Алтайский край

Администрация города Алейска

**П О С Т А Н О В Л Е Н И Е**

22.02.2023 № 119

г. Алейск

|  |  |
| --- | --- |
| О внесении дополнений в положение «Об обеспечении безопасности общедоступной информации при ее обработке в информационных системах администрации города Алейска Алтайского края», утвержденное постановлением администрации города Алейска от 09.12.2013 № 1760  |  |

# В целях соблюдения требований Федеральных законов "О персональных данных" от 27.07.2006 N 152-ФЗ и "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ,

ПОСТАНОВЛЯЮ:

1. Внести дополнения в положение «Об обеспечении безопасности общедоступной информации при ее обработке в информационных системах администрации города Алейска Алтайского края», утвержденное постановлением администрации города Алейска Алтайского края от 09.12.2013 №1760 следующего содержания:

дополнить положение приложениями:

* 1. № 7 «Модель угроз информационной безопасности»;
	2. № 8 «Регламент резервного копирования данных»;
	3. № 9 «Политика безопасности рабочих станций и серверов администрации города Алейска Алтайского края»;
	4. № 10 «Политика управления парольной защитой администрации города Алейска Алтайского края».

2. Контроль исполнения настоящего постановления возложить на начальника отдела программного обеспечения администрации города Русакова В.А.

3. Отделу по печати и информации администрации города (Ориненко Ю.В.) разместить настоящее постановление на официальном Интернет-сайте администрации города Алейска Алтайского края и опубликовать в «Сборнике муниципальных правовых актов города Алейска Алтайского края».

Глава города И.В. Маскаев

Приложение № 7

к Положению об обеспечении безопасности общедоступной информации в информационных системах администрации города Алейска Алтайского края

**Модель угроз информационной безопасности**

## 1. Методика определения актуальности угроз

Определение перечня актуальных угроз безопасности ИТ-инфраструктуры администрации города Алейска Алтайского края осуществлялось на основе Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой 14 февраля 2008 г. заместителем директора ФСТЭК России. Определение перечня актуальных угроз безопасности ИТ-инфраструктуры администрации города Алейска Алтайского края осуществлялось в следующей последовательности:

* определялся уровень исходной защищённости ИТ-инфраструктуры соответствующий ему коэффициент Y1;
* с учётом используемых средств защиты информации и реализованных организационных мер по защите экспертным методом, в том числе путём дополнительного опроса персонала ИТ-инфраструктуры, определялась вероятность возникновения угроз и соответствующие коэффициенты Y2, с использованием которых рассчитывались коэффициенты реализуемости угроз Y;
* проводилась экспертная оценка опасности реализации угроз безопасности ИТ-инфраструктуры;
* осуществлялся расчёт актуальности угроз безопасности ИТ-инфраструктуры.

При определении актуальных угроз в качестве исходного перечня угроз использовался перечень угроз в соответствии с банком данных угроз безопасности информации ФСТЭК России, представленном на веб-сайте *http://www.bdu.fstec.ru/*.

## 2. Определение типов угроз

В соответствии с частью 10, (п. «е») Требований к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, для ИТ-инфраструктуры администрации города Алейска Алтайского края актуальны угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в информационной системе.

При обработке информации в локальных ИС, имеющих подключение к сетям связи общего пользования, возможна реализация следующих угроз безопасности персональным данным:

1. Угрозы деструктивных воздействий (искажение, уничтожение, подмена, блокирование) на информацию с использованием мошеннических манипуляционных схем данными и/или документами и «тонких» мест бизнес процессов:
* угрозы фальсификации данных в ИТ-инфраструктуре администрации города Алейска Алтайского края;
* угрозы ввода в информационные ресурсы ИТ-инфраструктуры администрации города Алейска Алтайского края заведомо ложных данных с использованием мошеннических схем.
1. Угрозы хищения информации по техническим каналам:
* угрозы утечки акустической (речевой) информации;
* угрозы утечки видовой информации.
1. Угрозы хищения информации по каналам ПЭМИН:
* утечка информации по сетям электропитания;
* утечка за счёт наводок на линии связи, технические средства, расположенные в помещении и системы коммуникаций;
* утечки побочные излучений технических средств;
* утечки за счёт, электромагнитного воздействия на технические средства.
1. Угрозы деструктивных воздействий и хищение информации путём несанкционированного доступа к ПДн и операционной среды АРМ администратора и серверов путём получения физического доступа к ИТ-инфраструктуре администрации города Алейска Алтайского края или средствам вывода информации:
* угрозы, реализуемые в ходе загрузки операционной системы и направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS), перехват управления загрузкой;
* угрозы, реализуемые после загрузки операционной системы и направленные на выполнение несанкционированного доступа с применением стандартных функций операционной системы или какой-либо прикладной программы, с применением специально созданных для выполнения НСД программ;
* угрозы внедрения вредоносных программ при непосредственном физическом доступе.
1. Угрозы хищения аппаратно–технических средств ИТ-инфраструктуры администрации города Алейска Алтайского края;
2. Угрозы хищения отчуждаемых носителей информации;
3. Угрозы хищения информации путём:
* использования средств копирования на съёмные носители;
* несанкционированной передачи по каналам связи;
* НСД к ключам и атрибутам доступа.
1. Угрозы хищения информации в ходе ремонта, модификации и утилизации программно-аппаратных средств;
2. Угрозы деструктивных воздействий и хищения информации путём:
* непреднамеренного отключения средств защиты;
* «Анализа сетевого трафика»:
	+ с перехватом информации за пределами контролируемой зоны;
	+ с перехватом передаваемой по внутренней сети информации.
* сканирования, направленных на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций, топологии сети, открытых портов и служб, открытых соединений и др.;
* навязывания ложного маршрута путём несанкционированного изменения маршрутно-адресных данных;
* внедрения ложного объекта как внутри ИС, так и во внешних сетях;
* подмены доверенного объекта;
* выявления паролей по сети;
* организации режима типа «Отказа в обслуживании»;
* удаленного запуска приложений;
* внедрения по сети вредоносных программ;
* нанесения ущерба информации системы путём целенаправленного воздействия на данные с использованием РЭП.

## 3. Определение уровня исходной защищённости ИТ-инфраструктуры администрации города Алейска Алтайского края

Под уровнем исходной защищённости ИТ-инфраструктуры администрации города Алейска Алтайского края понимается обобщённый показатель, зависящий от технических и эксплуатационных характеристик ИТ-инфраструктуры администрации города Алейска Алтайского края, приведённых в Таблица 1.

Таблица 1.

Показатели исходной защищённости ИТ-инфраструктуры администрации города Алейска Алтайского края

| № п/п | Технические и эксплуатационные характеристики | Уровень защищённости |
| --- | --- | --- |
| Высокий | Средний | Низкий |
| 1 | По территориальному размещению: |
| 1.1 | - распределённая ИС, которая охватывает несколько областей, краёв, округов или государство в целом |  |  | **+** |
| 1.2 | - городская ИС, охватывающая не более одного населённого пункта (города, посёлка) |  |  | **-** |
| 1.3 | - корпоративная распределённая ИС, охватывающая многие подразделения одной организации |  | **-** |  |
| 1.4 | - локальная (кампусная) ИС, развёрнутая в пределах нескольких близко расположенных зданий |  | **-** |  |
| 1.5 | - локальная ИС, развёрнутая в пределах одного здания | **-** |  |  |
| 2 | По наличию соединения с сетями общего пользования: |
| 2.1 | - ИС, имеющая многоточечный выход в сеть общего пользования |  |  | **-** |
| 2.2 | - ИС, имеющая одноточечный выход в сеть общего пользования |  | **+** |  |
| 2.3 | - ИС, физически отделённая от сети общего пользования | **-** |  |  |
| 3 | По встроенным (легальным) операциям с защищаемой информацией: |
| 3.1 | - чтение, поиск | **+** |  |  |
| 3.2 | - запись, удаление, сортировка |  | **+** |  |
| 3.3 | - модификация, передача |  |  | **+** |
| 4 | По разграничению доступа к защищаемой информации: |
| 4.1 | - ИС, к которой имеет доступ определённый перечень сотрудников организации, являющейся владельцем ИС, либо субъект ПДн |  | **+** |  |
| 4.2 | - ИС, к которой имеют доступ все сотрудники организации, являющейся владельцем ИС |  |  | **-** |
| 4.3 | - ИС с открытым доступом |  |  | **-** |
| 5 | По наличию соединений с другими базами защищаемой информации иных ИС: |
| 5.1 | - интегрированная ИС (организация использует несколько баз защищаемой информации, при этом организация не является владельцем всех используемых баз защищаемой информации) |  |  | **-** |
| 5.2 | - ИС, в которой используется одна база данных защищаемой информации, принадлежащая организации - владельцу данной ИС | **+** |  |  |
| 6 | По уровню обобщения (обезличивания) ПДн: |
| 6.1 | - ИС, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.) | **-** |  |  |
| 6.2 | - ИС, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации |  | **-** |  |
| 6.3 | - ИС, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн) |  |  | **+** |
| 7 | По объёму защищаемой информации, который предоставляются сторонним пользователям ИС без предварительной обработки: |
| 7.1 | - ИС, предоставляющая всю БД с защищаемой информацией |  |  | **-** |
| 7.2 | - ИС, предоставляющая часть защищаемой информации |  | **+** |  |
| 7.3 | - ИС, не предоставляющие никакой информации | **-** |  |  |
|  | Сумма характеристик по столбцам: | 2 | 4 | 3 |

В таблице знаком «+» обозначены актуальные характеристики ИТ-инфраструктуры администрации города Алейска Алтайского края.

ИТ-инфраструктура администрации города Алейска Алтайского края имеет низкий уровень исходной защищённости, т.к. менее 70% (6/9\*100%) характеристик, указанных в таблице, соответствуют уровню не ниже «среднего». Следовательно, коэффициент Y1 равен 10.

## 4. Определение актуальных угроз

### *4.1 Определение возможности реализации угроз*

Под частотой (вероятностью) реализации угрозы понимается показатель, определяемый экспертным путём, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности в складывающихся условиях обстановки. Введено четыре вербальных градации этого показателя:

* маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);
* низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют её реализацию (например, использованы соответствующие средства защиты информации);
* средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны;
* высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты.

При определении вероятности реализации угроз учитывались, в том числе, следующие факторы, оказывающие влияние на вероятность реализации:

* потенциал, которым должны обладать внешние и/или внутренние нарушители для реализации угрозы;
* наличие реализованных в ИТ-инфраструктуре администрации города Алейска Алтайского края мер физической защиты и контроля доступа к объектам защиты, существенно снижающих вероятность реализации отдельных угроз;
* наличие реализованных в ИТ-инфраструктуре администрации города Алейска Алтайского края мер обеспечения защиты информации от НСД, снижающих вероятность реализации отдельных угроз;
* отсутствие в составе ИТ-инфраструктуре администрации города Алейска Алтайского края средств защиты информации, прошедших процедуру оценки соответствия в установленном законодательством порядке.

При определении вероятности реализации угроз не рассматривались угрозы из исходного перечня угроз, неприменимые к ИТ-инфраструктуре администрации города Алейска Алтайского края. Угрозы могут быть неприменимы к ИТ-инфраструктуре администрации города Алейска Алтайского края, например, в следующих случаях:

* объект воздействия угрозы не входит в состав ИТ-инфраструктуры (например, для тех угроз, объектом воздействия которых является сетевой трафик, передаваемый по каналам, расположенным за пределами контролируемой зоны);
* источником угрозы является внутренний нарушитель с высоким потенциалом (рассматриваемый внутренний нарушитель безопасности не обладает высоким потенциалом);
* в составе ИТ-инфраструктуры не применяются технологии, связанные с реализацией угрозы.

При составлении перечня актуальных угроз безопасности каждой градации вероятности возникновения угрозы был поставлен в соответствие числовой коэффициент Y2, а именно:

* 0 – для маловероятной угрозы;
* 2 – для низкой вероятности угрозы;
* 5 – для средней вероятности угрозы;
* 10 – для высокой вероятности угрозы.

С учётом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением: Y = (Y1 + Y2) / 20.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

* если 0≤Y≤0,3, то возможность реализации угрозы признается низкой;
* если 0,3<Y≤0,6, то возможность реализации угрозы признается средней;
* если 0,6<Y≤0,8, то возможность реализации угрозы признается высокой;
* если Y>0,8, то возможность реализации угрозы признается очень высокой.

### *4.2 Оценка опасности реализации угроз*

Оценка опасности реализации угроз проводится экспертным методом. При оценке опасности определяется вербальный показатель опасности, который имеет три значения:

* низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных, ИТ-инфраструктуры администрации города Алейска Алтайского края;
* средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных, ИТ-инфраструктуры администрации города Алейска Алтайского края;
* высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных, ИТ-инфраструктуры администрации города Алейска Алтайского края.

При определении опасности реализации угроз учитывалось в том числе:

* характеристики ИТ-инфраструктуры
* – состав и уровень значимости обрабатываемой информации, масштаб и класс защищённости;
* последствия реализации угрозы, включая перечень свойств безопасности информации, к нарушению которых может привести реализация угрозы.

### *4.3 Правила отнесения угроз безопасности к актуальным*

После расчёта возможности реализации и оценки опасности реализации угроз осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным, в соответствии с правилами, приведёнными в Таблица .

Таблица 2. Правила отнесения угроз безопасности к актуальным

| Возможность реализации угрозы | Показатель опасности угрозы |
| --- | --- |
| Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |
| Очень высокая | актуальная | актуальная | актуальная |

## 5. Результаты определения актуальных угроз

Результаты определения актуальных угроз приведены в Перечне средств и мер защиты информации, обеспечивающих нейтрализацию актуальных угроз безопасности информации и формируются в ходе технического проектирования системы защиты.

**Модель нарушителя объекта информатизации администрации города Алейска Алтайского края**

Настоящая модель содержит описание потенциального нарушителя безопасности и описывает предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в ИТ-инфраструктуре администрации города Алейска Алтайского края, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

При разработке Модели нарушителя было учтено, что применяемые организационно-технические меры по физической защите обеспечивают ограничение и контроль доступа в помещения и к расположенным в них программно-аппаратным средствам ИТ-инфраструктуры администрации города Алейска Алтайского края.

Исходя их состава обрабатываемых данных и архитектуры ИТ-инфраструктуры администрации города Алейска Алтайского края можно выделить основной интерес потенциального нарушителя:

* к хранимым в базах данных сведениям ограниченного доступа;
* к корректировке данных о гражданах;
* к доступности интернет-сервисов ИТ-инфраструктуры администрации города Алейска Алтайского края.

## 1. Общее описание нарушителя

Под нарушителем (субъектом атаки) понимается лицо (или инициируемый им процесс), проводящее (проводящий) атаку на объекты защиты. Таким лицом может быть работник администрации города Алейска Алтайского края, или постороннее лицо. Работник администрации города Алейска Алтайского края может иметь доступ на участок служебных помещений, где расположены объекты защиты, к которым этот работник не имеет прав допуска. Постороннее лицо может иметь временный доступ в служебные помещения (например, для временных работ), где расположены объекты защиты.

Нарушителей можно категорировать в зависимости от прав допуска в контролируемую зону:

* лица, не имеющие права доступа в контролируемую зону, где расположены объекты защиты;
* лица, имеющие право постоянного или разового доступа в контролируемую зону, где расположены объекты защиты.

Потенциальных нарушителей в зависимости от места совершения атаки можно разделить на:

* внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны;
* внутренних нарушителей, осуществляющих атаки в пределах контролируемой зоны.

Внутренними нарушителями могут быть:

* лица, не являющиеся пользователями информационной системы (включая обслуживающий персонал подрядных организаций, привлекаемый к проведению работ; лица, имеющие разовый или временный доступ в контролируемую зону);
* пользователи информационной системы с типовыми полномочиями по реализации технологических процессов;
* администраторы информационной системы, на которых возлагаются задачи по эксплуатации и сопровождению программно-аппаратных средств, СЗИ в том числе СКЗИ, и баз данных ИТ-инфраструктуры администрации города Алейска Алтайского края.

Внешними нарушителями могут быть:

* специальные службы иностранных государств;
* преступные группы (криминальные структуры);
* внешние субъекты (физические лица, не имеющие доступа к программно-аппаратным средствам ИТ-инфраструктуры).

Допускается возможность сговора внутреннего нарушителя с внешним нарушителем.

Ниже приводится описание классов внутренних и внешних нарушителей, а также описание степени их информированности, используемых средств атак по возможным каналам их проведения.

## 2. Описание классов нарушителей

Предположения о целях (мотивации) нарушителей делаются с учётом целей и задач ИТ-инфраструктуры администрации города Алейска Алтайского края, вида обрабатываемой информации, а также с учётом результатов оценки степени возможных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации. Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации приведены в Таблице 1.

Таблица 1. Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Виды нарушителя | Типы нарушителя | Возможные цели (мотивация) реализации угроз безопасности информации |
| 1 | Специальные службы иностранных государств (блоков государств) | Внешний | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности налоговых органов. |
| 2 | Преступные группы (криминальные структуры) | Внешний | Причинение имущественного ущерба путём мошенничества или иным преступным путём. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды |
| 3 | Внешние субъекты (физические лица, не имеющие доступа к программно-аппаратным средствам ИТ-инфраструктуры) | Внешний | Идеологические или политические мотивы. Причинение имущественного ущерба путём мошенничества или иным преступным путём. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Любопытство или желание самореализации (подтверждение статуса). |
| 4 | Лица, не являющиеся пользователями информационных систем (включая обслуживающий персонал подрядных организаций, привлекаемый к проведению работ; лица, имеющие разовый или временный доступ в контролируемую зону); | Внутренний | Причинение имущественного ущерба путём обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия |
| 5 | Пользователи информационной системы | Внутренний | Месть за ранее совершенные действия. Причинение имущественного ущерба путём мошенничества или иным преступным путём. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Любопытство или желание самореализации (подтверждение статуса). |
| 6 | Администраторы информационной системы и администраторы безопасности | Внутренний | Месть за ранее совершенные действия. Причинение имущественного ущерба путём мошенничества или иным преступным путём. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды |

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

* нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;
* нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;
* нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

Потенциал нарушителей и их возможности приведены в Таблица 2.

Потенциал нарушителей и их возможности.

Таблица 2.

Потенциал нарушителей и их возможности

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Потенциал нарушителя | Виды нарушителя | Возможности по реализации угроз безопасности информации |
| 1. | Нарушители с базовым (низким) потенциалом | Внешние субъекты (физические лица, не имеющие доступа к программно-аппаратным средствам ИТ-инфраструктуры)Лица, не являющиеся пользователями информационных систем (включая обслуживающий персонал подрядных организаций, привлекаемый к проведению работ; лица, имеющие разовый или временный доступ в контролируемую зону);Пользователи информационной системы | Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках.Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему |
| 2. | Нарушители с базовым повышенным (средним) потенциалом | Администраторы информационной системы и администраторы безопасностиПреступные группы (криминальные структуры) | Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомлённость о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путём проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы |
| 3. | Нарушители с высоким потенциалом | Специальные службы иностранных государств (блоков государств) | Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами.Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищённых организационными мерами).Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок.Имеют хорошую осведомлённость о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе.Имеют возможность получить информацию об уязвимостях путём проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения.Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на неё.Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений |

Возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования информационной системы.

Угрозы безопасности информации могут быть реализованы нарушителями за счёт:

* несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));
* несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);
* несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);
* несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);
* несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;
* воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

Возможности нарушителей класса пользователи информационной системы, администраторы информационной системы и администраторы безопасности ограничены следующими организационно-техническими мерами:

* проводятся работы по подбору персонала;
* пользователи информационной системы, администраторы информационной системы и администраторы безопасности проинформированы о правилах работы в информационной системе и ответственности за несоблюдение правил обеспечения безопасности информации;
* осуществляется разграничение и контроль доступа пользователей и администраторов к защищаемым ресурсам.

Возможности нарушителей всех классов по использованию штатных средств ИТ-инфраструктуры администрации города Алейска Алтайского края существенно ограничены следующими организационно-техническими мерами:

* меры по ограничению и контролю физического доступа к техническим средствам ИТ-инфраструктуры;
* меры по ограничению и контроля доступа к ресурсам технических средств ИТ-инфраструктуры, реализованные механизмами применяемых средств защиты и штатных средств ИТ-инфраструктуры.

Таким образом, в рамках настоящей модели угроз и нарушителей актуальными считаются следующие классы нарушителей:

### *2.1 Класс нарушителей I – Специальные службы иностранных государств (блоков государств)*

При организации безопасности информации на объектах КСИИ 3-й и выше категорий, в качестве потенциальных нарушителей в обязательном порядке должны рассматриваться представители иностранных технических разведок, с точки зрения возможных деструктивных воздействий по техническим каналам на информацию, циркулирующую в КСИИ.

### *2.2 Класс нарушителей II – Преступные группы (криминальные структуры)*

К классу нарушителей II потенциально относятся лица, не имеющие права доступа в контролируемую зону и не являющиеся пользователями и/или администраторами ИТ-инфраструктуры. Квалификация данного класса нарушителей может быть разнообразной.

Указанные лица могут иметь высшее или среднее образование, обладать навыками работы с СВТ, с программным обеспечением, а также с СЗИ и СКЗИ, однако их возможности ограничены реализуемыми режимными и организационно-техническими мероприятиями:

* по допуску к ресурсам ИТ-инфраструктуры;
* по контролю выполнения требований, предъявляемых должностными инструкциями и иной организационно-распорядительной документацией.

### *2.3 Класс нарушителей III – Внешние субъекты*

К классу нарушителей III потенциально относятся внешние пользователи, которые не имеют доступа в контролируемую зону, но имеют санкционированный удалённый доступ к ресурсам ИТ-инфраструктуры в соответствии с организационно-техническими требованиями.

Указанные лица могут иметь высшее или среднее образование, обладать навыками работы с СВТ, с программным обеспечением, а также с СЗИ и СКЗИ, однако их возможности ограничены реализуемыми режимными и организационно-техническими мероприятиями:

* по допуску к ресурсам ИТ-инфраструктуры;
* по контролю выполнения требований, предъявляемых должностными инструкциями и иной организационно-распорядительной документацией.

### *2.4 Класс нарушителей IV – Лица, не являющиеся пользователями информационных систем*

К классу нарушителей IV потенциально относятся работники администрации города Алейска Алтайского края и работники сторонних организаций (в том числе технический персонал, выполняющий работы по уборке помещений, обслуживанию инженерно-технических средств и систем, пожарной, охранной сигнализации и т. д.), которые имеют доступ в помещения, где размещаются компоненты ИТ-инфраструктуры. Квалификация указанных лиц может быть разнообразной.

Возможности внутреннего нарушителя класса IV существенно ограничены следующими организационно-техническими мерами:

* предотвращение и пресечение несанкционированных действий – только зарегистрированные пользователи системы имеют права на доступ к ресурсам системы, попытка несанкционированного доступа будет немедленно обнаружена;
* контроль над порядком проведения работ в соответствии с требованиями организационно-распорядительной документации администрации города Алейска Алтайского края.

|  |  |
| --- | --- |
|  | Приложение № 8к Положению об обеспечении безопасности общедоступной информации в информационных системах администрации города Алейска Алтайского края |

**РЕГЛАМЕНТ**

резервного копирования данных

Настоящий «Регламент обслуживания технологических процессов» (далее Регламент) определяет порядок резервного копирования баз данных и других программных продуктов администрации города Алейска Алтайского края.

Регламент содержит инструкции и рекомендации по проведению резервного копирования баз данных.

Данный Регламент является обязательным для выполнения. В особых случаях допускаются отступления от требований Регламента.

*Администратор файлового сервера* – начальник отдела программного обеспечения, осуществляющий управление файловым сервером *Служебная записка* – запрос сотрудника на решение какой-либо технической проблемы.

*Ресурс файлового сервера (далее Ресурс)* – это каталог на файловом сервере, предназначенный для хранения файлов.

**1. Общие положения**

Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах администрации города Алейска Алтайского края разработан с целью:

* определения порядка резервирования данных для последующего восстановления работоспособности автоматизированных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
* определения порядка восстановления информации в случае возникновения такой необходимости;
* упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

* резервное копирование;
* контроль резервного копирования;
* хранение резервных копий;
* полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация следующих основных категорий:

* Персональная информация пользователей (личные каталоги на файловых серверах);
* Групповая информация пользователей (общие каталоги отделов);
* Информация, необходимая для  восстановления серверов и систем управления базами данных (далее – СУБД);
* Персональные профили пользователей сети;
* Информация автоматизированных систем, в т.ч. баз данных;
* Справочно-информационная информация систем общего использования («Гарант», «Консультант +» и т.п.);
* Рабочие копии установочных компонент программного обеспечения рабочих станций;
* Регистрационная информация системы информационной безопасности автоматизированных систем.

**2. Порядок резервного копирования**

Резервное копирование автоматизированных систем производится на основании следующих данных:

* состав и объем копируемых данных, периодичность проведения резервного копирования;
* максимальный срок хранения резервных копий - 5 лет;
* ежемесячный архив создается на 1-е число текущего месяца

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в  установленные сроки и с заданной периодичностью. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, сообщается сотруднику, ответственному за информационную безопасность служебной запиской в течение рабочего дня после обнаружения указанного события..

**3. Контроль результатов резервного копирования**

Контроль результатов всех процедур резервного копирования осуществляется ответственным должностным лицом, в срок до 12 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает сотруднику, ответственному за информационную безопасность до 15 часов текущего рабочего дня. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

**4. Ротация носителей резервной копии.**

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования.

В случае необходимости замены испорченных носителей информации новыми,  работник заблаговременно за 10 рабочих дней согласовывает с сотрудником, ответственным за информационную безопасность спецификации новых носителей информации. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также перемещение, осуществляются администратором резервного копирования. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться.

**5. Восстановление информации из резервных копий**

В случае необходимости восстановление данных из резервных копий производится на основании Служебной записки сотрудника согласованной с Ответственным за информационные ресурсы. Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Перечень резервируемой информации

|  |  |  |
| --- | --- | --- |
| № п/п | Адрес хранения информации | Примечание |
| 1 | \\SERVER-GOROD\Общая\ | Копии файлов пользователей. |
| 2 | \\ADM-44-2\1с | Копии БД 1С ночные |
| 3 | \\WIN-4O34QTHRCRP \SAUMI | Копии SAUMI ночные |

Перечень лиц ответственных за резервное копирование

|  |  |  |
| --- | --- | --- |
| № п/п | Выполняемая роль | ФИО ответственного сотрудника |
| 1 | Первоначальная настройка системы резервного копирования Запуск в промышленную эксплуатацию системы резервного копирования. | Русаков В.А., начальник отдела программного обеспечения  |
| 2 | Внесение существенных изменений в настройку системы резервного копирования. | Русаков В.А., начальник отдела программного обеспечения  |
| 3 | Анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования. Ежедневный контроль корректности создания резервной копии и повторного резервного копирования в случае ее отсутствия. | Русаков В.А., начальник отдела программного обеспечения  |
| 4 | Восстановление баз с резервных копий БД. | Русаков В.А., начальник отдела программного обеспечения  |
| 5 | Контроль проведения операций резервного копирования и восстановления БД. | Русаков В.А., начальник отдела программного обеспечения  |

Приложение № 9

к Положению об обеспечении безопасности общедоступной информации в информационных системах администрации города Алейска Алтайского края

### **Политика безопасности рабочих станций и серверов**

### **администрации города Алейска Алтайского края**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика безопасности рабочих станций и серверов (далее – Политика), включает в себя взаимоувязанный комплекс организационных мер, программных и технических средств защиты, применяемых при эксплуатации серверов и подготовке рабочих станций для работы в локальной вычислительной сети (ЛВС).

1.2. Требования настоящей Политики являются неотъемлемой частью комплекса мер безопасности и средств защиты информации (СЗИ).

1.3. Требования настоящей Политики распространяются на всех должностных лиц и работников комитетов, использующих в работе СВТ (включая работу в ЛВС администрации города Алейска Алтайского края(далее администрация)) и должны применяться для всех средств вычислительной техники, эксплуатируемой в администрации. Исключением из этого общего правила являются работники, выполняющие функции администраторов (информационных ресурсов и занимающихся подготовкой рабочих станций к работе).

1.4. Организационное и техническое обеспечение процесса подготовки рабочих станций к эксплуатации возлагается на специально выделенного работника отдела программного обеспечения (включая администраторов информационных ресурсов). Методическое обеспечение и функции контроля необходимой достаточности технических и программных средств, используемых в процессе подготовки рабочих станций к эксплуатации, а также контроль за действиями работников, использующих рабочие станции, для выполнения служебных обязанностей, возлагается на сотрудника отдела программного обеспечения, в функции которого входит обеспечение информационной безопасности.

1.5. Ознакомление всех работников администрации, использующих средства ВТ, с требованиями Политики проводит специалист отдела программного обеспечения. Факт ознакомления работника фиксируется на контрольном экземпляре «Политики безопасности рабочих станций» с указанием даты и личной подписи работника. При ознакомлении с Политикой внимание работников акцентируется на предупреждении их о персональной ответственности за несоблюдение требований, сформулированных в данной Политике. При необходимости сотрудник ответственный за информационную безопасность проводит персональные повторные инструктажи.

1.6. В целях закрепления знаний по вопросам практического исполнения требований Политики, разъяснения возникающих вопросов, проводятся, организуемые отделом программного обеспечения, семинары (не реже 1 раз в год) и персональные инструктажи (при необходимости) пользователей средств ВТ администрации.

1.7. В случае невозможности исполнения требований настоящей Политики в полном объеме, например:

- в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний;

- злоумышленных действий;

- в случае программно-технических особенностей эксплуатируемых СВТ;

- практическая «глубина» исполнения настоящей Политики определяется отделом программного обеспечения, в функции которого входит обеспечение информационной безопасности.

1.8. Несоблюдение требований данной Политики может быть классифицировано как целенаправленное (умышленное или неумышленное) действие/бездействие, направленное на преодоление специальных мер, обеспечивающих информационную безопасность объекта администрации.

2. ЦЕЛЬ ПОЛИТИКИ БЕЗОПАСНОСТИ РАБОЧИХ СТАНЦИЙ

Целью настоящего документа является:

- организация в администрации единой системы подготовки рабочих станций для эксплуатации в ЛВС cо строго определенным и согласованным перечнем программных средств;

- систематизация и упорядочение требований, предъявляемых к составу базового программного обеспечения необходимого и достаточного для выполнения служебных функций работниками администрации.

- запрет и максимальное ограничение действий, направленных на нарушение нормального функционирования рабочих станций и ЛВС в целом.

3. ЛОКАЛЬНАЯ БЕЗОПАСНОСТЬ

(безопасность рабочих станций)

3.1. Антивирусный и анти-хакерный контроль (далее - антивирусный контроль).

Обязательными требованиями являются:

- выполнение пользователями антивирусного контроля локальных дисков своих рабочих станциях и общедоступных (конкретному отделу) сетевых дисков;

- автоматический запуск антивирусного монитора и его работа в фоновом режиме;

- актуализация антивирусных баз должна выполнятся администратором антивирусной защиты с использованием сетевого центра управления не реже одного раза в сутки.

3.2. Защита от несанкционированного доступа (НСД)

3.2.1. При подготовке рабочих станций к эксплуатации:

- подготовка рабочих станций выполняется в соответствии с разработанным в администрации стандартом, представляющим собой, согласованный, со специалистом, в функции которого входит обеспечение информационной безопасности, перечень программных средств; установка дополнительного программного обеспечения для допуска пользователей к требуемым информационным ресурсам осуществляется по специальным служебным запискам;

- присвоение фиксированных IP-адресов рабочим станциям, серверам, библиотекам и другому сетевому оборудованию производится исключительно системным администратором;

- блокировать доступ в сетап (BIOS) всех рабочих станций всем пользователям кроме администратора сети, занимающихся подготовкой рабочих станций к эксплуатации в администрации;

- блокировать доступ пользователей к внешним устройствам и портам рабочих станций;

- эксплуатация операционной системы рабочих станций должна выполняться пользователями с правами Пользователя (User’а) и отключенным режимом доступа к функции работы с командной строкой;

- отключить неиспользуемые службы Windows, а другие (используемые) службы настроить на использование нестандартных портов;

- для пользователей не являющихся членами административных групп, удалять существующие (по молчанию) права на чтение и исполнение определенных функционально опасных системных файлов;

- обеспечить защиту системного реестра путем:

|  |  |
| --- | --- |
| а)  |  блокирования возможности корректировки функционально важных областей системного реестра; |
| б) |  отключения автозапуска приложений для потенциально опасных типов файлов. |

3.2.2. При эксплуатации рабочих станций:

- аутентификация всех пользователей должна производиться при помощи ввода паролей, удовлетворяющих требованиям политики управления парольной защиты; исключением, из этого общего правила, являются работники, выполняющие функции администраторов (информационных ресурсов и занимающихся подготовкой рабочих станций к работе);

- строгое соблюдение требований «Политики управления парольной защитой», в части периодичности смены паролей и их качества;

- обеспечение своевременной установки всем пользователям новых изменений для системы безопасности WINDOWS и текущих обновлений для используемого программного обеспечения;

- настройку антивирусного контроля всей обрабатываемой на рабочей станции информации, посредством использование резидентного монитора;

- использование, лично каждым работником администрации, отработанных методик, обеспечивающих надежное резервное копирование служебной информации;

- санкционированный доступ к необходимым внешним устройствам рабочих станций выполняется только по специальным служебным запискам;

- сотрудником ответственным за информационную безопасность выполняется постоянный контроль доступа к внешним устройствам и портам рабочих станций;

- настройка основных программных продуктов на автоматическое («по умолчанию») сохранение служебной информации на не системных разделах рабочих станций;

- запрещается установка на рабочие станции любых программных средств без согласования с сотрудником ответственным за информационную безопасность;

- пользователь обязан блокировать доступ к своей рабочей станции когда он покидает рабочее место;

4. СЕТЕВАЯ БЕЗОПАСНОСТЬ

(безопасность серверов и сетевых ресурсов)

4.1. В обязательном порядке использования межсетевого экрана.

4.2. Предусмотреть выделение всем отделам ограниченных объемов дискового пространства на сетевых дисках отделов.

4.3. Строгое соблюдение согласованного регламента резервного копирования служебной информации, размещенной на сетевых дисках.

4.4. Запрещается использование любых средств для получения через ЛВС доступа к локальным дискам других работников.

4.5. Запрещается фальсификация IP-адресов, а также использование IP-адресов не зарегистрированных в отделе информатизации и на сотрудника, ответственного за информационную безопасность.

4.6. Запрещается хранение на сетевых дисках отделов любой информации не связанной с функциями этих подразделений.

5. ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

5.1. Все серверы, межсетевые экраны и коммутационное оборудование должны находиться в отдельных, специальным образом оборудованных помещениях, доступ в которые разрешен только администраторам; в рабочее время двери в эти помещения должны быть закрыты.

5.2. Допуск в помещения с оборудованием, обеспечивающим бесперебойное питание серверов и рабочих станций, строго ограничен списком лиц, имеющих право на техническое обслуживание и ремонт этого оборудования.

5.3. Обязательным условием физической безопасности рабочих станций, является блокирование несанкционированного доступа в системные блоки работников администрации не имеющих соответствующих полномочий. Это производится с целью осуществления контроля за несанкционированным снятием накопителей на жестких магнитных дисках и исключения возможности бесконтрольного подключения дополнительных внешних устройств..

5.4. Все рабочие станции, закрепляются лично за каждым из работников администрации, который несет полную (дисциплинарную и административную) ответственность за:

|  |  |
| --- | --- |
| 1 | сохранность комплектности оборудования; |
| 2 | целевое использование локальных (информационное пространство рабочей станции) и сетевых ресурсов ЛВС, предоставленных ему (ей) для выполнения служебных обязанностей; |
| 3 | самостоятельное и (или) с помощью третьих лиц несанкционированное подключение любых внешних устройств и ноутбуков; |
| 4 | допуск других работников и лиц, не являющихся работниками администрации, к работе на закрепленной за ним (ней) рабочей станции (исключение составляют администраторы рабочих станций и информационных ресурсов и работник ответственный за информационную безопасность) |

6. ПЕРЕСМОТР ПОЛИТИКИ

6.1. Политика подлежит полному пересмотру в случае несоответствия определенных данной Политикой мер безопасности, реальным условиям их применения для доступа пользователей к информационным ресурсам, а также для контроля доступа к рабочим станциям и ЛВС, и соответствия существующим требованиям ПТД на средства защиты конфиденциальной и/или иной защищаемой информации.

6.2. Частичный пересмотр данной Политики проводится по указанию руководства или письменному обоснованному предложению администратора информационной безопасности В обязательном порядке изменения (сведения о них) фиксируется в «Листе регистрации изменений в Политике».

6.3. Вносимые изменения не должны противоречить другим положениям Политики.

7. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПОЛИТИКИ

7.1. Ответственность за организацию в администрации выполнения требований данной Политики, организацию контрольных и проверочных мероприятий по вопросам безопасности рабочих станций и серверов возлагается на отдел программного обеспечения, в функции которого входит обеспечение информационной безопасности.

7.2. Ответственность за доведение Политики до работников в части их касающейся и обеспечение условий для выполнения требований данной Политики возлагается на начальников отделов, эксплуатирующих СВТ.

7.3. Ответственность за соблюдение требований настоящей Политики возлагается на всех работников, использующих СВТ.

7.4. Работники, в должностные обязанности которых входит обеспечение информационной безопасности, проводят постоянный выборочный контроль выполнения работниками требований Политики с соответствующими отметками в отдельном журнале. О фактах нарушения требований настоящей Политики работники обязаны докладывать должностному лицу, в обязанности которого входит контроль за обеспечением информационной безопасности.

Лист регистрации изменений в Политике

**ЛИСТ**

**регистрации изменений**

|  |  |  |  |
| --- | --- | --- | --- |
| Дата | Содержание вносимого изменения | Кем санкционировано изменение (каким документом) | Подпись лица, произведшего изменения |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Приложение № 10

к Положению об обеспечении безопасности общедоступной информации в информационных системах администрации города Алейска Алтайского края

Политика

управления парольной защитой

администрации города Алейска Алтайского края

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика управления парольной защитой (далее – Политика), включает в себя взаимоувязанный комплекс организационных мер, программных и технических средств защиты, применяемых при генерации и (или) выборе, использовании, уничтожении парольной информации, а также контроль за действиями пользователей и обслуживающего персонала автоматизированных систем (далее АС) администрации города Алейска Алтайского края (далее администрация) при работе с паролями.

1.2. Требования настоящей Политики являются неотъемлемой частью комплекса мер безопасности и защиты информации (СЗИ).

1.3. Требования настоящей Политики распространяются на всех должностных лиц и работников комитетов, использующих в работе СВТ (включая работу в ЛВС) и должны применяться для всех средств вычислительной техники.

1.4 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в АС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на сотрудника на которого возложены обязанности по информационной безопасности - администратора парольной защиты.

1.5. Ознакомление всех работников администрации, использующих средства ВТ, с требованиями Политики проводит сотрудник ответственный за информационную безопасность. Факт ознакомления сотрудника фиксируется на контрольном экземпляре “Политики управления парольной защитой” с указанием даты и личной подписи работника. При ознакомлении с Политикой внимание работников акцентируется на предупреждении их о персональной ответственности за разглашение парольной информации. При необходимости сотрудник ответственный за информационную безопасность проводит персональные повторные инструктажи.

1.6. В целях закрепления знаний по вопросам практического исполнения требований Политики, разъяснения возникающих вопросов, проводятся семинары организуемые сотрудником ответственным за информационную безопасность (не реже 1 раз в год) и персональные инструктажи (при необходимости) пользователей средств ВТ.

1.7. В случае невозможности исполнения требований настоящей Политики в полном объеме, например:

- в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний;

- злоумышленных действий;

- в случае программно-технических особенностей эксплуатируемых СВТ

практическая «глубина» исполнения настоящей Политики определяется отделом программного обеспечения.

2. ЦЕЛЬ УПРАВЛЕНИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

Целью управления парольной защиты (подсистемы) является:

- организация в администрации единой системы управления парольной защитой информации, обрабатываемой с использованием средств вычислительной техники;

- систематизация и упорядочение требований на средства защиты информации в едином специальном документе для практической работы пользователей ВТ при генерации (выборе) ими качественных (трудно подбираемых) паролей

3. КАЧЕСТВО И ОБРАЩЕНИЕ ПАРОЛЬНОЙ ИНФОРМАЦИИ

3.1. Пароли доступа к аппаратно-программным вычислительным средствам, информационным ресурсам первоначально формируются администратором парольной защиты, а в дальнейшем выбираются пользователями самостоятельно, но с учетом следующих требований к качеству парольной информации (таблица 1):

Таблица 1

Требования к качеству парольной информации

|  |  |  |
| --- | --- | --- |
| **Параметр качества пароля** | **Администратор** | **Пользователь** |
| Минимальная длина пароля в символах | 8 | 8 |
| Максимальная длина пароля в символах | 16 | 16 |
| Содержание в пароле букв верхнего и нижнего регистра | да | да |
| Содержание в пароле специальных символов (@, #, $, &, \* и т.п.) и цифр | обязательно | обязательно при обработке информации конфиденциального характера |
| Содержание в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, именований АРМ и т.д. и т.п.; | нет | нет |
| Содержание в пароле общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP и т.д.) | нет | нет |
| Минимальное отличие нового пароля от предыдущего (в позициях)  | 6 | 6 |
| Максимальный срок действия пароля: |  |  |
| - администратор  | 90 дней | - |
| - пользователь ЛВС | - | 60 дней |
| - доступ к информационным ресурсам: |  |  |
| - доступ к региональным информационным ресурсам  | 90 дней | 90 дней |
| Минимальный срок действия пароля | нет | нет |
| Сдача копий паролей на резервное хранение | да | необязательно |
| Парольная заставка монитора рабочей станции | да | да |

3.2. Резервные копии всех паролей каждого из системного администратора, администраторов информационных ресурсов и администратора информационной безопасности должны сдаваться на хранение в сейфе начальника отдела программного обеспечения.

3.3. Свои (личные) пароли и/или персональные идентификаторы (электронные USB-ключи) администраторы и пользователи самостоятельно никому не имеют права сообщать и(или) передавать. В случае производственной необходимости (командировка, отпуск и т.п.) и/или при проведении контрольно-проверочных мероприятий, выполняемых отделом программного обеспечения, допускается раскрытие значений своего пароля и/или передача персональный идентификатор) только своим непосредственным руководителям. По окончанию производственных и/или контрольно-проверочных работ работники производят немедленную смену значений «раскрытых» паролей;

администратор (владелец) вскрытой парольной информации немедленно (в первом же сеансе работы с ЛВС и(или) ВТ) меняет скомпрометированную парольную информацию.

3.4. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п., а также технологической необходимости использования имен и паролей некоторых работников (в их отсутствие) допускается изменение паролей, администратором парольной защиты. В подобных случаях, сотрудники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения.

3.5. Внеплановая смена личного пароля или удаление учетной записи пользователя в локальной вычислительной сети в случае прекращения его полномочий (увольнение, переход на другую работу внутри администрации и т.п.) должна производиться уполномоченными сотрудниками отдела программного обеспечения (системными администраторами).

3.6. Организационное обеспечение данного требования:

3.6.1. Администратор парольной защиты, получив выписку из приказа о приеме работника (о назначении работника на должность в другом отделе; о расторжении служебного контракта с работником (увольнении); об уходе работника в декретный отпуск и т.д.), из которой вытекает прекращение полномочий работника администрации по работе с СВТ и/или ЛВС, выполняет следующие действия:

 изымает персональный идентификатор (электронный USB-ключ еToken) у работника(ов) сразу же (незамедлительно, в течение получаса) после получения выписки из приказа;

 факт изъятия электронный USB-ключ еToken фиксируется в специальном журнале учета персональных идентификаторов или специальном списке, являющимся неотъемлемой частью Политики идентификации пользователей в ЛВС;

3.6.2. Системный администратор, немедленно выполняет: в случае увольнения (ухода в декретный отпуск) работника - удаление из ЛВС учетной записи (имени компьютера в ЛВС) и соответствующего имени регистрации и других реквизитов доступа работника к ЛВС. В случае перевода работника в другой отдел – выполняет: перевод имени регистрации пользователя ЛВС в другую группу, соответствующую новому отделу, куда переведен работник; соответствующую подготовку рабочей станции для работы в ЛВС.

Администраторы соответствующих информационных ресурсов незамедлительно блокируют доступ пользователя ко всем, ранее ему доступным, информационным ресурсам.

3.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри администрации и другие обстоятельства) администратора парольной защиты.

3.8. Организационное обеспечение данного требования:

3.8.1. Администратор информационной безопасности, получив информацию организовывает в администрации полную смену паролей, направляя по электронной почте соответствующие указания и (или) предложения начальникам отделов о полной смене парольной информации в ЛВС и рабочих станциях;

3.8.2. Начальники отделов, получив указание о полной смене парольной информации, организовывают такие работы в своих подразделениях и по окончанию работ, направляют соответствующее отчеты-уведомления сотруднику ответственному за информационную безопасность.

3.9. В случае компрометации пароля хотя бы одного субъекта доступа к ЛВС, рабочим станциям и/или информационным ресурсам, работник, выявивший данный факт, обязан незамедлительно поставить в известность сотрудника ответственного за информационную безопасность, который обязан оперативно предпринять меры, в соответствии с вышеизложенными пунктами настоящей Политики, в зависимости от полномочий владельца скомпрометированного пароля и обстоятельств компрометации.

3.10. Хранение работником (пользователем) значений своих паролей на бумажном носителе допускается только в опечатываемом владельцем пароля конверте в сейфе у руководителя подразделения или администратора парольной защиты (возможно вместе с персональным идентификатором (электронным USB-ключeм еToken).

3.11. Повседневный контроль за действиями пользователей ЛВС при работе с паролями, соблюдением порядка их смены и использования возлагается на ответственных за информационную безопасность.

4. ПЕРЕСМОТР ПОЛИТИКИ

4.1. Политика подлежит полному пересмотру:

- в случае приобретения новых (дополнительных к имеющимся штатным) автоматизированных средств управления парольной защитой и(или) генерации (выбора) паролей. В остальных случаях Политика подлежит частичному пересмотру;

- с целью проверки соответствия определенных данной Политикой мер защиты, реальным условиям их применения для доступа пользователей в ЛВС и информационным ресурсам, а также для контроля доступа к рабочим станциям, и соответствия существующим требованиям ПТД на средства защиты конфиденциальной и/или иной защищаемой информации.

4.2. Частичный пересмотр данной Политики проводится по указанию руководства или письменному обоснованному предложению администраторов информационной безопасности и парольной защиты..

5. ОТВЕТСТВЕННЫЕ ЗА ОРГАНИЗАЦИЮ И КОНТРОЛЬ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПОЛИТИКИ

5.1. Ответственность за организацию выполнения требований данной Политики, организацию контрольных и проверочных мероприятий по вопросам парольной защиты возлагается на сотрудника ответственного за информационную безопасность.

5.2. Ответственность за доведение Политики до работников в части их касающейся и обеспечение условий для выполнения требований данной Политики возлагается на руководителей отделов, эксплуатирующих СВТ.

5.3. Ответственность за соблюдение требований настоящей Политики возлагается на всех работников, использующих СВТ.

5.4. Все работники обязаны по первому требованию сотрудника ответственного за информационную безопасность предъявить значения действующего личного пароля для контроля соответствия установленным требованиям, а после проверки провести немедленную его смену..

5.5. Администратор парольной защиты проводит ежеквартальный выборочный контроль выполнения работниками требований Политики. О фактах несоответствия качества паролей и/или условий обеспечения их сохранности администратор парольной защиты докладывает начальнику отдела.