.

**19.3 Управление жизненным циклом приложения**

* Обслуживание приложений - это структурированный и запланированный процесс в соответствии с процедурами управления изменениями в организации.
* Учреждение проверяет, что ИТ-инфраструктура и ИТ-приложения, которые оно использует, поддерживаются разработчиком / поставщиком и доступны ли обновления безопасности (патчи).
* Решения для уязвимостей в приложениях, такие как исправления, влияют на приоритизацию регулярного обслуживания ИТ-приложений.

**20.1 Защита технологии безопасности**

* Организация знает, какие технологии безопасности имеют к ней отношение.
* Принимая во внимание изначально высокий профиль риска, к технологии безопасности применяются особые меры безопасности.
* Документация о технологии безопасности и мерах безопасности предоставляется только по служебной необходимости.

**21.1 Меры физической безопасности**

* Организация определила и внедрила политику физической безопасности офисных зданий, территорий и местоположений ИТ-инфраструктуры, таких как центры обработки данных и серверные комнаты.
* Меры безопасности физического доступа соответствуют профилю рисков организации.
* Меры безопасности физического доступа регулярно проверяются.

**21.2 Физический доступ**

* Организация определила и внедрила политику безопасности зданий, территорий, зон, центров обработки данных и серверных комнат, которые имеют решающее значение для операционных процессов организации.
* Профили доступа согласованы с руководством. Доступ к зданиям, площадям, зонам и серверным комнатам зависит от должности и обязанностей сотрудника / посетителя.
* Организация регулярно проверяет эффективность мер физического доступа и сообщает о результатах руководству. Также включена оценка предоставленных прав доступа (SOLL-IST) и оценка регистрации системы безопасного доступа.

**22.1 Тестирование на проникновение и этический взлом**

* На основе анализа рисков и текущих киберугроз организация определяет тесты безопасности, которые необходимо выполнить, а также их объем и глубину.
* Характер и частота этих тестов зависят от профиля риска учреждения. Они могут включать следующие типы тестов безопасности: тестирование на проникновение, этический взлом и / или Red Teaming.
* Организация гарантирует, что сторона, проводящая тесты безопасности, обладает соответствующими знаниями, опытом, сертификатами и рекомендациями.