Приложение № 1
к протоколу заседания Совета директоров
АО «КазАгроФинанс»
от «27» октября 2023 года № 10

УТВЕРЖДЕНА
решением Совета директоров
АО «КазАгроФинанс»
от «27» октября 2023 года № 10

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «КАЗАГРОФИНАНС»

Срок введения в действие установлен
« » _____ 2023 года

г. Астана, 2023 год

издание: пятое

Оглавление

Глава 1. Общие положения

1. Настоящая Политика информационной безопасности (далее - Политика) АО «КазАгроФинанс» (далее - Общество) разработана с целью обеспечения устойчивого функционирования информационных систем Общества, предотвращения возможности совершения финансовых преступлений при помощи вычислительных и телекоммуникационных средств, утраты, утечки, искажения и уничтожения информации ограниченного распространения, определения наиболее эффективных способов использования вычислительных и коммуникационных ресурсов Общества.

2. Политика определяет основные требования и позицию Общества в сфере сохранности и неразглашения защищаемой информации в Центральном аппарате и филиалах Общества в любом виде: устно, письменно, на магнитных, оптических и других носителях, а также данных, передаваемых посредством глобальных и локальных сетей.

3. Политика разработана в соответствии с законодательством Республики Казахстан и внутренними нормативными документами Общества.

Область действия Политики распространяется на все структурные подразделения и филиалы Общества, включая все бизнес-процессы.

Глава 2. Термины и определения

4. В Политике используются следующие понятия:

1) **автоматизированная система обработки информации** - организационно упорядоченная совокупность технических средств обработки и передачи данных, методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей потребителей информации;

2) **атака на информационную систему** - любое действие, выполняемое нарушителем, которое приводит к реализации угрозы, путем использования уязвимостей системы;

3) **аутентификация** - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа имеющимся в системе;

4) **безопасность информации** - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования;

5) **безопасность информационной технологии** - защищенность технологического процесса переработки информации;

6) **блокирование** - искусственное затруднение доступа пользователей к информации, содержащейся в компьютере, не связанное с ее уничтожением;

7) **внешний воздействующий фактор** - воздействующий фактор, внешний по отношению к объекту информатизации;

8) **внутренний воздействующий фактор** - воздействующий фактор, внутренний по отношению к объекту информатизации;

9) **вредоносные программы** - программы или измененные программы объекта информатизации, приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нарушению работы;

10) **документированная информация (документ)** - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

11) **доступность** - состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно;

12) **идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

13) **информация** - упорядоченная последовательность знаков, символов, цифр звуковых сигналов, другой материи, закрепленных на различных носителях информации и носящих определенный смысл;

14) **информационная безопасность** - защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, утечки, хищения, утраты, уничтожения, искажения, копирования, подделки, блокирования и других угроз, возникающих в результате несанкционированного доступа;

15) **информационные процессы** - процессы сбора, обработки, обмена, накопления, хранения, уничтожения, поиска и распространения информации;

16) **информационная система** - совокупность информационных технологий, информационных сетей и средств их программно-технического обеспечения, предназначенных для реализации информационных процессов;

17) **информационные ресурсы** - отдельные документы и отдельные массивы документов, данные и массивы информации в информационных системах (библиотеках, архивах, фондах, базах данных);

18) **источник угрозы** - это потенциальные антропогенные, техногенные или стихийные носители угрозы информационной безопасности;

19) **конфиденциальность** - доступность компонента системы только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия;

20) **несанкционированные действия** - действия субъекта в нарушение установленных в системе правил обработки информации;

21) **обработка информации** - передача, прием, преобразование, хранение и отображение информации;

22) **объект информатизации** - совокупность информационных ресурсов, программного обеспечения, компьютерного и периферийного, оборудования вместе с помещениями, в которых они установлены;

2 3) **пользователь (потребитель) информации** - субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации;

24) **последствия реализации угрозы информационной безопасности** - возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся факторы уязвимости в СУИБ;

25) **разграничение доступа** - система мероприятий, организованных в информационной системе и обеспечивающих предоставление пользователям доступа к информации на основе предоставленных им прав;

26) **сеть (локальная сеть, ЛВС, LAN)** - группа точек, узлов или других устройств, соединенных коммуникационным набором оборудования, обеспечивающая соединение станций и передачу между ними информации;

2 7) **система управления информационной безопасности (СУИБ)** - часть общей системы менеджмента Общества, основанной на риск-ориентированном подходе,

предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования информационной безопасности компании;

28) **угроза информационной безопасности** - совокупность условий и факторов, создающих предпосылки к возникновению инцидента, связанного с нарушением информационной безопасности;

29) **фактор уязвимости** - это присущие объекту информатизации причины, приводящие к нарушению информационной безопасности на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемым программным обеспечением и аппаратной платформой, условиями эксплуатации;

30) **хакер** - лицо, совершающее различного рода незаконные действия:

- несанкционированное проникновение в чужие компьютерные сети и получение из них информации;
- незаконные снятие защиты с программных продуктов и их копирование;
- создание и распространение компьютерных программ, содержащих вредоносный код (вирусы);

31) **целостность информации** - свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому ее состоянию);

32) **штатные средства -** совокупность программных, аппаратных средств, имеющихся в Обществе и позволяющих выполнять определенные функциональные задачи.

Глава 3. Цели, задачи и направления Политики

5. Целями Политики являются:

1) обеспечение устойчивого функционирования информационных систем Общества путем предотвращения реализации угроз безопасности информационных систем;

2) недопущение разглашения, утраты, утечки, искажения и уничтожения защищаемой информации;

3) исключение угрозы негативного воздействия на репутацию Общества.

6. Основными задачами Политики являются:

1) своевременное выявление угроз безопасности информационным ресурсам Общества, причин и условий, способствующих нанесению финансового, материального и морального ущерба информационным ресурсам и процессам;

2) защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

3) создание условий функционирования Общества с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;

4) создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Общества, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности.

7. Основные пути решения задач СУИБ достигаются:

1) строгим учетом всех подлежащих защите ресурсов информационной системы Общества (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

2) полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Общества по вопросам обеспечения безопасности информации;

3) четким знанием и строгим соблюдением всеми пользователями информационной системы Общества требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

4) персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Общества;

5) применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

6) эффективным контролем над соблюдением пользователями информационных ресурсов Общества требований по обеспечению безопасности информации;

7) юридической защитой интересов Общества при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

8. Основными направлениями Политики являются:

1) обеспечение информационной безопасности;

2) создание условий для эффективного и качественного информационного обеспечения решений задач, стоящих перед Обществом, обеспечение условий для развития защиты информационных ресурсов;

3) совершенствование СУИБ;

4) совершенствование внутренних нормативных документов Общества в области СУИБ;

5) разработка мероприятий и рекомендации по обеспечению информационной безопасности структурных подразделений Общества.

Глава 4. Требования Политики

9. Техническая инструкция к Политике, а также правила, требования и регламенты Общества, регламентирующие порядок обеспечения информационной безопасности, являются внутренними нормативными документами Общества, реализующими Политику путем определения ключевых требований:

1) по обеспечению информационной безопасности в Обществе;

2) к осуществлению мониторинга деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

3) к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности;

4) к проведению анализа информации об инцидентах информационной безопасности;

5) к ответственности работников Общества за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей.

10. Требования к осуществлению мониторинга событий информационной безопасности, возникающих в процессе работы с информацией при доступе, обработке, передаче данных в информационных системах Общества, определяются в соответствии с Правилами мониторинга событий информационной безопасности АО «КазАгроФинанс». Мониторинг событий информационной безопасности осуществляется непрерывно, с использованием системы управления событиями информационной безопасности, а также через консоли централизованного управления соответствующих систем защиты информации, в том числе:

1) систем антивирусной защиты;

2) систем обнаружения вторжения;

3) межсетевых экранов и маршрутизаторов;

4) систем предотвращения утечек конфиденциальной информации;

5) систем аудита операционных систем, систем управления базами данных, систем виртуализации, прикладного программного обеспечения;

6) систем управления и контроля логическим доступом;

7) других компонентов информационной системы.

11. Требования к осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности, а также проведению анализа информации об инцидентах информационной безопасности, определяются в соответствии с Регламентом управления инцидентами АО «КазАгроФинанс».

12. Требования о применимости мер и средств контроля и управления информационной безопасностью определяются Положением о применимости средств управления информационной безопасностью в АО «КазАгроФинанс», являющимся Приложением к настоящей Политике.

Глава 5. Угрозы информационной безопасности

13. Организация обеспечения безопасности информации Общества носит комплексный характер и основывается на анализе возможных негативных последствий. Анализ возможных негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и способов их предотвращения.

14. Виды угроз информационной безопасности:

1) **антропогенные** - в качестве антропогенного источника угроз следует рассматривать субъекты, имеющие доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта.

Субъекты антропогенного источника угроз делятся на 2 (два) вида, действия которых могут привести к нарушению безопасности информации, внешние и внутренние.

Внешние субъекты случайные или преднамеренные, имеют разный уровень квалификации. К ним относятся:

- криминальные структуры;
- хакеры;
- недобросовестные партнеры;
- технический персонал поставщиков коммуникационных услуг;
- представители надзорных организаций и аварийных служб;
- любые другие субъекты, имеющие доступ в здание.

Внутренние субъекты, представляют собой персонал Общества в области разработки и эксплуатации программного обеспечения и технических средств, а также персонал, выполняющий работу технического и вспомогательного характера. Вышеописанный персонал имеет возможность использования штатного оборудования, технических средств сети и доступа в помещения их непосредственного расположения. К ним относятся:

- основной персонал (пользователи, программисты, разработчики);
- вспомогательный персонал (уборщики, охрана);

- технический персонал (жизнеобеспечение, эксплуатация);

2) **техногенные -** угрозы, вызываемые технократической деятельностью человека и развитием цивилизации. Данный класс источников угроз безопасности информации выделяется Обществом особенно, так как в сложившихся условиях ожидается резкий рост числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования.

К техническим средствам, являющимся источниками потенциальных угроз безопасности относятся:

Внешние:

- средства связи;
- сети инженерных коммуникации (водоснабжения, канализации).

Внутренние:

- некачественные технические средства обработки информации;
- некачественные программные средства обработки информации;
- вспомогательные средства (охраны, сигнализации, телефонии);
- другие технические средства, применяемые в Обществе;

3) **стихийные** - угрозы, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех, процесс развития которых не управляем Обществом. Такие источники угроз не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними Обществом определены следующие понятия:

- пожары;
- землетрясения;
- ураганы;
- другие аналогичные явления.

Глава 6. Принципы организации и функционирования СУИБ

15. В целях организации и полноценного функционирования СУИБ Общество руководствуется следующими основными принципами:

1) **комплексность** - обеспечение информационной безопасности от возможных угроз всеми доступными методами и средствами на всех технологических этапах обработки и использования информации, во всех режимах функционирования;

2) **системность** - логичный и последовательный подход к вопросам организации информационной безопасности:

- оценка риска информационной безопасности, исходя из реальных угроз и уязвимости информационных ресурсов;
- создание комплекса организационных и технических мер, а также средств защиты, учитывающих специфику Общества;

3) **своевременность** - предполагает постановку задач по комплексной информационной безопасности на ранних стадиях разработки системы безопасности, на основе анализа и прогнозирования угроз информационной безопасности Общества, финансовой обстановки, а также разработку эффективных мер предупреждения возможных рисков и посягательств на его законные интересы;

4) **непрерывность** - принцип постоянного функционирования системы информационной безопасности, учитывающий возможность обхода защитных мер с использованием легальных и нелегальных методов;

5) **законность** - предполагает разработку системы информационной безопасности на основе законодательства Республики Казахстан и внутренних нормативных документов Общества по безопасности, с применением всех дозволенных методов обнаружения и пресечения правонарушений;

6) **обоснованность** - используемые средства защиты информации, их функции и возможности должны соответствовать современному уровню развития техники, быть адекватными уровню информационной безопасности;

7) **экономическая целесообразность** - сопоставимость возможного ущерба затратам на обеспечение безопасности (критерий «эффективность - стоимость»). Во всех случаях стоимость систем безопасности должна быть меньше размера возможного ущерба от реализации любых видов риска;

8) **взаимодействие и координация** - означает осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи подразделений службы безопасности, информационных технологий и подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами.

Эксплуатация технических средств и реализация мер информационной безопасности Общества должны осуществляться профессионально подготовленными работниками подразделений;

9) **совершенствование системы информационной безопасности** - предусматривает внедрение и совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;

10) **централизация управления** - предполагает функционирование системы информационной безопасности по единым правовым, организационным, функциональным и методологическим принципам и централизованное управление деятельностью системы безопасности с учетом изменяющихся условий и имеющихся факторов риска.

Глава 7. Информационная инфраструктура и объекты защиты

16. Информационная инфраструктура Общества включает в себя информационные ресурсы, автоматизированные системы, средства вычислительной техники, инженерные системы их жизнеобеспечения, а также помещения, в которых функционируют автоматизированные системы и обрабатывается информация. С информационной инфраструктурой неразрывно связаны работники Общества.

17. Информационные ресурсы Общества складываются из исходной информации, баз данных, системного, сетевого, операционного и инструментального программного обеспечения, информации хранящейся на бумажных носителях, представленная как в документарной, так и в иной форме.

18. Часть информации Общества обрабатывается на средствах оргтехники, документирования, документальной и речевой связи общего пользования (персональные компьютеры, лазерные и матричные принтеры, факсимильные аппараты, телефоны внутренней и городской автоматических телефонных станций и другое).

19. Отдельные элементы инфраструктуры Общества (системы электропитания, пожарной и охранной сигнализации, проводного радиовещания и другое), в силу соприкосновения с информационными системами, являются вторичными носителями защищаемой информации или каналами ее утечки.

Глава 8. Правовое обеспечение информационной безопасности

20. Правовая защита экономических интересов, репутации Общества от преступных посягательств обеспечивается в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами Общества.

21. Эффективное решение задач обеспечения безопасности достигается формированием системы внутренних нормативных правовых актов и неукоснительным выполнением функциональных обязанностей работников Общества.

Глава 9. Техническое обеспечение информационной безопасности

22. Техническое обеспечение информационной безопасности Общества базируется:

1) на системе унификации и взаимного дополнения применяемых средств защиты;

2) на системе государственной сертификации всего программного обеспечения и средств защиты;

3) на системе лицензирования деятельности.

23. СУИБ Общества предусматривает комплекс организационных, технических, программных и криптографических средств, а также мер по защите информации в процессе документооборота, при работе пользователя, имеющего санкционированный доступ к конфиденциальным документам и сведениям, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров. СУИБ также предусматривает резервирование и восстановление ресурсов информационных систем Общества, для компенсации угроз, связанных с техногенными факторами, защиты от уничтожения, изменения информации, а также обеспечения устойчивости к критическим ситуациям, связанным с уничтожением информации по вине человеческого фактора.

Предоставление прав доступа работникам Общества к соответствующей информации определяется в соответствии с внутренними нормативными документами Общества.

24. В рамках обеспечения информационной безопасности Общества, предусматриваются следующие мероприятия:

1) контроль ограничение доступа работников и посторонних лиц в здания, помещения, где обрабатывается (хранится) информация конфиденциального характера;

2) контроль разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;

3) контроль за несанкционированным доступом и действиями пользователей;

4) предотвращение внедрения в автоматизированные информационные системы программ вирусного характера.

25. Защита информационных ресурсов Общества от несанкционированного доступа предусматривает:

1) контроль определения групп пользователей информационных систем и разделение их на категории по выполняемым функциям, а также установление им уровней доступа к информации;

2) персональную ответственность работника, предполагающую ответственность в случае разглашения конфиденциальной информации (документов, носителей информации);

3) надежность хранения, предполагающую хранение информации (документов, носителей информации, информационных массивов, резервных копий информации, содержащихся в

информационных системах Общества) в условиях, максимально защищенных от возможности уничтожения, подделки, искажения или несанкционированного доступа;

4) централизованный контроль за действиями работников с конфиденциальными документами и защищаемой информацией в автоматизированных системах;

5) целостность технической и программной среды, обрабатываемой информации и средств защиты, предполагающих физическую сохранность средств информатизации, неизменность программной среды, определяемой предусмотренной технологией обработки информации, выполнение средствами защиты предусмотренных функций, изолированность средств защиты от пользователей;

6) надежность хранения кабелей связи, схем их расположения в условиях, защищенных от несанкционированного подключения.

26. В процессе формирования заказа на построение информационной системы, Общество учитывает не только основной набор функциональных сервисов (бухгалтерские системы, системы автоматизации офисных процедур, делопроизводства и т.д.), но и ряд необходимых вспомогательных сервисов, обеспечивающих надежное функционирование системы и требуемый уровень безопасности. В случае, если не все функционально законченные сервисы обладают полным набором механизмов безопасности, они требуют объединения в составные сервисы, в совокупности обладающих таким набором и с внешней точки зрения представляющих собой единое целое.

27. Надежность хранения информации Общества обеспечивается оборудованием помещений, в которых ведется обработка и хранение защищаемой информации, сейфами и металлическими шкафами для хранения документов.

28. Целостность автоматизированных систем Общества достигается комплексом программно-технических средств и организационных мероприятий, осуществляемых уполномоченными подразделениями Общества.

29. При необходимости передачи защищаемой информации Общества, на небольших расстояниях используются защищенные линии связи.

30. В целях обеспечения функционирования СУИБ Общество проводит предпроектное обследование и проектирование информационных систем, выработку требований по средствам защиты информации и контроля, предполагаемых к использованию в этих системах, а также контроль защищенности информационных ресурсов.

Глава 10. Организационное обеспечение информационной безопасности

31. В работе с персоналом основными организационными мерами в плане достижения информационной безопасности являются:

1) получение у работников Обществе добровольного, письменного согласия на соблюдение требований, регламентирующих режим информационной безопасности и сохранность защищаемой информации при заключении контрактов о найме, индивидуальных трудовых договоров;

2) проведение периодического обучения и повышения квалификации персонала в области информационной безопасности;

3) обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;

4) организация контроля доступа и режима выполнения работ персоналом подразделения информационных технологий;

5) инспектирование правильности и полноты выполнения персоналом подразделения информационных технологий Общества мер по обеспечению сохранности необходимых дубликатов файлов, библиотеки программ, оборудования системы;

6) практическая проверка функционирования отдельных мер защиты и предотвращения недозволенных изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.

32. Отчет об исполнении плана мероприятий по реализации Стратегии Общества в части обеспечения информационной безопасности, информация о состоянии информационной безопасности, предоставляется Совету директоров Общества периодичностью один раз в год.

Глава 11. Участники СУИБ, контроль и ответственность

33. Участниками СУИБ являются:

1) орган управления - Совет директоров Общества, утверждает Политику;

2) исполнительный орган - Правление Общества, уполномочено принимать решения, в том числе по задачам обеспечения информационной безопасности, утверждает внутренние документы по информационной безопасности;

3) подразделение по информационной безопасности - отдел информационной безопасности Департамента безопасности, осуществляет координацию и контроль деятельности подразделений Общества в области СУИБ;

4) подразделение по информационным технологиям - Департамент развития информационных технологий, обеспечивает деятельность информационной инфраструктуры Общества;

5) подразделение по безопасности - Департамент безопасности, реализует меры физической и технической безопасности;

6) подразделение по работе с персоналом - Департамент управления человеческими ресурсами, обеспечивает подписание работниками обязательств о неразглашении конфиденциальной информации;

7) юридическое подразделение - Правовой департамент, осуществляет правовую экспертизу внутренних документов по вопросам обеспечения информационной безопасности;

8) подразделение по комплаенс-контролю - Антикоррупционная комплаенс-служба, совместно с юридическим подразделением определяет виды информации, подлежащие включению в перечень защищаемой информации;

9) подразделение внутреннего аудита - Служба внутреннего аудита, проводит оценку состояния СУИБ в соответствии с внутренними документами;

10) подразделение по управлению рисками информационной безопасности - в связи с отсутствием в штатной структуре одноименного подразделения его функции выполняются отделом информационной безопасности Департамента безопасности.

34. Ответственность за соблюдение требований Политики несут:

1) руководство Общества, члены Правления, Управляющие директора;

2) подразделение по развитию информационных технологий - ответственные за создание и поддержание непрерывности функционирования информационных систем и ресурсов, реализацию технических мер, необходимых для настройки данной информационной политики безопасности;

3) подразделение по информационной безопасности - ответственные за определение необходимой политики безопасности и поддержание систем защиты и безопасности информационных систем и ресурсов Общества;

4) пользователи, имеющие доступ к информационным ресурсам, которые обязаны выполнять политику безопасности и ставить в известность подразделение по информационной безопасности обо всех подозрительных ситуациях;

5) руководители структурных подразделений - ответственные за обеспечение ознакомления работников с внутренними документами Общества, содержащими требования к информационной безопасности, а также ответственные за обеспечение информационной безопасности в возглавляемых ими подразделениях.

35. В соответствии с возложенными должностными обязанностями, структурные подразделения Общества и работники, ответственные за выполнение требований настоящей Политики, обязаны контролировать и обеспечивать следующие направления:

1) подразделение по информационной безопасности выполняет функции по управлению информационной защиты, выявлению уязвимых мест информационных систем и ресурсов, требующих защиты, выбирая для их устранения эффективные средства защиты;

2) подразделение по информационной безопасности совместно с Подразделением по развитию информационных технологий проводят анализ уязвимых мест информационных систем и ресурсов, требующих защиты и выбирают для их устранения эффективные средства технической и программной защиты совместимые с телекоммуникационными системами Общества;

3) подразделение по информационной безопасности обеспечивает обучение персонала мерам безопасности и правилам поведения в чрезвычайных ситуациях в части защиты информационной безопасности;

4) в случае перевода в другое подразделение, нахождения работника в отпуске, командировке либо увольнения, подразделение по работе с персоналом обеспечивает незамедлительное информирование подразделения по развитию информационных технологий для блокирования учетной записи отсутствующего работника или изменения прав доступа.

36. Администраторы сетей, систем и приложений обеспечивают:

1) эффективное функционирование и отвечают за реализацию технических и организационных мер по обеспечению требований информационной безопасности по конкретным информационным системам, за корректное применение штатных механизмов защиты системных и информационных ресурсов и использование своих администраторских привилегий;

2) техническую и программную возможность обязательности процедур идентификации и аутентификации для доступа к ресурсам информационных систем;

3) уникальные идентификаторы и начальные пароли (или другую идентификационную и аутентификационную информацию) каждому пользователю только после того, как будет получено разрешение на доступ от подразделения по информационной безопасности;

4) недопущение появления и распространения в информационной системе Общества потенциально опасного программного обеспечения (вирусов), проверку рабочих станций и серверного оборудования на предмет правильной работы и своевременного обновления антивирусных программ.

37. Работники подразделения по информационной безопасности обязаны:

1) контролировать доступными методами состояние защищенности сетей, систем и приложений, оперативно и эффективно реагировать на события, влияющие на безопасность информации, своевременно выявлять и пресекать попытки нарушения защиты, информировать руководителей и представлять материалы для расследования инцидентов и применения санкций;

2) использовать проверенные средства мониторинга и аудита для обнаружения подозрительных ситуаций, ежедневно анализировать регистрационную системную информацию, относящуюся к безопасности сети, систем и приложений, вести архив регистрационной системной информации достаточной глубины;

3) планировать и периодически проводить проверку надежности защиты, достоверности системного программного обеспечения и целостности критичной информации.

38. Каждый пользователь отвечает за свои действия при обращении с информацией и при работе в информационных системах и ресурсах. Работники подразделений Общества обязаны:

1) знать и соблюдать установленные в Общества правила и процедуры обработки информации. Подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность подразделение по информационной безопасности обо всех нештатных или подозрительных ситуациях;

2) использовать информационные системы и ресурсы в соответствии с настоящей Политикой, требованиями безопасности к конкретным системам и приложениям. Использовать

доступные защитные механизмы для обеспечения целостности и конфиденциальности своей информации;

3) выбирать надежные пароли, регулярно менять их, не сообщать их другим лицам. Корректно идентифицировать себя при доступе в системы и к информационным ресурсам, не работать под именем другого пользователя;

4) не использовать и не распространять в информационной системе Общества постороннее программное обеспечение;

5) обеспечивать корректное поведение в информационной сети;

6) не предпринимать каких-либо действий по обходу или блокированию механизмов безопасности;

7) использовать только корпоративную электронную почту;

8) незамедлительно уведомлять администраторов информационных систем и работников подразделения по информационной безопасности о найденных уязвимостях или ошибках в программном обеспечении, а также информировать о неправомерных действиях других пользователей, нарушающих установленные правила информационной безопасности.

Глава 12. Заключительные положения

39. Пересмотр настоящей Политики и изменения/дополнения к ней осуществляются подразделением по информационной безопасности по мере необходимости в соответствии с порядком, определенным внутренними нормативными документами Общества.

40. Настоящая Политика обязательна для исполнения всеми работниками Общества.