КГУ «Управление архитектуры, градостроительства и земельных отношений города Нур-Султан»

УТВЕРЖДЕНО

Директор ТОО «АстанаГорАрхитектура» города Нур-Султан

_____ Кенжебеков Н. К.

М. П.

«__19__» _____октября_____ 20__20__г.

УТВЕРЖДЕНО

Руководитель Управления архитектуры, градостроительства и земельных отношений города Нур-Султан

_____ Уранхаев Н. Т.

М. П.

«__18__» _____октября_____ 20__20__г.

Правила проведения внутреннего аудита информационной безопасности Информационной системы «Геоинформационный портал города Нур-Султан» ГПГ.СМИБ.ПР.06.r02.20

г. Нур-Султан
2020 г.

1. Область применения

Целью настоящего документа является описание правил проведения внутреннего аудита информационной безопасности и определение порядка действий ответственных сотрудников Организации, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта обеспечения работы ИС.

Настоящий документ применим к любой деятельности, относящейся к аудиту информационной безопасности проекта ИС.

2. Нормативные ссылки

Настоящий документ содержит указания к практическому исполнению требований, изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

3. Термины, определения и сокращения

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

4. Общие положения

Настоящий документ рассматривает два вида проверок (аудита):

a) внутренний аудит – проводится в соответствии с утвержденным графиком рабочей группой из состава сотрудников Организации; внутренний аудит производится с целью проверки соблюдения требований действующих документов по информационной безопасности сотрудниками, клиентами, поставщиками, пользователями ИС Организации.

b) внешний аудит – проводится по инициативе руководства Организации с привлечением сторонних специалистов обладающими соответствующими навыками и опытом и проводится с целью определения пригодности, адекватности и эффективности самого подхода Организации к управлению информационной безопасностью, а также пригодности, адекватности и эффективности применяемых методов и мер по обеспечению ИБ.

Внутренний аудит ИБ должен проводиться не реже одного раза в год в соответствии с Графиком аудита информационной безопасности (по форме Приложения 1), а также в случае выявления инцидентов ИБ требующих корректировки методов обеспечения информационной безопасности.

Периодичность проведения внутреннего аудита ИБ определяется руководством на основе потребностей в такой деятельности.

Плановый аудит на предмет исполнения и соблюдения требований ИБ проводится согласно утвержденному плану-графику планового аудита, который составляется ежегодно.

Контроль нецелевого использования средств обработки информации (пп. 15.1.5 Политики ИБ) осуществляется ответственным за обеспечение ИБ в рамках внутреннего аудита, но не реже четырех раз в год. Установленная периодичность контроля должна быть отражена в Графике аудита информационной безопасности.

Результаты аудита подлежат документированию, а связанные с ним записи должны быть сохранены.

Порядок организации и управления информационной безопасностью и ее реализация (например, изменения целей и мер управления, политики, процессов и процедур обеспечения информационной безопасности) должны подвергаться аудитам через определенные промежутки времени или при появлении существенных изменений в способах реализации мер безопасности.

Если в результате аудита выявляется, что осуществление подхода организации по управлению информационной безопасностью является недостаточным или не соответствует направлению информационной безопасности, определенные в документированной политике информационной безопасности, то руководству необходимо предпринять корректирующие действия.

В методах аудита могут использоваться опросы руководства, проверка записей или анализ документирования политики информационной безопасности и других документов по ИБ.

На усмотрение руководства Организации результаты аудита могут стать причиной внепланового пересмотра Политики информационной безопасности или других действующих документов по ИБ.

В настоящем документе описаны требования к мероприятиям по обеспечению информационной безопасности операционной среды и инструментальных средств аудита в процессе проведения аудита систем с целью повышения эффективности процесса аудита информационных систем и снижение негативного влияния, связанного с данным процессом.

Защита также требуется для поддержания целостности информационной системы и предотвращения неправильного использования инструментальных средств аудита.

5. Порядок проведения внутреннего аудита

Ответвленный сотрудник за обеспечение информационной безопасности составляет график проведения внутреннего аудита (по форме Приложения 1), составляет предложение участников рабочей группы, согласовывает с заинтересованными подразделениями Организации и вносит на утверждение руководству Организации.

Для проведения внутреннего аудита ИБ должна быть подобрана рабочая группа. руководителем Организации должен быть назначен

руководитель рабочей группы, ответственный за проведение мероприятий по аудиту ИБ. При наличии только одного аудитора, последний должен выполнять все предусмотренные обязанности руководителя рабочей аудиторской группы.

При определении размера и состава рабочей группы должны учитываться:

1) цели, предмет аудита ИБ, критерии аудита и его ориентировочная продолжительность;

2) общая компетентность и уровень квалификации рабочей группы;

3) необходимость исполнения принципов проведения аудита ИБ;

4) законодательные, регламентирующие, контрактные требования и требования органов аккредитации/сертификации, если применимо;

5) способность членов рабочей группы к совместной работе и к эффективному взаимодействию с проверяемой организацией;

6) понимание особенностей структурных подразделений Организации (это может быть достигнуто либо собственным опытом аудитора, либо с помощью эксперта).

Если в определенной области (по определенному вопросу) знаний рабочей группы недостаточно, то недостающие знания и умения могут быть восполнены включением в группу экспертов. Эксперты должны работать под руководством аудитора.

Руководителем рабочей группы назначается руководитель Организации, секретарем совещаний назначается ответственный за обеспечение ИБ.

График внутреннего аудита (по форме согласно Приложению 1), состав рабочей группы, роли руководителя и секретаря утверждаются приказом руководства Организации. В приказе должна быть отражена поддержка руководства Организации беспрепятственному проведению внутреннего аудита информационной безопасности, выделению финансовых и человеческих ресурсов для совершенствования обеспечения ИБ там, где это оправдано и необходимо.

Руководитель рабочей группы на первом совещании распределяет среди ее участников компоненты системы управления информационной безопасностью, секретарь совещания составляет график заседаний рабочей группы по аудиту компонентов СМИБ.

Полученные документы прикладываются к протоколу совещания, согласуются всеми участниками и утверждаются руководством Организации.

Ответственный за обеспечение ИБ сотрудник отвечает за соблюдение сроков утвержденного графика внутреннего аудита, секретарь рабочей группы отвечает за соблюдение сроков графика совещаний. В случае нарушения сроков об этом должно быть уведомлено руководство Организации для принятия мер стимуляции процесса аудита. Выбор способов стимуляции находится в ответственности руководства Организации и должен соответствовать законодательству РК.

Все выявленные нарушения требований действующих в Организации документов по ИБ выносятся на рассмотрение рабочей группы с указанием документа и пункта, которому они противоречат, указанием причин нарушения, предложением действий для исправления и предложением соответствующих корректирующих действий для недопущения повторных нарушений и с предложением исполнителей этих действий.

Все принятые замечания протоколируются, согласовываются участниками рабочей группы и хранятся у секретаря.

По окончании внутреннего аудита компонентов СМИБ секретарь составляет отчет проведения внутреннего аудита, график применения исправлений и корректирующих действий с указанием ответственных лиц. График согласуется рабочей группой и утверждается руководством Организации.

Ответственность за соблюдение графика применения исправлений и корректирующих действий, и применения исправлений, и корректирующих действий возлагается на ответственного за обеспечение ИБ сотрудника.

6. Порядок проведения внешнего аудита

Внешний аудит инициируется руководством Организации. Такой аудит необходим для обеспечения постоянной пригодности, адекватности и эффективности подхода организации по управлению информационной безопасностью. Аудит должен включать оценку возможностей для улучшения и необходимости изменений в подходе к безопасности, включая политику, цели и меры управления.

При инициировании внешнего аудита, руководство Организации дает поручение ответственному за обеспечение ИБ сотруднику определить границы проведения внешнего аудита и критерии оценки состояния СМИБ. Полученные результаты с обоснованием выносятся на согласование структурным подразделениям Организации, подвергающимся аудиту.

Области, подлежащие регулярному пересмотру внутренними аудиторами, могут также рассматриваться при независимой проверке (аудите).

Согласованные границы проведения внешнего аудита и критерии оценки состояния СМИБ служат основанием для выбора исполнителя способного выполнить внешний аудит.

В случае наличия на рынке более одного потенциального поставщика услуг выбор производится в соответствии с установленным в Организации порядком.

С выбранным Исполнителем заключается договор с соблюдением всех требований действующего порядка Организации и действующих документов по информационной безопасности.

Исполнитель, при участии ответственного за обеспечение ИБ сотрудника, составляет график проведения внешнего аудита, составляет

предложение участников рабочей группы, согласовывает с подразделениями Организации, подвергающихся аудиту, и вносит на утверждение руководству Организации.

В состав рабочей группы должны входить компетентные представители подразделений Организации, подвергающихся аудиту, ответственный за обеспечение ИБ сотрудник, ответственные представители Исполнителя.

Руководителем рабочей группы назначается представитель Исполнителя, секретарем совещаний назначается ответственный за обеспечение ИБ.

График внешнего аудита, состав рабочей группы, роли руководителя и секретаря утверждаются приказом руководства Организации. В приказе должна быть отражена поддержка руководства Организации беспрепятственному проведению внешнего аудита информационной безопасности, выделению финансовых и человеческих ресурсов для совершенствования обеспечения ИБ там, где это оправдано и необходимо.

Руководитель рабочей группы на первом совещании распределяет среди сотрудников Исполнителя компоненты СМИБ подвергающиеся аудиту, секретарь совещания составляет график заседаний рабочей группы по аудиту.

Полученные документы прикладываются к протоколу совещания, согласуются всеми участниками и утверждаются руководством Организации.

Ответственный за обеспечение ИБ сотрудник отвечает за соблюдение сроков утвержденного графика внешнего аудита, секретарь рабочей группы отвечает за соблюдение сроков графика совещаний. В случае нарушения сроков об этом должно быть уведомлено руководство Организации для принятия мер стимуляции процесса аудита. Выбор способов стимуляции находится в ответственности руководства Организации и должен соответствовать договорным отношениям с Исполнителем и законодательству РК.

Все выявленные Исполнителем нарушения выносятся на рассмотрение рабочей группы с указанием документа и пункта, которому они противоречат, указанием причин нарушения, предложением действий для исправления и предложением соответствующих корректирующих действий для недопущения повторных нарушений и с предложением исполнителей этих действий.

Все принятые замечания протоколируются, согласовываются участниками рабочей группы и хранятся у секретаря.

По окончании внешнего аудита компонентов СМИБ Исполнитель составляет отчет проведения внешнего аудита, график применения исправлений и корректирующих действий с указанием ответственных лиц. График согласуется рабочей группой и утверждается руководством Организации.

Ответственность за соблюдение графика применения исправлений и корректирующих действий возлагается на ответственного за обеспечение ИБ сотрудника.

7. Меры управления аудитом информационных систем

Требования и процедуры аудита, включающие в себя проверки операционных систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск прерывания бизнес-процессов.

Ответственный за обеспечение ИБ должен учитывать следующие условия при планировании аудита:

a) требования аудита необходимо согласовать с руководством Организации;

b) объем работ и время проведения проверок следует согласовывать с руководителями структурных подразделений и контролировать;

c) при проведении проверок необходимо использовать доступ только для чтения к программному обеспечению и данным;

d) другие виды доступа могут быть разрешены только в тестовой среде с фиктивными данными;

e) необходимо четко идентифицировать и обеспечивать доступность необходимых ресурсов информационных систем для выполнения проверок;

f) требования в отношении специальной или дополнительной обработки данных следует идентифицировать и согласовывать;

g) весь доступ должен повергаться мониторингу и регистрироваться с целью обеспечения протоколирования для последующих ссылок;

h) все процедуры, требования и обязанности аудита следует документировать;

i) лицо, выполняющее аудит, должно быть независимым от проверяемой деятельности.

7.1 Требования по предоставлению доступа аудиторам

При предоставлении доступа аудиторам к информационным ресурсам ИС необходимо выполнять следующие требования:

a) доступ аудиторов должен быть контролируем и прослеживаться ответственным за обеспечение ИБ;

b) доступ аудиторов к информационным ресурсам ИС должен оговариваться заранее для подготовки необходимых мер обеспечения ИБ;

c) при проведении проверок необходимо использовать доступ только для чтения к программному обеспечению и данным;

d) допуск в служебные помещения проекта ИС должен осуществляться только по письменному запросу и только в присутствии ответственного за обеспечение ИБ;

e) предоставление запрашиваемой аудитором информации в электронном виде или на бумажных носителях должен осуществляться

только с разрешения руководства Организации в присутствии ответственного за обеспечение ИБ;

f) запрос о доступе аудиторов должен быть обоснован, в запросе должны быть указаны сведения о лицах, которым будет предоставлен доступ;

g) электронные копии или копии на бумажных носителях могут передаваться только с разрешения руководства Организации по акту приемо-передачи;

h) доступ аудитора к ресурсам ИС должен быть аннулирован сразу же после окончания работ;

i) ответственным за обеспечения ИБ в процессе доступа аудиторов к ИС назначается Ответственный за обеспечение ИБ.

Менеджер проекта ИС обязан:

a) своевременно информировать своих сотрудников о предстоящем аудите;

b) обеспечить рабочие места для аудиторов и осуществимость аудита;

c) предоставлять необходимую документацию по требованию аудитора;

d) своевременно устранять несоответствия, выявленные в ходе аудита и выявлять их причины;

e) организовать работы по выявлению причин каждого несоответствия, подготовку и осуществление корректирующих действий по результатам аудита.

8. Требования к инструментальному аудиту

При проведении аудитов ИБ может применяться соответствующее инструментальное обеспечение, обладающее следующим функционалом:

a) выявление уязвимостей программного обеспечения, опубликованных разработчиками ПО или определяемых встроенными алгоритмами;

b) автоматизировать процесс оценки степени выполнения требований ИБ с учетом их важности;

c) оценивать эффективность различных вариантов защитных мер;

d) автоматизировать процессы анализа идентифицированных и зафиксированных системами мониторинга ИБ событий;

e) генерировать документальные отчеты с результатами выполнения различных процедур.

В случае отсутствия инструментального обеспечение должны применяться встроенные механизмы проверки в операционную систему ИС.

9. Защита инструментальных средств аудита информационных систем

В случае использования, инструментальные средства аудита подлежат обязательной защите и контролируемому авторизованному

доступу для предотвращения любой возможности их неправильного использования или компрометации.

Ответственным за защиту инструментальных средств аудита является ответственный за обеспечение ИБ.

Инструментальные средства должны быть отделены от среды функционирования ИС и для удобства использования и быстрого реагирования должны располагаться на рабочей станции системного администратора.

В качестве инструментальных средств аудита могут использоваться штатные утилиты операционной системы. В этом случае они должны быть установлены на серверном оборудовании ИС.

В случае если сторонняя организация, выполняющая аудит, использует инструментальные средства, ее действия должны контролироваться ответственным за обеспечение ИБ и менеджером проекта.

10. Ответственность

СОИБ несет ответственность за:

a) контроль исполнения требований настоящего документа,
b) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

a) исполнение настоящей Инструкции.

Приложение 1

График аудита информационной безопасности Информационной системы «Геоинформационный портал города Нур-Султан» на 2020-2021 гг. ГПГ.СМИБ.ПР.06-01.r02.20

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Введение														СОИБ
2. Область действия														СОИБ
3. Нормативные ссылки														СОИБ
4. Применяемые термины и сокращения														СОИБ
5. Цели и задачи Политики информационной безопасности														СОИБ
5.1. Цели														СОИБ
5.2. Задачи														СОИБ
5.3. Документирование политики информационной безопасности														СОИБ
5.4. Пересмотр политики информационной безопасности														СОИБ
5.4.1. Процедура пересмотра политики информационной безопасности														СОИБ
6. Организация информационной безопасности														СОИБ
6.1. Внутренняя организация														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
6.1.1. Обязанности руководства по обеспечению информационной безопасности														СОИБ
6.1.2. Координация вопросов обеспечения информационной безопасности														СОИБ
6.1.3. Распределение обязанностей по обеспечению информационной безопасности														СОИБ
6.1.4. Процедура получения разрешения на использование средств обработки информации														СОИБ
6.1.5. Соглашения о соблюдении конфиденциальности														СОИБ
6.1.6. Взаимодействие с компетентными органами														СОИБ
6.1.7. Взаимодействие с ассоциациями и профессиональными группами														СОИБ
6.1.8. Независимая проверка (аудит) информационной безопасности														СОИБ
6.2. Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам														СОИБ
6.2.1. Определение рисков, связанных со сторонними организациями														СОИБ
6.2.2. Процедура предоставления доступа сторонним организациям и частным лицам														СОИБ
6.2.3. Рассмотрение вопросов безопасности при работе с клиентами														СОИБ
6.2.4. Рассмотрение требований безопасности в соглашениях со сторонними организациями														СОИБ
7. Управление активами														СОИБ
7.1. Ответственность за защиту активов организации														СОИБ
7.1.1. Инвентаризация активов														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
7.1.2. Ответственность за активы														СОИБ
7.1.3. Приемлемое использование активов														СОИБ
7.2. Классификация информации														СОИБ
7.2.1. Основные принципы классификации														СОИБ
7.2.2. Маркировка и обработка информации														СОИБ
8. Правила безопасности, связанные с персоналом														СОИБ
8.1. Перед трудоустройством														СОИБ
8.1.1. Функции и обязанности персонала по обеспечению безопасности														СОИБ
8.1.2. Проверка при приеме на работу														СОИБ
8.1.3. Условия трудового договора														СОИБ
8.2. Работа по трудовому договору														СОИБ
8.2.1. Обязанности руководства														СОИБ
8.2.2. Осведомленность, обучение и переподготовка в области информационной безопасности														СОИБ
8.2.3. Дисциплинарная практика														СОИБ
8.3. Прекращение или изменение действия трудового договора														СОИБ
8.3.1. Ответственность по окончании действия трудового договора														СОИБ
8.3.2. Возврат активов														СОИБ
8.3.3. Аннулирование прав доступа														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
9. Физическая защита и защита от воздействия окружающей среды														СОИБ
9.1. Охраняемые зоны														СОИБ
9.1.1. Периметр физической безопасности														СОИБ
9.1.2. Контроль доступа в охраняемую зону														СОИБ
9.1.3. Обеспечение безопасности зданий, производственных помещений и оборудования														СОИБ
9.1.4. Защита от внешних угроз и угроз со стороны окружающей среды														СОИБ
9.1.5. Выполнение работ в охраняемых зонах														СОИБ
9.1.6. Зоны общественного доступа, приема и отгрузки материальных ценностей														СОИБ
9.2. Безопасность оборудования														СОИБ
9.2.1. Размещение и защита оборудования														СОИБ
9.2.2. Вспомогательные услуги														СОИБ
9.2.3. Безопасность кабельной сети														СОИБ
9.2.4. Техническое обслуживание оборудования														СОИБ
9.2.5. Обеспечение безопасности оборудования, используемого вне помещений организации														СОИБ
9.2.6. Безопасная утилизация (списание) или повторное использование оборудования														СОИБ
9.2.7. Вынос имущества														СОИБ
10. Управление передачей данных и операционной деятельностью														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
10.1. Операционные процедуры и обязанности														СОИБ
10.1.1. Документальное оформление операционных процедур														СОИБ
10.1.2. Контроль изменений														СОИБ
10.1.3. Разграничение обязанностей														СОИБ
10.1.4. Разграничение средств разработки, тестирования и эксплуатации														СОИБ
10.2. Управление поставкой услуг лицами и/или сторонними организациями														СОИБ
10.2.1. Оказание услуг														СОИБ
10.2.2. Мониторинг и анализ услуг, оказываемых сторонними лицами и/или организациями														СОИБ
10.2.3. Изменения при оказании сторонними организациями услуг по обеспечению безопасности														СОИБ
10.3. Планирование производительности и загрузки систем														СОИБ
10.3.1. Управление производительностью														СОИБ
10.3.2. Приемка систем														СОИБ
10.4. Защита от вредоносного кода и мобильного кода														СОИБ
10.4.1. Меры защиты от вредоносного кода														СОИБ
10.4.2. Меры защиты от мобильного кода														СОИБ
10.5. Резервирование														СОИБ
10.5.1. Резервное копирование														СОИБ
10.6. Управление безопасностью сети														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
10.6.1. Средства контроля сети														СОИБ
10.6.2. Безопасность сетевых сервисов														СОИБ
10.7. Обращение с носителями информации														СОИБ
10.7.1. Управление съемными носителями информации														СОИБ
10.7.2. Утилизация носителей информации														СОИБ
10.7.3. Процедуры обработки информации														СОИБ
10.7.4. Безопасность системной документации														СОИБ
10.8. Обмен информацией														СОИБ
10.8.1. Политики и процедуры обмена информацией														СОИБ
10.8.2. Соглашения по обмену информацией														СОИБ
10.8.3. Защита физических носителей информации при транспортировке														СОИБ
10.8.4. Электронный обмен сообщениями														СОИБ
10.8.5. Системы бизнес-информации														СОИБ
10.9. Услуги электронной торговли														СОИБ
10.9.1. Электронная торговля														СОИБ
10.9.2. Транзакции в режиме реального времени (on-line)														СОИБ
10.9.3. Общедоступная информация														СОИБ
10.10. Мониторинг														СОИБ
10.10.1. Ведение журналов аудита														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
10.10.2. Мониторинг использования средств обработки информации														СОИБ
10.10.3. Защита информации журналов регистрации														СОИБ
10.10.4. Журналы регистрации действий администратора и оператора														СОИБ
10.10.5. Регистрация неисправностей														СОИБ
10.10.6. Синхронизация часов														СОИБ
11. Контроль доступа														СОИБ
11.1. Бизнес-требования к контролю доступа														СОИБ
11.1.1. Политика контроля доступа														СОИБ
11.2. Управление доступом пользователей														СОИБ
11.2.1. Регистрация пользователей														СОИБ
11.2.2. Управление привилегиями														СОИБ
11.2.3. Управление паролями пользователей														СОИБ
11.2.4. Пересмотр прав доступа пользователей														СОИБ
11.3. Ответственность пользователей														СОИБ
11.3.1. Использование паролей														СОИБ
11.3.2. Оборудование, оставленное пользователем без присмотра														СОИБ
11.3.3. Политика «чистого стола» и «чистого экрана»														СОИБ
11.3Б Политика использования сетей и сетевых услуг, передачи информации, подключения к Интернету, сетям телекоммуникаций и связи и использования беспроводного доступа к сетевым ресурсам														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
11.4. Контроль сетевого доступа														СОИБ
11.4.1. Политика в отношении использования сетевых услуг														СОИБ
11.4.2. Аутентификация пользователей для внешних соединений														СОИБ
11.4.3. Идентификация оборудования в сетях														СОИБ
11.4.4. Защита диагностических и конфигурационных портов при удаленном доступе														СОИБ
11.4.5. Принцип разделения в сетях														СОИБ
11.4.6. Контроль сетевых соединений														СОИБ
11.4.7. Управление маршрутизацией сети														СОИБ
11.5. Контроль доступа к операционной системе														СОИБ
11.5.1. Безопасные процедуры регистрации с терминала														СОИБ
11.5.2. Идентификация и аутентификация пользователя														СОИБ
11.5.3. Система управления паролями														СОИБ
11.5.4. Использование системных утилит														СОИБ
11.5.5. Периоды бездействия в сеансах связи														СОИБ
11.5.6. Ограничение времени соединения														СОИБ
11.6. Контроль доступа к прикладным системам и информации														СОИБ
11.6.1. Ограничение доступа к информации														СОИБ
11.6.2. Изоляция систем, обрабатывающих важную информацию														СОИБ
11.7. Работа с переносными устройствами и работа в дистанционном														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
режиме														
11.7.1. Работа с переносными устройствами и средствами связи														СОИБ
11.7.2. Работа в дистанционном режиме														СОИБ
12. Разработка, внедрение и обслуживание информационных систем														СОИБ
12.1. Требования к безопасности информационных систем														СОИБ
12.1.1. Анализ и детализация требований безопасности														СОИБ
12.2. Правильная обработка данных в приложениях														СОИБ
12.2.1. Подтверждение корректности ввода данных														СОИБ
12.2.2. Контроль обработки данных в системе														СОИБ
12.2.3. Целостность сообщений														СОИБ
12.2.4. Подтверждение достоверности выходных данных														СОИБ
12.3. Криптографические средства защиты														СОИБ
12.3.1. Политика использования криптографических средств защиты														СОИБ
12.3.2. Управление ключами														СОИБ
12.4. Безопасность системных файлов														СОИБ
12.4.1. Контроль программного обеспечения, находящегося в промышленной эксплуатации														СОИБ
12.4.2. Защита данных тестирования системы														СОИБ
12.4.3. Контроль доступа к исходным кодам														СОИБ
12.5. Безопасность в процессах разработки и поддержки														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
12.5.1. Процедуры контроля изменений														СОИБ
12.5.2. Технический анализ прикладных систем после внесения изменений в операционные системы														СОИБ
12.5.3. Ограничения на внесение изменений в пакеты программ														СОИБ
12.5.4. Утечка информации														СОИБ
12.5.5. Разработка программного обеспечения с привлечением сторонних организаций														СОИБ
12.6. Управление техническими уязвимостями														СОИБ
12.6.1. Контроль технической уязвимости														СОИБ
13. Управление инцидентами информационной безопасности														СОИБ
13.1. Оповещения о нарушениях и недостатках информационной безопасности														СОИБ
13.1.1. Оповещение о случаях нарушения информационной безопасности														СОИБ
13.1.2. Оповещение о недостатках безопасности														СОИБ
13.2. Управление инцидентами информационной безопасности и его усовершенствование														СОИБ
13.2.1. Ответственность и процедуры														СОИБ
13.2.2. Извлечение уроков из инцидентов информационной безопасности														СОИБ
13.2.3. Сбор доказательств														СОИБ
14. Управление непрерывностью бизнеса														СОИБ
14.1. Вопросы информационной безопасности управления непрерывностью бизнеса														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
14.1.1. Включение информационной безопасности в процесс управления непрерывностью бизнеса														СОИБ
14.1.2. Непрерывность бизнеса и оценка риска														СОИБ
14.1.3. Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность														СОИБ
14.1.4. Структура планов обеспечения непрерывности бизнеса														СОИБ
14.1.5. Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса														СОИБ
15. Соответствие требованиям														СОИБ
15.1. Соответствие правовым требованиям														СОИБ
15.1.1. Определение применимого законодательства														СОИБ
15.1.2. Права на интеллектуальную собственность (IPR)														СОИБ
15.1.3. Защита учетных записей организации														СОИБ
15.1.4. Защита данных и конфиденциальность персональной информации														СОИБ
15.1.5. Предотвращение нецелевого использования средств обработки информации														СОИБ
15.1.6. Регулирование использования средств криптографической защиты														СОИБ
15.2. Пересмотр политики безопасности и техническое соответствие требованиям безопасности														СОИБ
15.2.1. Соответствие политикам и стандартам безопасности														СОИБ
15.2.2. Проверка технического соответствия требованиям безопасности														СОИБ

Раздел Политики информационной безопасности	Декабрь	Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь	Ответственный
0	12	1	2	3	4	5	6	7	8	9	10	11	12	13
15.3. Вопросы аудита информационных систем														СОИБ
15.3.1. Меры управления аудитом информационных систем														СОИБ
15.3.2. Защита инструментальных средств аудита информационных систем														СОИБ