**Лабораторная работа № 5**

Методология анализа защищенности информационной системы

**Цель работы:** выявление значимых составляющих информационной безопасности и характеристик информационной системы в конкретных ситуациях, провести анализ нарушений информационной безопасности, научиться работать с нормативными документами в области защиты информации, научиться составлять практические рекомендации по защите информации на основе ГОСТа, научиться выполнять оценку защищенности информационной системы.

**Задачи**

1. Проанализируйте данные нарушения:

1.1. Сотрудники сидят в интернете на развлекательных сайтах по 4 часа. Играют в игры на работе. Перекладывают свои обязанности на других. Сотрудники копируют конфиденциальные данные компании. Сотрудники одновременно работают на другой работе. Сотрудники работают на конкурента. Сотрудник хочет создать собственную конкурентную компанию. Сотрудники распространяют государственную тайну.

1.2. Используется потенциальное опасное ПО, содержащее уязвимости, позволяющие скрытую передачу данных, дающие возможность деструктивного влияния на ИТ инфраструктуру компании. Выясняется, что административные пароли передаются по открытым каналам. Сотрудники используют средства удаленного управления. Администраторы сделали бреши в межсетевом периметре компании для удобства. Оставлены закладки в самописном программном обеспечении.

1.3. Как предотвратить потерю информации?

1.4. Что следует предпринять для устранения данных нарушений?

2. Определение класса ИС организации (согласно варианту лабораторных работ № 2,3,4) в соответствии с Приказом и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации» [https://adilet.zan.kz/rus/docs/V1600013349#z4](https://adilet.zan.kz/rus/docs/V1600013349)

2.1. Определите принадлежность объекта информатизации к одной из категорий классификатора объектов информатизации

2.2. Определите схему классификации объектов информатизации в рамках определенной категории вашей организации

2.3. Выберите характеристики категории - совокупность отличительных параметров классификатора объектов информатизации, характеризующих объект информатизации, суммарное значение которых определяет класс объекта информатизации.

2.4. Определите к какому классу относится информационная система вашей организации.

2.5. Заполните таблицы Классификационная оценка ИС, Результаты расчета категорий ИС, Классификационные характеристики ИС.

3. Управление рисками.

3.1. Выполните идентификацию рисков в отношении перечня идентифицированных и классифицированных активов ИС предприятия.

3.2. Выполните выбор критериев принятия идентифицированных рисков.

3.3. Выполните идентификацию уязвимостей и последствий инцидентов ИБ.

3.4. Оцените тяжесть влияния (воздействия) последствий от реализации рисков ИБ, вероятность возникновения (реализации) риска ИБ, вычислите уровень риска.

3.5. Сформируйте каталог угроз (рисков) ИБ, включающего оценку (переоценку) идентифицированных рисков в соответствии с требованиями стандарта Республики Казахстан СТ РК ISO/IEC 27005 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».

3.6. Сформируйте Карту рисков.

3.7. Разработайте план обработки угроз (рисков) ИБ, содержащий мероприятия по их нейтрализации или снижению, рассчитайте остаточный риск, относительно которого принимается решение о завершении обработки риска.

**Порядок выполнения работы**

1. Изучить предлагаемый теоретический материал, **Постановление** Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»; **Приказ** и.о. Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации», стандарты СТ РК ISO/IEC 27005 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности», СТ РК ИСО/МЭК 31010 «Менеджмент риска. Методы оценки рисков».
2. Заполнить таблицы согласно заданиям, из п. 2 и 3.
3. Сформировать Карту рисков.
4. Разработать план обработки угроз (рисков).
5. Построить отчёт, включающий разработанные таблицы и карту.

**Контрольные вопросы:**

1. Что принято называть угрозой информационной безопасности?

2. Какие составляющие информационной безопасности должны быть соблюдены?

3. Что будет если одна из составляющих информационной безопасности будет нарушена?

4. Что понимается под термином информационный объект?

5. Что представляет собой угроза права собственности?

6. Какова классификация методов защиты информации, в том числе по характеру проводимых мероприятий?

7. Какова классификация угроз информационной безопасности?

8. Для чего нужны законодательные меры в области информационной безопасности?

9. Какими документами регулируется информационная безопасность в РК?

10. Какие основополагающие документы в области информационной безопасности вам известны?

**Методические указания**

При разработке архитектуры и создании инфраструктуры ИС неизбежно встает вопрос о её защищенности от угроз. Решение вопроса состоит в подробном анализе таких взаимно пересекающихся видов работ, как реализация ИС и её аттестация, аудит и обследование безопасности ИС.

Информационная безопасность в самом широком смысле – это совокупность средств защиты информации от случайного или преднамеренного воздействия. Независимо от того, что лежит в основе воздействия: естественные факторы или причины искусственного характера – владелец информации несет убытки.

**Принципы информационной безопасности**

Целостность информационных данных означает способность информации сохранять изначальный вид и структуру как в процессе хранения, как и после неоднократной передачи. Вносить изменения, удалять или дополнять информацию вправе только владелец или пользователь с легальным доступом к данным.

Конфиденциальность – характеристика, которая указывает на необходимость ограничить доступа к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, который включены в информационные системы и успешно прошли идентификацию.

Доступность информационных ресурсов означает, что информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям ресурсов своевременно и беспрепятственно.

Достоверность указывает на принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации.

Обеспечение и поддержка информационной безопасности включают комплекс разноплановых мер, которые предотвращают, отслеживают и устраняют несанкционированный доступ третьих лиц. Меры ИБ направлены также на защиту от повреждений, искажений, блокировки или копирования информации. Принципиально, чтобы все задачи решались одновременно, только тогда обеспечивается полноценная, надежная защита.

**Информационный объект** – это среда, в которой информация создается, обрабатывается, хранится и передается.

Под угрозой информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу.

Рассмотрим их классификацию по различным классификационным признакам.

По виду:

– физической и логической целостности (уничтожение или искажение информации);

– конфиденциальности (несанкционированное получение);

– доступности;

– права собственности.

По характеру:

– случайные (отказы, сбои, ошибки, стихийные явления);

– преднамеренные (злоумышленные действия людей);

По источникам:

– человек;

– технические устройства;

– программное обеспечение;

– внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

Угроза конфиденциальности – нарушение свойства информации быть известной только определенным субъектам.

Угроза целостности – несанкционированное изменение, искажение, уничтожение информации.

Угроза доступности (отказ в обслуживании) – нарушение работоспособности объекта, доступ к которому получил злоумышленник.

Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются, как правило, в теории надежности, программировании, инженерной психологии.

Преднамеренные угрозы связаны с действиями людей (работники спецслужб либо самого объекта, хакеры).

Для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться штатными каналами доступа, если по отношению к ним не предприняты никакие меры защиты, либо нештатными каналами доступа, к которым принято относить:

– побочное электромагнитное излучение информации с аппаратуры системы;

– побочные наводки информации по сети электропитания и заземления;

– побочные наводки информации на вспомогательных коммуникациях;

– подключение к внешним каналам связи.

В таблице 2 представлена подробная классификация угроз информационной безопасности в зависимости от их источника и происхождения.

Все методы защиты информации по характеру проводимых действий можно разделить на:

* законодательные (правовые);
* организационные;
* технические;
* комплексные.

Таблица 2

Классификация угроз информационной безопасности

| **Природные угрозы** | **Угрозы техногенного характера** | **Угрозы, созданные людьми** |
| --- | --- | --- |
| * магнитные бури; * радиоактивные излучения и осадки; * стихийные бедствия. | – сбои в работе компьютерной сети (КС), вызванные отключением или колебанием электропитания либо другими средствами функционирования КС;  –отказы и сбои КС вследствие её ненадёжности;  –электромагнитные излучения и наводки;  –утечки через каналы связи – электрические, акустические, оптические и др. | – непреднамеренные либо преднамеренные действия:  а) обслуживающего персонала;  б) пользователей;  в) архивной службы;  г) службы безопасности;  д) управленческого персонала;  – хакерские атаки; |

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение.

Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации.

К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты.

Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

**Приложение** **А. Шкала критериев влияния воздействия (потерь) от последствий реализации 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  значительные, но могут быть полностью исправлены |
| 2 | Низкое | Последствия от реализации риска не значительные |
| 1 | Крайне  Незначительное | Отсутствие каких-либо последствий в случае реализации риска |

**Приложение Б. Шкала вероятностей возникновения рисков (угроз)**

| **Балл** | **Вероятность** | **Качественная характеристика** | **Количественная характеристика** |
| --- | --- | --- | --- |
| 5 | Крайне высокая | Вероятность реализации угрозы (уязвимости) крайне высокая. Существует история многократной реализации данного риска. Угроза (уязвимость) реализовывалась в недавнем прошлом. | 1 раз в месяц |
| 4 | Высокая | Вероятность реализации угрозы (уязвимости) высокая. Существует история неоднократной реализации данной угрозы (уязвимости). | 1 раз в квартал |
| 3 | Средняя | Угроза (уязвимость) может реализоваться. Существует история данной угрозы (уязвимости). | 1 раз в полугодие |
| 2 | Низкая | Вероятность реализации угрозы (уязвимости) низкая. Угроза (уязвимость) никогда не реализовывались ранее. Однако угроза (уязвимость) требуют контроля, так как при определенных условиях их реализация возможна. | 1 раз в год |
| 1 | Крайне низкая | Вероятность реализации угрозы (уязвимости) крайне низкая. Угроза (уязвимость) никогда не реализовывался ранее. Однако угроза (уязвимость) требует контроля, так как при определенных условиях вероятность его реализации может увеличиться. | 1 раз в 3 и более лет |

**Приложение В. Каталог угроз рисков информационной безопасности**

| **№ риска** | **Наимено вание риска** | **Факторы (причины, источники) возникновения риска** | **Последствия от реализа ции риска** | **Первичная оценка с учетом имеющихся предупредительных мероприятий**  **(оценка вероятности реализации риска)** | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Предупредительные мероприятия** | **Лицо/ подразделе ние, ответст венное за предупредительное ме- роприятие** | **Вероят- ность возникновения риска** | **Степень опасности потерь** | **Уровень риска** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Приложение Г. Карта рисков**



| **Степень опасности потерь** |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Критическая |  |  |  |  |  |  |
| Существенная |  |  |  |  |  |  |
| Средняя |  |  |  |  |  |  |
| Низкая |  |  |  |  |  |  |
| Крайне незначительная |  |  |  |  |  |  |
|  | Крайне Низкая | Низкая | Средняя | Высокая | Крайне высокая | **Вероятность возникновения рисков** |



*Номер риска в состоянии, соответствующем текущему уровню риска*

**Приложение Д. План обработки рисков информационной безопасности**

| **№ пп** | **Наименование риска** | **Последствия от реализации риска** | **Метод обработки риска** | **Вероятность возникновения риска** | **Степень опасности потерь** | **Ожидаемый**  **уровень**  **остаточного**  **риска** | **Мероприятия по обработке риска, сроки,**  **ответственный** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Приложение Е. Шкала критериев принятия рисков (угроз) ИБ**

| **Шкала** | **Наименование** | **Качественное описание** |
| --- | --- | --- |
| 1 – 4 | Очень низкий | Риск не требует обработки. |
| 5 – 9 | Умеренный | Риск требует обработки, и методы обработки оцениваются повторно во время следующего цикла оценки рисков. |
| 10 – 25 | Высокий | Риск требует обработки, и методы обработки предварительно разрабатываются.  Методы обработки рисков отслеживаются руководителем ИБ. |

**Приложение Ж. Типичные угрозы (риски)**

| **Виды рисков** | **Возможные причины и последствия** |
| --- | --- |
| 1. **риски**, **связанные с неблагоприятными событиями природного, техногенного и социального характера** | |
| 1 пожар | неконтролируемый процесс горения, сопровождающийся уничтожением материальных ценностей и создающий опасность для жизни людей. Возможные причины: поджог, самовозгорание, природное явление |
| 2 природные катастрофы, чрезвычайные ситуации и стихийные бедствия | природные явления разрушительного характера (наводнения, землетрясения, извержения вулканов, ураганы, смерчи, тайфуны, цунами и т.д.) |
| техногенные катастрофы | разрушительный процесс, развивающийся в результате нарушения нормального взаимодействия технологических объектов между собой или с компонентами окружающей природной среды, приводящий к гибели людей, разрушению и повреждению объектов экономики и компонентов окружающей природной среды |
| 3 нарушение внутриклиматических условий | негативное изменение климатических условий в помещениях, где расположены технические средства и/или находится персонал: значительные изменения температуры и влажности, повышение содержания углекислого газа, пыли и т.п. Возможные последствия: сбои, отказы и аварии технических средств, снижение работоспособности и нанесение ущерба здоровью персонала, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| 4 нарушение электропитания | нарушение или снижение качества электропитания. Возможные причины: техногенная катастрофа, стихийное бедствие, природное явление, террористический акт, пожар и т.п. Возможные последствия: сбои и отказы технических средств |
| 5 нарушение функционирования систем жизнеобеспечения | сбои и аварии в системах водоснабжения, канализации, отопления |
| 6 угроза здоровью персонала | угроза здоровью персонала в результате радиационных, биологических, механических, термических, химических и иных воздействий со стороны окружающей среды, объектов инженерной инфраструктуры, технических средств, пищевые отравления, производственный травматизм. Возможные причины: техногенные или природные катастрофы, аварии объектов инженерной инфраструктуры, неисправность оборудования, несоблюдение правил техники безопасности и охраны труда, санитарных правил и т.д. Возможные последствия: нехватка персонала, денежные выплаты, судебные разбирательства |
| **2. риски, связанные с деятельностью лиц, совершающих преступления и правонарушения** | |
| 1 нарушения общественного порядка, вандализм, массовые беспорядки, политическая нестабильность | уничтожение или повреждение имущества Министерства |
| 2 социальный инжиниринг | умышленные действия сторонних лиц, преследующих мошеннические цели, реализуемые посредством обмана, введения в заблуждение работников, осуществляющих обслуживание и сопровождение ИС . Возможные последствия: ошибки работников, нарушение свойств, утрата информационных активов, нарушение непрерывности процессов, снижение качества информационных услуг (сервисов) ИС |
| **3. риски, связанные с деятельностью поставщиков/провайдеров/партнеров** | |
| 1 зависимость от партнеров/клиентов | зависимость от партнеров заставляет Министерство полагаться на их информационную безопасность (далее – ИБ) |
| 2 ошибки, допущенные при заключении контрактов с провайдерами внешних услуг | неточности и неопределенности в договоре с провайдером внешних услуг, которые могут создавать проблемы в работе ИС |
| 3 нарушения договорных обязательств сторонними (третьими) лицами | невыполнение со стороны третьих лиц, взятых на себя обязательств по качеству, составу, содержанию и/или порядку оказания услуг, поставки продукции и т.д., например, невыполнение требований разработчиками, поставщиками программно-технических средств и услуг или внешними пользователями |
| 4 ошибки в обеспечении ИБ ИС на стадиях жизненного цикла | ошибки в обеспечении ИБ при разработке, эксплуатации, сопровождении и выводе из эксплуатации ИС |
| 5 разработка и использование некачественной документации | некачественное выполнение документированного описания технологических процессов обработки, хранения, передачи данных, руководств для персонала, участвующего в этих технологических процессах, а также описания средств обеспечения ИБ и руководств по их использованию |
| 6 использование программных средств и информации без гарантии источника | использование в информационной системе организации непроверенных данных или нелицензионного программного обеспечения (далее – ПО) |
| **4. риски, связанные со сбоями, отказами, разрушениями/повреждениями программных и технических средств** | |
| 1 превышение допустимой нагрузки | неумышленное превышение допустимой нагрузки на вычислительные, сетевые ресурсы системы. Выполнение работниками объема операций большего, чем это допускается психофизиологическими нормами. Возможные причины: малая вычислительная и/или пропускная мощность, неправильная организация бизнес-процессов. Возможные последствия: сбои и отказы технических средств, нарушение доступности технических средств, ошибки персонала, нанесение вреда здоровью |
| 2 разрушение/ повреждение, аварии технических средств и каналов связи | физическое разрушение/повреждение технических средств (канала связи) или определенное сочетание отказов его элементов, приводящее к нарушениям функционирования, сопряженным с особо значительными техническими потерями, делающее невозможным функционирование технического средства (канала связи) в целом в течение значительного периода времени. Возможные причины: действие внешних (физический несанкционированный доступ, террористический акт, техногенная катастрофа, стихийное бедствие, природное явление, массовые беспорядки) и/или внутренних (значительные отказы элементов технических средств) факторов. Возможные последствия: нарушение свойств информационных активов, их утрата, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| 3 сбои и отказы программных средств | нарушение работоспособности программных средств. Возможные причины: недопустимое изменение параметров или свойств программных средств под влиянием внутренних процессов (ошибок) и/или внешних воздействий со стороны вредоносных программ, оператора и технических средств. Возможные последствия: нарушение свойств информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| 4 сбои и отказы технических средств и каналов связи | прерывание работоспособности технических средств или невозможность выполнения ими своих функций в заранее установленных границах. Возможные причины: недопустимое изменение характеристик технических средств под влиянием внутренних процессов, сложность технических средств, нехватка персонала, недостаточное техническое обслуживание. Возможные последствия: сбои, отказы программных средств, аварии систем, нарушение доступности информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| 5 нарушения функциональности криптографической системы | случайное или намеренное неправильное управление криптографическими ключами, криптографическими протоколами и алгоритмами, программно-аппаратными средствами систем криптографической защиты информации, приводящее к потере конфиденциальности, целостности и доступности информации, нарушению неотказуемости приема-передачи информации |
| **5. риски, связанные с деятельностью внутренних нарушителей ИБ** | |
| 1 недобросовестное исполнение обязанностей | сознательное неисполнение работниками определенных обязанностей или небрежное их исполнение |
| 2 халатность | неисполнение или ненадлежащее исполнение должностным лицом своих обязанностей вследствие недобросовестного или небрежного отношения к работе |
| 3 причинение имущественного ущерба | умышленное нанесение персоналом вреда информационным активам. В первую очередь вредительство может быть направлено на технические и программные средства, а также на информационные активы. Возможные последствия: ущерб, вызванный нарушением свойств активов, включая их разрушение и уничтожение |
| 4 ошибка персонала | любые не соответствующие установленному регламенту или сложившимся практикам действия персонала, совершаемые без злого умысла. Возможные причины: недостаточно четко определенные обязанности, халатность, недостаточное обучение или квалификация персонала. Возникновению ошибок способствуют отсутствие дисциплинарного процесса и документирования процессов, предоставление избыточных полномочий, умышленное использование методов социального инжиниринга по отношению к персоналу. Возможные последствия: нарушение конфиденциальности и целостности информации, утрата информационных активов, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов), сбои и отказы технических и программных средств |
| 5 хищение | совершенное с корыстной целью противоправное безвозмездное изъятие и/или обращение имущества Министерства |
| 6 выполнение вредоносных программ | внедрение в ИС и выполнение вредоносных программ. Возможные причины: беспечность, халатность, низкая квалификация персонала (пользователей), наличие уязвимостей используемых программных средств. Возможные последствия: несанкционированный доступ к информационным активам, нарушение их свойств, сбои, отказы и уничтожение программных средств, нарушение непрерывности выполнения процессов, снижение качества информационных услуг (сервисов) |
| 7 использование информационных активов не по назначению | умышленное использование информационных активов организации в целях, отличных от целей организации. Возможные причины: отсутствие контроля персонала. Возможные последствия: нехватка вычислительных, сетевых или людских ресурсов, прямой ущерб Министерству |
| 8 нарушения персоналом организационных мер по обеспечению ИБ | несоблюдение персоналом требований технической документации по ИБ |
| ошибки кадровой работы | ошибки кадровой работы заключаются в приеме на работу неквалифицированных сотрудников, увольнении/перемещении сотрудников без проведения сопутствующих процедур по обеспечению ИБ, не проведении или нерегулярном проведении тренингов и проверок персонала |
| **6. риски, связанные с деятельностью внешних нарушителей ИБ** | |
| 1 действия неавторизованного субъекта | умышленные действия со стороны субъекта из внешней по отношению к области обеспечения ИБ среды. Возможные последствия: разрушение и уничтожение технических и программных средств, внедрение и выполнение вредоносных программ, нарушение свойств, утрата информационных активов и сервисов |
| 2 неконтролируемое уничтожение информационного актива | неумышленное уничтожение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: прямой ущерб Министерству |
| 3 неконтролируемая модификация информационного актива | неумышленное изменение информационных активов. Возможные причины: сбои оборудования, природные факторы и техногенные катастрофы. Возможные последствия: нарушение непрерывности функционирования ИС |
| 4 несанкционированный логический доступ | несанкционированный логический доступ неавторизованных субъектов к компонентам ИС **и** информационным активам. Возможные причины: компрометация пароля, предоставление пользователям/администраторам избыточных прав доступа, недостатки (отсутствие) механизмов аутентификации пользователей и администраторов, ошибки администрирования, оставление без присмотра программно-технических средств. Одним из путей получения несанкционированного доступа к системе является умышленное внедрение вредоносных программ с целью хищения пароля для входа в систему или получения прав доступа. Возможные последствия: нарушение свойств информационных активов, сбои, отказы и аварии программных и технических средств, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов) |
| 5 несанкционированный физический доступ | физический несанкционированный доступ неавторизованных лиц в контролируемую зону расположения технических средств и/или информационных активов. Возможные причины: может осуществляться путем обхода средств контроля физического доступа или использования утраченных/похищенных средств обеспечения доступа. Возможные последствия: разрушение и уничтожение технических и программных средств, нарушение конфиденциальности, целостности, доступности информационных активов, нарушение непрерывности процессов и/или снижение качества информационных услуг (сервисов) |
| **7. риски, связанные с несоответствием требованиям надзорных и регулирующих органов, действующему законодательству** | |
| 1 несоответствие технической документации по ИБ действующему законодательству | несоответствие может привести к административным и уголовным санкциям со стороны судебных, надзорных и регулирующих органов в отношении должностных лиц подразделения, вызвать остановку отдельных видов деятельности |
| изменчивость и несогласованность требований надзорных и регулирующих органов, вышестоящих инстанций | непостоянство, различия и коллизии в содержании требований и/или порядке их выполнения способны дезорганизовать деятельность подразделения или его отдельных служб, снизить ее эффективность и качество, а при определенных обстоятельствах — затруднить ее осуществление. Способствует «размыванию» или пересечению зон ответственности исполнителей и служб, манипуляции со стороны ответственных лиц и служб своими правами и обязанностями в ущерб общей деятельности |