Приложение 1
к приказу ФГБОУ ВО «ИВГПУ»
от 01.08.2025 № 124-01-07

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ивановский государственный политехнический университет»

УТВЕРЖДАЮ
и.о. ректора ИВГПУ
_____ Е.Н. Никифорова
01.08.2025 г.

ПОЛИТИКА
информационной безопасности
федерального государственного бюджетного образовательного учреждения высшего образования
«Ивановский государственный политехнический университет»

Иваново – 2025

Содержание

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с требованиями законодательства Российской Федерации в области информационной безопасности с целью документально опередить и зафиксировать требования, правила, процедуры обеспечения информационной безопасности (далее – ИБ) в федеральном государственном бюджетном образовательном учреждении высшего образования «Ивановский государственный политехнический университет» (далее – ИВГПУ, Университет).

1.2. Положения Политики распространяются на деятельность ИВГПУ в области защиты конфиденциальной информации (в том числе персональных данных) и не затрагивают вопросы защиты информации, составляющей государственную тайну Российской Федерации, а также служебной информации ограниченного распространения с пометкой «Для служебного пользования».

2. Термины, определения и сокращения

В настоящем документе используются следующие термины и определения:

Безопасность – состояние защищенности интересов (целей) Университета в условиях угроз ИБ.

Доступность – свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная безопасность – свойство информации сохранять конфиденциальность, целостность и доступность.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Университета, находящаяся в распоряжении Университета и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме (сама информация, а также вспомогательные системы и средства, используемые для защиты и надлежащей работы информационных систем Университета, оборудования, носители информации и прочее).

Информация – сведения (сообщения, данные) независимо от формы их представления.

Инцидент ИБ – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Конфиденциальная информация – информация, для которой в соответствии с законодательством Российской Федерации и (или) внутренними документами Университета обеспечивается сохранение свойства конфиденциальности.

Конфиденциальность – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

Пользователь – работник Университета или иное лицо, использующее активы Университета.

Регистрация событий защиты информации – фиксация данных о совершенных действиях или данных о событиях ИБ.

Риск ИБ – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Событие ИБ – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Угроза ИБ – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Управление рисками ИБ – систематический процесс применения установленных процедур (оценки рисков, обработки рисков, мониторинга рисков и пересмотра рисков) к деятельности Университета, связанной с использованием основных информационных активов.

Утечка информации – несанкционированное предоставление или распространение конфиденциальной информации, не контролируемое Компанией.

Целостность – свойство сохранять правильность и полноту активов. В настоящем документе используются следующие сокращения:

ИБ – информационная безопасность;

ИС – информационная система;

СКЗИ – средства криптографической защиты информации;

СКУД – система контроля и управления доступом;

ФСБ России – Федеральная служба безопасности;

ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

3. Цели и задачи информационной безопасности

3.1. Основной целью Университета в области обеспечения ИБ является минимизация рисков ИБ, которым подвержены технологии и информационные системы, используемые в Университете, а также обеспечение эффективности мероприятий по ликвидации неблагоприятных последствий реализации угроз и инцидентов ИБ.

3.2. Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для авторизованных пользователей – устойчивого функционирования ИС Университета, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время;
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в ИС Университета и передаваемой по каналам связи;
- конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

3.3. Достижение данной цели должно обеспечиваться решением следующих задач:

- вовлечение руководителей структурных подразделений Университета в процесс обеспечения ИБ;
- документирование требований ИБ;
- реализация мер по защите информационных активов Университета от угроз ИБ;
- оптимизация стоимости владения средствами защиты информации в Университете;
- прогнозирование угроз и оценка рисков ИБ;
- предотвращение и/или снижение до приемлемого уровня ущерба от реализации актуальных угроз ИБ в Университете;
- соблюдение законодательных, нормативных и договорных требований в области ИБ;
- повышение стабильности функционирования Университета в условиях возможной реализации угроз ИБ;
- реагирование на инциденты ИБ;
- контроль состояния ИБ Университета;
- повышение осведомленности в вопросах обеспечения ИБ;
- постоянное совершенствование систем обеспечения ИБ Университета.

4. Основные информационные активы

4.1. Основными информационными активами Университета, подлежащими защите, являются:

- персональные данные, внутренние документы Университета, информация, составляющая коммерческую тайну, иная информация, чувствительная по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности (в том числе открытая (общедоступная) информация), представленная в виде документов и информационных массивов, независимо от формы и вида их представления;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства обработки, передачи и отображения информации, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные компоненты ИС;
- процессы обработки информации в ИС – информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, процессы жизненного цикла ИС.

4.2. Перечень информационных активов, подлежащих защите, определяется по результатам инвентаризации (учета) / идентификации и классификации, проводимой рабочей группой, утвержденной приказом ректора.

5. Основные угрозы информационным активам

5.1. Основные угрозы информационным активам Университета включают в себя:

- разглашение защищаемой информации;
- компрометацию ключевой информации, персональных идентификаторов, паролей;
- несанкционированный доступ к защищаемой информации Университета;
- ввод некорректных (ложных) данных в ИС Университета;
- выход из строя материальных носителей защищаемой информации;
- уничтожение (утеря) защищаемой информации;
- нештатная ситуация в работе программного обеспечения ИС Университета;
- вирусное заражение;
- злонамеренные действия, осуществляемые посредством локальной вычислительной сети Университета;
- целенаправленные атаки на информационные активы Университета;
- выход из строя программно-технических средств Университета;
- нарушение функционирования технических мер защиты;
- несанкционированное или некорректное внесение изменений в информационные системы Университета;
- несанкционированное делегирование полномочий и/или использование привилегий;
- халатность, игнорирование установленных правил обеспечения ИБ, увеличивающие вероятность реализации угрозы ИБ.

5.2. Источники угроз ИБ делятся на два основных класса:

- источники, связанные с действиями людей – внешние и внутренние нарушители;
- источники, связанные с природными явлениями (стихийными бедствиями) и неблагоприятными техногенными факторами.

5.3. В качестве внешних нарушителей ИБ рассматриваются лица, не входящие в состав пользователей ИС Университета, например, внешние лица (хакеры, члены криминальных организаций, бывшие работники Университета и т.п.).

5.4. В качестве потенциальных внутренних нарушителей ИБ рассматриваются пользователи ИС Университета, другие субъекты (лица), вовлеченные в информационные процессы Университета, которые также имеют возможность санкционированного доступа к ИС и информационным активам Университета.

5.5. Перечень угроз безопасности информации и нарушителей безопасности определяется в ходе процедуры моделирования угроз.

6. Принципы обеспечения информационной безопасности

6.1. В основе реализации обеспечения ИБ лежит комплексный подход, который включает в себя следующие группы мер защиты информации:

- нормативно-правовые;
- организационные;
- программно-технические.

6.2. При построении ИБ Университет руководствуется рядом основополагающих принципов:

6.2.1. Неотъемлемость.

Безопасность ИС является их неотъемлемым свойством (характеристикой), а не дополнительным сервисом. Соблюдение требований ИБ должно быть обязательным для всех работников и являться частью корпоративной культуры Университета.

6.2.2. Комплексность.

Необходимо согласованное применение разнородных средств при построении целостной системы защиты информации, перекрывающей все каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна обеспечиваться физическими средствами,

организационными, технологическими и правовыми мерами, обеспечивающими в комплексе инженерно-техническую защиту объектов, защиту от несанкционированного доступа к компьютерам пользователей и серверам, разграничение доступа работников к информационным ресурсам, криптографическую защиту информации, защиту каналов обмена информацией, защиту информации от утечек по техническим каналам и т.д.

6.2.3. Системность.

Деятельность по защите информации должна быть строго и всесторонне регламентирована – Политика как совокупность норм, требований, положений, порядков и инструкций, должна учитывать все наиболее слабые и уязвимые места ИС и охватывать весь их жизненный цикл. При этом необходим учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения ИБ в ИС. Необходим анализ и учет всех текущих слабых и уязвимых мест ИС, возможных объектов и направлений атак, и, учитывая высокую квалификацию злоумышленников, возможных в будущем каналов реализации угроз ИБ.

6.2.4. Непрерывность.

Защита информации – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Университета, начиная с самых ранних стадий их проектирования.

6.2.5. Адекватность.

Применяемые методы и средства защиты информации должны быть адекватны угрозам ее уничтожения, утечке или искажения. Недопустима как недостаточная, так и чрезмерная защита. Создать абсолютно защищенную систему принципиально невозможно, взлом системы есть вопрос только времени и средств. В связи с этим, при проектировании систем защиты информации необходимо говорить только о некотором приемлемом уровне безопасности. Важно выбрать золотую середину между стойкостью защиты и ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими характеристиками систем защиты информации.

6.2.6. Идентификация и оценка активов.

Реализация принципа должна основываться на идентификации всех информационных активов и определении их ценности для целей и задач Университета.

6.2.7. Гибкость и управляемость.

Системы защиты информации должны обеспечивать возможность варьировать уровень защищенности ИС. Гибкость управления и применения системы защиты информации избавляет от необходимости принятия кардинальных мер по полной замене средств защиты на новые при смене условий функционирования защищаемых систем. В целях обеспечения гибкости и управляемости защиты ИС, при выборе между организационными и техническими мерами, приоритет должен отдаваться мерам технического характера.

6.2.8. Упреждение.

Акцент в работе системы обеспечения ИБ должен делаться на предотвращении (предупредительных мерах) событий ИБ, которые могут повлиять на целостность, доступность и конфиденциальность информации.

6.2.9. Контролируемость.

Обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации. Постоянный контроль ИБ Университета, выявление и устранение уязвимостей, мониторинг событий, влияющих на ее состояние, является обязательной составляющей эффективной системы обеспечения ИБ.

6.2.10. Следование лучшим практикам.

При реализации мер по обеспечению ИБ рекомендуется учитывать требования отечественных и международных стандартов в области ИБ как лучших практик.

6.2.11. Анализ и совершенствование.

Необходима постоянная работа по оценке эффективности и совершенствованию мер и средств защиты информации на основе анализа функционирования ИС, изменений в методах и средствах перехвата информации и воздействия на компоненты систем, изменений нормативных требований по защите, отечественного и зарубежного опыта в области защиты информации.

6.2.12. Минимизация полномочий.

Предоставление пользователям прав доступа определяется исключительно производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это минимально необходимо работнику для выполнения его должностных обязанностей.

6.2.13. Разделение функций.

При определении состава ролей, использующихся для распределения прав доступа, запрещается совмещение в рамках одной роли такого состава функций (концентрации полномочий), которое позволило бы одному работнику единолично осуществлять выполнение критичных операций или получать полный и неконтролируемый доступ к какой-либо системе Университета. Действия работников, обладающих административными полномочиями, должны находиться под особым контролем со стороны руководителей структурных подразделений

6.2.14. Персонификация.

Действия всех работников Университета должны осуществляться от имени персонифицированной учетной записи. Такая учетная запись у каждого работника должна быть единственной в связи с тем, что наличие у работника двух и более учетных записей делает не эффективной систему распределения и контроля полномочий. Исключение по решению руководства Университета могут составлять администраторы систем, должностные обязанности которых предполагают внесение изменений в указанные системы. Для них в дополнение к учетной записи с стандартными правами пользователя, может быть создана административная учетная запись с расширенными привилегиями. Наличие учетных записей, не закрепленных за конкретным работником, не допустимо.

6.2.15. Запрещено все, что не разрешено.

Доступ к любому объекту ИС должен предоставляться только при наличии соответствующего разрешения (правила), зафиксированного в документации, регламенте бизнес-процесса или настройках средств защиты информации. Любой доступ (не разрешенный явно) должен быть запрещен. Функция безопасности – разрешать необходимые доступы. Такой подход обеспечивает только известные безопасные доступы (действия) и освобождает от необходимости распознавать любую угрозу.

6.2.16. Стойкость средств защиты.

Уровень стойкости применяемых средств и эффективность мер защиты информации должны определяться ценностью защищаемого объекта и требовать от злоумышленника неадекватно больших затрат времени и вычислительных мощностей на их преодоление.

6.2.17. Осведомленность.

Осведомленность работников и обучающихся в вопросах ИБ – обязательное условие безопасного функционирования систем.

6.2.18. Персональная ответственность.

Ответственность за обеспечение безопасности информации и систем ее обработки возлагается на каждого работника Университета в пределах его полномочий.

7. Управление рисками информационной безопасности

7.1. Обеспечение ИБ Университета основывается на управлении рисками ИБ, что предусматривает анализ существующих угроз ИБ, оценку рисков реализации указанных угроз и принятие необходимых мер (в том числе применение средств защиты информации) по отношению к рискам ИБ, недопустимым для Университета.

7.2. Целью управления рисками ИБ является:

- минимизация негативных последствий от реализации рисков;
- оптимизация затрат, направленных на предотвращение негативных последствий от реализации рисков.

7.3. Непосредственную ответственность за процесс управления рисками ИБ структурных подразделений Университета несут руководители структурных подразделений.

8. Основные направления информационной безопасности

8.1. Документирование требований по ИБ:

8.1.1. В Университете разработан, утвержден и доведен до работников и обучающихся комплект документов (положения, инструкции), регламентирующий отдельные направления ИБ.

8.1.2. Документы по ИБ для гарантии их постоянной пригодности, соответствия и результативности должны пересматриваться через запланированные интервалы времени или в случае существенных изменений бизнес-процессов Университета или изменений требований законодательства Российской Федерации, нормативных документов Министерства науки и высшего образования Российской Федерации.

8.2. Организация ИБ:

8.2.1. Управление ИБ должно обеспечиваться как при осуществлении информационного обмена внутри Университета, так и при взаимодействии со сторонними организациями и третьими лицами (субъектами).

8.2.2. В Университете должно быть определено структурное подразделение и лица, ответственные за организацию планирования, совершенствования и развития обеспечения и управления ИБ в целом в ИВГПУ.

8.2.3. В структурных подразделениях Университета лицом ответственным за обеспечение ИБ, является руководитель данного подразделения.

8.2.4. При выборе средств обеспечения и контроля ИБ необходимо ориентироваться на использование отечественных продуктов, в том числе на использование отечественного и санкционно-устойчивого системного и прикладного ПО, вычислительной техники и сетевого оборудования.

8.3. Контроль соблюдения требований ИБ

8.3.1. Для оценки эффективности применяемых мер и средств обеспечения ИБ, а также пригодности и адекватности подхода к обеспечению ИБ, в Университете должны периодически проводиться мероприятия по проверке ИБ (Приложение 1 Положение о внутреннем контроле при обработке персональных данных).

8.3.2. Контроль ИБ может быть, как внутренним, так и внешним. Цель, порядок и периодичность проведения контрольных мероприятий ИБ Университета в целом или его отдельных структурных подразделений указываются в программе контроля ИБ.

8.3.3. При проведении контроля ИБ должны использоваться стандартные процедуры документальной проверки, опрос и интервью с руководством и сотрудниками, технические процедуры тестирования (тестирование на проникновение, нагрузочное стресс тестирование).

8.3.4. К проведению внутреннего контроля ИБ могут привлекаться специалисты, обладающие специальными навыками и знаниями, имеющих значение для проведения проверки.

8.4. Управление информационными активами

8.4.1. Защите подлежит любая информация, принадлежащая Университету или переданная Университету контрагентом в рамках договорных отношений. Степень защиты информации должна выбираться в зависимости от ее категории. Все информационные активы Университета должны защищаться в соответствии с их степенью важности для достижения целей Университета.

8.4.2. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных регламентируется Положением о защите и обработке персональных данных работников и обучающихся ИВГПУ.

8.5. Управление доступом к информационным активам

8.5.1. Управление доступом (в т.ч. удаленного) к информационным активам Университета определяется принципами предоставления работникам и иным третьим лицам минимально необходимых для осуществления их деятельности привилегий. Доступ к информационным активам Университета должен предоставляться только на основании документально обоснованной производственной необходимости (подписанная служебная записка, электронное письмо, согласование в бизнес-процессах Битрикса и т.д.).

8.6. Защита от вредоносного кода

8.6.1. В Университета должны быть реализованы меры защиты от вредоносного программного обеспечения (вредоносного кода) для всех компонентов информационной инфраструктуры.

8.6.2. Должны быть внедрены меры обнаружения, предупреждения и восстановления

последствий воздействия вредоносного кода.

8.6.3. Вопросы защиты от вредоносного кода должны регламентироваться отдельным внутренним документом Университета (Приложение 2 Практические рекомендации по противодействию вредоносному программному обеспечению).

8.7. Защита от утечек информации

8.7.1. В Университета должны осуществляться мероприятия для защиты информации от ее несанкционированного разглашения (утечки).

8.7.2. В рамках данных мероприятий должен осуществляться контроль следующей информации:

- информации, передаваемой в информационно-телекоммуникационную сеть «Интернет»;
- информации, передаваемой с использованием средств электронной почты;
- информации, передаваемой на печать;
- информации, записываемой на съемные носители.

8.7.3. Распространение информации и передача информационных активов Университета (за исключением общедоступной информации) запрещены, если только такое действие не осуществляется согласно случаям, предусмотренным законодательством Российской Федерации, нормативными документами Министерства науки и высшего образования Российской Федерации, внутренними документами Университета.

8.7.4. При переводе работника Университета на другое место работы, вынос информационных активов из структурного подразделения, в котором он работал до перевода, запрещен, за исключением случаев, когда такие действия осуществляются в соответствии с внутренними документами Университета.

8.8. Безопасность сетевой инфраструктуры

8.8.1. В Университете должно быть обеспечено управление безопасностью телекоммуникационных сетей Университета и ее элементов, позволяющее обеспечить защиту информационных активов Университета от угроз, включая постоянный мониторинг состояния сетевой безопасности сети.

8.8.2. Обеспечение безопасности сетевой инфраструктуры регламентируется отдельным внутренним документом Университета (Приложение 3 Регламент использования локальной сети и сети Интернет)

8.9. Криптографические меры защиты информации

8.9.1. В целях защиты конфиденциальной информации в Университета могут применяться средства криптографической защиты информации (далее – СКЗИ).

8.9.2. Использование СКЗИ должно учитывать законодательство Российской Федерации и осуществляться в полном соответствии с технической и эксплуатационной документацией, представляемой производителем СКЗИ.

8.10. Защита среды виртуализации

8.10.1. В Университета должны осуществляться мероприятия для защиты среды виртуализации.

8.10.2. Защита среды виртуализации должна обеспечиваться в соответствии с общими подходами в части обеспечения ИБ, установленными в Университета.

8.11. Регистрация и мониторинг событий

8.11.1. В Университета должны осуществляться регулярный мониторинг и регистрация системных событий, действий пользователей и администраторов, ошибок и событий ИБ.

8.11.2. Все зарегистрированные события должны анализироваться на предмет наличия признаков инцидента ИБ.

8.11.3. Вопросы регистрации и мониторинга событий должны регламентироваться отдельным внутренним документом Университета. (Приложение 4 Регламент реагирования на инциденты компьютерной безопасности)

8.12. Обеспечение безопасности на этапах жизненного цикла информационных систем

8.12.1. Разработка, приобретение, а также внесение изменений (модернизация) в существующие элементы ИС Университета и их сопровождение должно проводиться только после выполнения следующих требований:

- определения требований ИБ, предъявляемых к разрабатываемой, приобретаемой, а также эксплуатируемой ИС Университета или ее элементам, удовлетворяющих требованиям законодательства Российской Федерации, нормативных документов Министерства науки и высшего образования Российской Федерации и внутренних документов Университета в области защиты информации, а также исключающих нарушение характеристик ИБ системы защиты информации Университета;
- создания отдельных сред и тестовых данных для тестирования изменений, вносимых в ИС;
- применения мер ИБ на всех этапах жизненного цикла ИС.

8.13. Резервное копирование и восстановление информации

8.13.1. В Университета должно выполняться регулярное резервное копирование информации, программного обеспечения и образов ИС.

8.13.2. Создаваемые резервные копии должны регулярно тестироваться. Должна быть обеспечена целостность создаваемых резервных копий.

8.14. Обеспечение соответствия требованиям в области ИБ

8.14.1. Для выполнения всех обязательных требований по защите конфиденциальной информации, предписанных законодательными и другими регулирующими (нормативными) документами, в Университета должен выполняться регулярный пересмотр документов по ИБ и содержащихся в них требований.

8.14.2. Руководители структурных подразделений Университета в пределах своей области ответственности должны регулярно анализировать соответствие обработки информации и процедур требованиям внутренних документов Университета по ИБ, в том числе требованиям Политики.

8.15. Повышение осведомленности в области ИБ

8.15.1. В Университете должно осуществляться обучение и повышение осведомленности работников в области обеспечения ИБ.

8.15.2. Должны проводиться регулярные обучающие мероприятия для работников, а также иных третьих лиц, допущенных к информационным активам Университета.

8.16. Организация защиты персональных данных

8.16.1. Персональные данные являются важным информационным активом Университета, в связи с чем Университет должен принимать меры по их защите в соответствии с требованиями законодательства Российской Федерации, нормативными документами Министерства науки и высшего образования Российской Федерации.

8.16.2. Защита персональных данных должна обеспечиваться путем организации корректной обработки, передачи и хранения персональных данных, а также комплексом организационных и технических мероприятий, направленных на обеспечение их безопасности.

8.16.3. Вопросы обеспечения защиты персональных данных регламентируются Положением о защите и обработке персональных данных работников и обучающихся ИВГПУ.

8.17. Организация физической защиты

8.17.1. С целью предотвращения несанкционированного доступа, повреждения оборудования, вторжения в здания и помещения Университета выделены зоны (области) безопасности (в том числе особо важные и выделенные помещения), в которых должен поддерживаться режим физической безопасности.

8.17.2. В зонах безопасности, а также во всех административных, учебных вспомогательных, технических и т.п. помещениях реализованы меры по противопожарной защите, защите от аварий в системах электро-, тепло-, водо-, газоснабжения, канализации и стихийных бедствий.

8.17.3. Лица, имеющие право на доступ в Университет, должны регистрироваться, должен осуществляться контроль доступа в Университет (в том числе с использованием системы контроля и управления доступом (СКУД));

8.17.4. Входные двери помещений должны быть оборудованы механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время;

8.17.5. Серверное и сетевое оборудование ИС должно быть расположено в запираемых серверных стоечных шкафах. Доступ к данным шкафам должен контролироваться;

8.17.6. В случае применения средств видеонаблюдения видеозаписи должны храниться не менее 14 (четырнадцати) календарных дней.

8.18. Применение технических средств защиты информации

8.18.1. Технические средства защиты информации перед их использованием должны быть размещены в информационной инфраструктуре Университета и настроены (сконфигурированы) в соответствии с требованиями эксплуатационной документации.

8.18.2. Для всех применяемых технических средств защиты информации должны быть обеспечена возможность их поддержки (сопровождения) в течение всего срока использования.

9. Ответственность

9.1. Ректор при обеспечении ИБ Университета несет ответственность за:

- утверждение Политики и внутренних документов Университета в части обеспечения ИБ;
- утверждение направлений развития ИБ в контексте снижения рисков;
- выделение финансовых и материальных средств, а также кадровых ресурсов для организации обеспечения ИБ;
- назначение ответственных лиц за обеспечение ИБ.

9.2. Сотрудник, назначенный ответственным за обеспечение ИБ Университета несет ответственность за:

- планирование, контроль, организацию и развитие мер обеспечения и управления ИБ в Университета.
- разработку, документирование и внедрение мер обеспечения и управления ИБ;
- определение мер, необходимых для реализации планов и стратегий в части управления и защиты информации на каждом этапе ее обработки;
- анализ угроз и рисков ИБ, планирование и реализация мероприятий по снижению угроз и управлению рисками, согласование бюджета мероприятий перед руководством Университета;
- выполнение требований законодательства Российской Федерации, нормативных документов Министерства науки и высшего образования Российской Федерации и иных применимых требований в области ИБ;
- управление применяемыми техническими средствами защиты информации, а также их сопровождение;
- контроль за применяемыми мерами ИБ и улучшение (совершенствование) применяемых мер;
- организацию обучения и повышения осведомленности работников в области ИБ.

9.3. Центр технической поддержки (ЦТП) несет ответственность за:

- поддержку и участие в процессах обеспечения ИБ, связанных с использованием информационных технологий;
- соблюдение установленных требований в части обеспечения ИБ при разработке, внедрении и эксплуатации информационных систем и информационных активов;
- участие в процессе анализа угроз и рисков ИБ, планирование и реализация мероприятий по снижению угроз и управлению рисками совместно с ответственным за обеспечение ИБ Университета;
- планирование, реализация мероприятий и бюджета, направленных на сопровождение закупок, эксплуатацию оборудования и информационных систем в целях информационной безопасности;
- управление применяемыми техническими средствами защиты информации, а также их сопровождение;
- предоставление информации о применяемых информационных технологиях и ИС ответственному за обеспечение ИБ Университета.

9.4. Руководители структурных подразделений Университета при обеспечении ИБ в Университета несут ответственность за:

- управление информационными активами, согласование прав доступа к информационным активам, принятие решений по рискам нарушения ИБ, связанным с информационными активами;
- доведение требований по обеспечению ИБ до работников подчиненных структурных подразделений;
- своевременное информирование ответственного за обеспечение ИБ Университета о

выявленных рисках и инцидентах информационной безопасности;

- исполнение требований внутренних документов Университета в части обеспечения ИБ.

9.5. Работники Университета при обеспечении ИБ в Университете несут ответственность за:

- исполнение требований внутренних документов Университета в части обеспечения ИБ.

10. Заключительные положения

10.1. Настоящая Политика подлежит регулярному пересмотру не реже 1 раза в 3 года, а также в следующих случаях:

- изменения требований законодательства Российской Федерации, нормативных документов Министерства науки и высшего образования Российской Федерации;
- существенных изменений в информационной инфраструктуре или организационной структуре Университета;
- выявления инцидентов ИБ, свидетельствующих о неполноте или несовершенстве настоящей Политики.

10.2. Предпосылками для пересмотра и совершенствования настоящей Политики могут также являться результаты мониторинга состояния ИБ, результаты анализа актуальных внутренних и внешних угроз, а также результаты анализа нарушений, выявленных в ходе внутреннего и внешнего контроля (несоответствие реальных технологий и состояния информационной безопасности требованиям нормативных и регламентирующих документов).

10.3. Политика должна быть доведена до всех работников и принята ими к обязательному исполнению. Политика также должна быть доведена до контрагентов и иных третьих лиц, допущенных к информационным активам Университета, и принята ими к обязательному исполнению в части, их касающейся.

10.4. Все работники и студенты Университета, а также иные третьи лица при обращении с информационными активами Университета должны руководствоваться утвержденными требованиями организационно-распорядительных, эксплуатационных, методических и иных документов, связанных с обеспечением ИБ, в том числе требованиями Политики.

10.5. За нарушение требований в области ИБ работники Университета несут персональную ответственность в соответствии с законодательством Российской Федерации.

10.6. Ответственность за осуществление общего контроля выполнения Политики, предоставление рекомендаций по их выполнению, поддержание Политики в актуальном состоянии с учетом требований международных и национальных стандартов, а также законодательства Российской Федерации, нормативных документов Министерства науки и высшего образования Российской Федерации несет сотрудник, назначенный ответственным за обеспечение ИБ Университета.

10.7. Настоящая Политика, а также все изменения к ней утверждаются ректором Университета и вступают в силу после их опубликования.

Разработал

Проректор по административной работе
и цифровому развитию А.Ю. Шарова

Приложение № 1
к Политике информационной безопасности
ФГБОУ ВО «ИВГПУ»

ПОЛОЖЕНИЕ
о внутреннем контроле при обработке персональных данных ФГБОУ ВО «ИВГПУ»

1. Настоящее Положение о внутреннем контроле при обработке персональных данных федерального государственного бюджетного образовательного учреждения высшего образования «Ивановский государственный политехнический университет» разработано в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных" и Положением о защите и обработке персональных данных работников и обучающихся ИВГПУ.

2. Внутренний контроль проводится в целях выявления и предотвращения нарушений законодательства Российской Федерации в области персональных данных.

3. Внутренний контроль подразделяется на плановый и внеплановый.

4. Плановый контроль при обработке персональных данных проводится не реже 1 раза в год на основании плана, утвержденного Приказом ректора федерального государственного бюджетного образовательного учреждения высшего образования «Ивановский государственный политехнический университет» (далее – ИВГПУ, Университет). Срок проведения планового внутреннего контроля составляет не более 10 рабочих дней.

5. Внеплановый контроль проводится на основании поступившего письменного или устного обращения от субъекта персональных данных о нарушении законодательства в области персональных данных. Внеплановый внутренний контроль должен быть завершен не позднее 30 дней со дня принятия решения о его проведении. О результатах внепланового внутреннего контроля информируется заинтересованное лицо.

6. Внутренний контроль проводится комиссией. В состав комиссии входят:

Председатель комиссии – начальник управления делами и кадрами.

Члены комиссии:

- проректор по административной работе и цифровому развитию;
- проректор по образовательной деятельности и воспитательной работе;
- директор Ивановского политехнического колледжа;
- главный бухгалтер;
- заведующий отделом администрирования университетской сети.

7. Комиссия имеет право:

- запрашивать у сотрудников информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства РФ;
- вносить предложения ректору о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства РФ в отношении обработки персональных данных.

8. Контроль осуществляется непосредственно на месте обработки персональных данных путем опроса либо при необходимости путем осмотра рабочих мест лиц, участвующих в процессе обработки персональных данных.

9. При проведении планового контроля соответствия обработки персональных данных установленным требованиям комиссией должно быть полностью, объективно и всесторонне установлено соответствие по следующим положениям:

- наличие, учет, порядок хранения и обезличивания персональных данных;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

10. Результаты внутреннего контроля оформляются в виде акта (Приложение 1), подписываемого членами комиссии.

11. При выявлении в ходе внутреннего контроля нарушений в акте отражаются перечень мероприятий по устранению нарушений и срок их исполнения.

12. В отношении персональных данных, ставших известными в ходе проведения внутреннего контроля лицам, ответственным за проведение внутреннего контроля, соблюдается конфиденциальность и обеспечивается безопасность при их обработке.

Приложение
к Положению о внутреннем контроле
при обработке персональных данных
ФГБОУ ВО «ИВГПУ»

ФОРМА АКТА

Акт №_ от __.__.202_

внутреннего контроля соответствия обработки персональных данных
в ФГБОУ ВО «ИВГПУ»
требованиям законодательства в сфере обработки персональных данных

Комиссия ФГБОУ ВО «ИВГПУ» в составе:

провела внутренний контроль соответствия обработки персональных данных в ФГБОУ ВО «ИВГПУ» требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на 202_/202_ учебный год, утвержденным приказом ректора ИВГПУ №__ от __.__.202_.

В ходе контрольных мероприятий проверены:
- документы, определяющие основания обработки персональных данных;
- утвержденный перечень работников ИВГПУ, имеющих доступ к персональным данным в силу своих служебных обязанностей;
- своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в ИВГПУ, в связи с достижением целей обработки или утраты необходимости в достижении этих целей;
- отсутствие неправомерно размещенных персональных данных граждан на сайте ИВГПУ и иных общедоступных местах.

Выявленные нарушения:
1.
Меры по устранению нарушений:
1.

Срок устранения нарушений:
Ответственный за исполнение:

Подписи членов комиссии: (дата, подпись, расшифровка)

Приложение № 2
к Политике информационной безопасности
ФГБОУ ВО «ИВГПУ»

Практические рекомендации
по противодействию вредоносному программному обеспечению
в ФГБОУ ВО «ИВГПУ»

Данные рекомендации применяются для обеспечения необходимого уровня безопасности информационных ресурсов ИВГПУ (включая информационные системы персональных данных) от вредоносного программного обеспечения.

Противодействие угрозам, связанным с вредоносным программным обеспечением (далее – вредоносное ПО), проводятся в четыре этапа:

1. Подготовка.
2. Регистрация инцидента.
3. Реакция на инцидент.
4. Постинцидентная деятельность.

Этапы 2, 3 и 4 отличаются для штатного (I) и нештатного (II) режимов защиты от вредоносного ПО.

Нештатный режим защиты от вредоносного ПО применяется в случае угрозу вирусной эпидемии, под которой понимается масштабное распространение вредоносного ПО среди компонентов ИС (заражение более трех компонентов ИС одним видом вредоносного ПО) в течение короткого (до суток) промежутка времени.

1. Подготовка

1.1. Для реагирования на инциденты, связанные с вредоносным ПО, должны привлекаться сотрудники отдела администрирования университетской сети ЦТП и отдела обслуживания СВТ и компьютерной техники ЦТП, а также, в случае необходимости, работники, ответственные за компоненты информационной системы, с которыми связан инцидент. Обязанность за координацию действий группы разбора инцидента возлагается на заведующих соответствующих подразделений.

1.2. В план работ ЦТП должно быть включено проведение тренировок для отработки процедур реагирования на инциденты.

1.3. При первичной установке компонентов средств антивирусной защиты в ИС ответственный за установка работник должен предоставить всем пользователям для ознакомления памятку по использованию средств антивирусной защиты и провести инструктаж.

1.4. Для поддержания приемлемого уровня защищенности ИС от вредоносного ПО сотрудники ЦТП в своей повседневной работе должны:

- контролировать процедуры обновления сигнатур угроз компонентов средств антивирусной защиты;
- проверять работоспособность системы централизованного управления компонентами средств антивирусной защиты (например, с помощью средств мониторинга);
- проверять средствами системы централизованного управления компонентами средств антивирусной защиты неизменность состава установленных компонентов средств антивирусной защиты, отслеживать их состояние и обрабатывать сообщения, поступающие от них;
- оперативно выяснять причины неработоспособности или невыполнения компонентами средств антивирусной защиты своих функций и принимать меры по их устранению;
- консультировать пользователей по вопросам работы средств антивирусной защиты и давать им разъяснения по соблюдения требований, указанных в памятках.

I. **Штатный режим**

2. Регистрация инцидента

В штатном режиме участие сотрудника ЦТП в обнаружении вредоносного ПО и применении контрмер не требуется, поскольку данные процедуры производятся средствами антивирусной

защиты автоматически.

3. Реакция на инцидент

Контрмеры по устранению вредоносного ПО применяются автоматически в следующем порядке:

1. Очистка файлов от вредоносного кода.

2. При невозможности очистки файл перемещается в карантин. В случае получения запроса на восстановление до истечения срока карантина сотрудник ЦТП восстанавливает его (по возможности целиком).

3. Удаление файла, содержащего вредоносный код, после истечения срока карантина.

4. Постинцидентная деятельность

Каждый рабочий день сотрудники ЦТП просматривают и анализируют сообщения систем оповещения и системный журнал средств антивирусной защиты на предмет:

- наличия большого числа срабатываний антивирусных средств на различные угрозы на рабочей станции (более 10) и Windows-сервере;

- наличия большого числа срабатываний на одну и ту же угрозу на компонентах информационных систем (для одного компонента информационной системы – более, для различных компонентов информационной системы – более 3).

В случае обнаружения угроз, превышающих обозначенные пороги срабатываний (за исключением ложных), и их рецидива в течение трех суток, сотрудник ЦТП применяет контрмеры в нештатном режиме.

В случае повторяющихся ложных срабатываний на файл данных (по согласованию с ответственным, за информационную безопасность) заносится в список исключений.

II. **Нештатный режим**

2. Регистрация инцидента

Обнаружение и анализ инцидента в нештатном режиме производится следующим образом:

1. Сотрудник ЦТП принимает сообщение об аномальной активности программного обеспечения, поступающие от пользователей, средств мониторинга и оповещения.

2. По факту обнаружения проводится и сопоставление информации об инциденте от первоисточников; сообщения пользователей, сообщения администраторов информационных систем и системные журналы (в т.ч. журналы средств антивирусной защиты, систем обнаружения вторжений и т.д.).

3. Вся собранная информация коррелируется и анализируется с целю выявления типа заражения, его серьезности, масштабов. Также следует выявить предпосылки, предшествующие заражению компонента информационной системы.

3. Реакция на инцидент

Политика сдерживания заключается в прекращении распространения вредоносного ПО и предотвращению дальнейшего повреждения компонентов информационной систем.

На данном этапе, исходя из приемлемости уровня риска, группа разбора инцидентов должна принять согласованное решение о дальнейших действиях, например:

1. Обеспечить пользователей инструкцией по определению вредоносного ПО и дать указания по самостоятельному принятию контрмер.

2. Организовать автоматическое обнаружение вредоносного ПО, предварительно произведя внеплановое обновление антивирусных средств.

3. Оценить последствия, отключить или заблокировать сервисы, используемые вредоносными ПО.

4. Изолировать пораженную систему путем разрыва сетевого соединения. Также в случае масштабного заражения информационных систем вредоносным ПО следует обратиться за помощью в службу техническое

поддержки разработчика средств антивирусной защиты.

На этапе уничтожения вредоносного ПО сотрудник ЦТП самостоятельно, либо привлекая необходимых специалистов из других подразделений, выполняет следующие операции:

- удаляет вредоносное ПО из компонента информационной системы;

- устраняет или уменьшает уязвимость, использованную вредоносным ПО;

- производит установку программных заплаток (патчей), исправляющих недостатки пораженного компонента информационной системы;

- при необходимости, восстанавливают систему из последней незараженной резервной копии;

- в случае рецидива в течение 30 суток, подмены системных файлов, получения вредоносным ПО администраторских привилегий или невозможности устранения деятельности вредоносного ПО – переустанавливается операционная система и перенастраиваются приложения.

После того, как все системы, затронутые в результате инциденты, очищены от вредоносного ПО, следует:

- восстановить данные и функциональность пораженных систем;

- при необходимости, отменить (с восстановлением исходного состояния затронутых компонентов ИС) временные меры, принятые при реагировании на угрозу.

3. Постинцидентная деятельность

В случае необходимости, после устранения связанных с инцидентом последствий следует произвести инструктаж пользователей и/или администраторов пораженной системы, пересмотреть настройки антивирусной политики, а также рассмотреть необходимость внесения изменений в структуре информационной системы (изменение сетевых взаимодействий, реконфигурация ПО и т.д.).

Приложение № 3
к Политике информационной безопасности
ФГБОУ ВО «ИВГПУ»

РЕГЛАМЕНТ
использования локальной сети и сети Интернет в ФГБОУ ВО «ИВГПУ»

1. Общие положения

Настоящий Регламент устанавливает порядок использования локальной сети и сети Интернет работниками и обучающимися федерального государственного бюджетного образовательного учреждения высшего образования «Ивановский государственный политехнический университет» (далее – ИВГПУ, Университет).

2. Основные термины, сокращения и определения

Администратор ИС – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО.

Адрес IP – уникальный идентификатор АРМ, подключенного к ИС ИВГПУ.

АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной задачи.

ИС – информационная система ИВГПУ – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

ПК – персональный компьютер.

ПО – программное обеспечение вычислительной техники, базы данных.

Пользователь – работник, обучающийся ИВГПУ.

3. Порядок использования локальной сети и сети Интернет

3.1. Доступ к локальной сети и сети Интернет предоставляется работникам и обучающимся ИВГПУ в целях выполнения ими своих служебных обязанностей, выполнения научных и учебных задач, требующих непосредственного подключения к внешним информационным ресурсам.

3.2. Операции по предоставлению доступа работников и обучающихся ИВГПУ к локальной сети и сети Интернет и контролю использования выполняются непосредственно (при участии) сотрудниками ЦТП.

3.3. АРМ, используемые для обработки государственной тайны, служебной информации ограниченного распространения (ДСП), не могут быть подключены к сети Интернет.

3.4. При использовании локальной сети и сети Интернет необходимо:

3.4.1. Соблюдать требования настоящего Регламента.

3.4.2. Использовать локальную сеть и сеть Интернет исключительно для выполнения своих служебных обязанностей (учебных и научных задач).

3.4.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Регламента.

3.5. При использовании локальной сети и сети Интернет запрещено:

3.5.1. Использовать предоставленный ИВГПУ доступ в локальную сеть и сеть Интернет в личных целях.

3.5.2. Использовать специализированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к локальной сети и сети Интернет.

3.5.3. Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС ИВГПУ.

3.5.4. Публиковать, загружать и распространять материалы содержащие:

- государственную тайну, служебную информацию ограниченного распространения

(ДСП), конфиденциальную информацию, а также информацию, составляющую коммерческую тайну;

- информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца;

- вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера приобретенного ИВГПУ коммерческого ПО и ПО для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам (если доступ к этим ресурсам был приобретен ИВГПУ), а также ссылки на вышеуказанную информацию;

- угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной и религиозной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.

3.5.5. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.

3.6. ИВГПУ оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, научной и учебной деятельности, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.

3.7. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

4. Ответственность

Работники и обучающиеся, нарушившие требования настоящего Регламента, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами ИВГПУ.

Приложение № 4
к Политике информационной безопасности
ФГБОУ ВО «ИВГПУ»

РЕГЛАМЕНТ
реагирования на инциденты компьютерной безопасности в ФГБОУ ВО «ИВГПУ»

1. Общие положения

1.1. Настоящий Регламент устанавливает порядок разбирательства и составления заключений по фактам несоблюдения условий хранения машинных носителей информации, несоблюдения правил использования средств защиты информации, которые могут привести (или привели) к нарушению конфиденциальности, целостности и доступности информации или другим нарушениям в компьютерных и телекоммуникационных сетях, приводящим к снижению уровня защищенности, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления, разбирательства и предотвращения иных инцидентов компьютерной безопасности в федеральном государственном бюджетном образовательном учреждении высшего образования «Ивановский государственный политехнический университет» (далее – ИВГПУ, Университет).

1.2. Регламент разработан в соответствии с федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", федеральным законом от 27.12.2002 № 184-ФЗ "О техническом регулировании", Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", национальным стандартом ГОСТ ИСО/МЭКТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

1.3. Настоящий Регламент разработан для реагирования на инциденты в компьютерных и телекоммуникационных сетях ИВГПУ, не обрабатывающих сведения, отнесенные к государственной тайне и/или к служебной информации ограниченного распространения (ДСП), и обязателен к соблюдению всеми работниками ИВГПУ, участвующими в выявлении, разбирательстве и предотвращении инцидентов компьютерной безопасности (далее – КБ).

1.4. Разбирательство по всем инцидентам КБ проводится центром технической поддержки (ЦТП) с привлечением в необходимых случаях руководителей и сотрудников других подразделений.

1.5. Разбирательство инцидентов КБ, затрагивающих два или более подразделения ИВГПУ, проводится ЦТП с привлечением сотрудников и руководителей соответствующих подразделений.

Сокращения и определения

АРМ – автоматизированное рабочее место;

ИТ – информационные технологии;

КБ – компьютерная безопасность;

ИР - Информационные ресурсы;

DDoS-атака (от англ. Distributed Denial of Service) – распределенная атака типа «отказ в обслуживании»;

DoS-атака (от англ. Denial of Service) – атака типа «отказ в обслуживании».

Инцидент компьютерной безопасности - какое-либо отклонение от нормального процесса использования информационных ресурсов и функционирования информационных систем, повлекшее ущерб для определенных информационных активов ИВГПУ или непосредственно создающее угрозу нанесения такого ущерба.

Внутренний инцидент – инцидент, источником которого является нарушитель, связанный с ИВГПУ непосредственным образом (трудовым договором или иным способом). Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- утечка персональных данных, циркулирующих в компьютерных или телекоммуникационных сетях;
- неправомерный доступ к информации;
- несанкционированное удаление информации;
- компрометация информации;
- мошенничество с помощью ИТ;
- аномальная сетевая активность;
- аномальное поведение бизнес-приложений;
- использование активов ИВГПУ в личных целях или в мошеннических операциях.

Внешний инцидент – инцидент, источником которого является нарушитель, не связанный с ИВГПУ непосредственным образом. Среди системных событий такого типа можно выделить следующие наиболее распространенные:

- атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);
- перехват и подмена трафика;
- фишинг (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям);
- взлом, попытка взлома, сканирование портала ИВГПУ;
- сканирование сети, попытка взлома сетевых узлов;
- вирусные атаки;
- неправомерный доступ к конфиденциальной информации.

2. Выявление инцидента компьютерной безопасности

2.1. Основными источниками информации об инцидентах КБ являются:

- факты, выявленные руководителем структурного подразделения ИВГПУ, сотрудником ЦТП, лицом, назначенным ответственным за информационную безопасность приказом ректора ИВГПУ, а также другими сотрудниками организации.
- результаты работы средств мониторинга КБ, результаты проверок и аудита (внутреннего или внешнего);
- журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;
- обращения субъектов защищаемой информации с указанием инцидента КБ;
- запросы и предписания органов надзора за соблюдением прав субъектов защищаемой информации;
- другие источники информации.

2.2. Основными видами инцидентов КБ в ИВГПУ могут являться:

- разглашение конфиденциальной или внутренней информации, либо угроза такого разглашения;
- несанкционированный доступ - доступ лиц, которые не имеют легального доступа к ресурсам ИВГПУ;
- превышение полномочий - несанкционированный доступ к каким-либо ресурсам сотрудников ИВГПУ;
- компрометация учетных записей или паролей;
- вирусная атака или вирусное заражение;
- нарушение или сбои в работе системы резервного копирования;
- нарушение правил использования защищаемой информации и персональных данных.

2.3. Сотрудник ЦТП может выявить признаки наличия инцидента КБ путем анализа текущей ситуации на предмет ее соответствия требованиям защиты информации. Выявление несоответствий дают основания предполагать факт возникновения инцидента КБ. Любые сведения о происшествие или инциденте КБ должны быть незамедлительно переданы выявившим их

сотрудником в ЦТП или ответственному за информационную безопасность.

3. Анализ исходной информации и принятие решения о проведения разбирательства

3.1. Сотрудник ЦТП после получения информации о предполагаемом инциденте КБ незамедлительно проводит первоначальный анализ полученных данных и докладывает руководителю. В процессе анализа сотрудник ЦТП проводит проверку наличия в выявленном факте нарушений.

3.2. По усмотрению руководителя единичный инцидент КБ, не приведший к негативным последствиям и совершенный сотрудником впервые, фиксируется в карточке данных об инциденте компьютерной безопасности (приложение №1) с присвоением статуса «Разбирательство не требуется»

3.4. В случае наличия признаков инцидента КБ, приведшего к негативным последствиям, классифицирует инцидент, определяет предварительную степень важности инцидента КБ и принимает решение о необходимости проведения разбирательства, информирует руководителя об инциденте КБ который инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

3.5. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте КБ, сотрудник ЦТП по согласованию с руководителем соответствующего подразделения определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

4. Разбирательство инцидента компьютерной безопасности

4.1. Цели и этапы разбирательства инцидента КБ:

4.1.1. Целями разбирательства инцидентов КБ являются:

- выработка организационных и технических решений, направленных на снижение рисков нарушения компьютерной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
- защита прав ИВГПУ, установленных законодательством Российской Федерации;
- защита репутации ИВГПУ и ее информационных ресурсов;
- обеспечение безопасности защищаемой информации;
- обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых в ИВГПУ;
- предотвращение несанкционированного доступа к конфиденциальной информации, и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство инцидента КБ, состоит из следующих этапов:

- подтверждение/опровержение факта возникновения инцидента КБ;
- классификация инцидента КБ;
- подтверждение/корректировка уровня значимости инцидента КБ;
- уточнение дополнительных обстоятельств (деталей) инцидента КБ;
- получение (сбор) доказательств возникновения инцидента КБ, обеспечение их сохранности и целостности;
- минимизация последствий инцидента КБ;
- информирование и консультирование персонала ИВГПУ по действиям обнаружения, устранения последствий и предотвращения инцидентов КБ;
- переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил КБ.

4.2. Порядок проведения разбирательства инцидента КБ:

4.2.1. В процессе проведения разбирательства инцидента КБ обязательными для установления являются:

- дата и время совершения инцидента КБ;
- ФИО, должность и подразделение нарушителя КБ;
- классификация инцидента;

- уровень критичности инцидента КБ;
- обстоятельства и мотивы совершения инцидента КБ;
- информационные ресурсы, затронутые инцидентом КБ;
- характер и размер реального и потенциального ущерба;
- обстоятельства, способствовавшие совершению инцидента КБ.

4.2.2. При инциденте КБ, затрагивающем не более одного структурного подразделения, ЦТП информирует о факте инцидента руководителя соответствующего структурного подразделения.

4.2.3. При инциденте КБ, затрагивающим более одного структурного подразделения, ЦТП информирует руководителей соответствующих подразделений и инициирует проведение разбирательства.

4.2.4. В случае проведения временного отключения прав доступа у предполагаемого нарушителя КБ информация об отключении прав доступа ЦТП направляет руководителю предполагаемого нарушителя КБ.

4.2.5. ЦТП в процессе проведения расследования инцидента КБ при необходимости запрашивает информацию в структурных подразделениях, запрос направляется на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

4.2.6. После получения необходимой информации по инциденту КБ осуществляющий разбирательство ЦТП проводит анализ полученных данных.

4.2.7. В течение 5 (пяти) рабочих дней с момента выявления инцидента КБ сотрудник ЦТП запрашивает у руководителя структурного подразделения объяснительную записку нарушителя КБ. Объяснительная записка должна быть составлена, подписана нарушителем в течение двух рабочих дней и представлена его непосредственным руководителем в ЦТП в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа нарушителя предоставить объяснительную записку, сотрудники ЦТП составляют акт об отказе дать объяснительную записку. В акте необходимо указать причину, по которой запрашивались объяснения, а также указание на то, что объяснения не были даны. Такой акт составляется комиссией не менее трех человек. С актом нарушитель должен быть ознакомлен под роспись. Если нарушитель ставить свою подпись в акте отказался, то необходимо этот факт отказа отразить в акте.

4.2.8. ЦТП совместно с заинтересованными подразделениями проводит оценку негативных последствий от реализации инцидента КБ. В ходе данной оценки учитываются;
- прямой финансовый ущерб;
- репутационный ущерб;
- потенциальный ущерб;
- косвенные потери, связанные с недоступностью сервисов, потерей информации;
- другие виды ущерба или аспекты негативных последствий для ИВГПУ или субъектов защищаемой информации.

4.2.9. С целью минимизации последствий инцидента КБ возможно временное отключение прав доступа сотрудника к информационным ресурсам (ИР) на время проведения расследования. Подобное отключение инициируется ЦТП с обязательным предварительным устным согласованием с руководителем сотрудника.

4.2.10. В случае, если у нарушителя КБ были отключены права доступа к ИР на время проведения разбирательства, то по его результатам ЦТП по согласованию с руководителем нарушителя КБ принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у нарушителя КБ прав доступа к ИР либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР. Если нарушение КБ было вызвано незнанием нарушителем правил (технологии) работы с информационными ресурсами, то основанием для возврата прав доступа является успешное прохождение инструктажа по компьютерной безопасности, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами ИВГПУ.

4.2.11. Восстановление временно отключенных у нарушителя КБ прав доступа к ИР

(разблокировка пользователя) производится на основании служебной записки руководителя структурного подразделения.

5. Оформление результатов проведенного разбирательства

5.1. Собранная в процессе разбирательства инцидента КБ информация фиксируется ЦТП в карточке данных об инциденте компьютерной безопасности (приложение №1) и учитывается при подготовке итогового заключения по инциденту КБ.

5.2. ЦТП формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента КБ.

5.3. Итоговое заключение по инциденту КБ ЦТП направляет руководителям структурных подразделений, затронутых инцидентом КБ.

5.4. Сотрудник ЦТП фиксирует завершение разбирательства в регистрационной карточке инцидента и присваивает инциденту статус «Разбирательство завершено».

5.5. В случае выявления в инциденте КБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, ЦТП передает все материалы по инциденту КБ руководству ИВГПУ для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

6. Завершение разбирательства, превентивные мероприятия

6.1. По завершению разбирательства инцидента КБ, ЦТП передает копии имеющихся материалов (в объеме, достаточном для принятия решения) вышестоящему руководителю нарушителя КБ для решения вопроса о целесообразности привлечения нарушителя КБ к дисциплинарной ответственности.

6.2. На основании полученных результатов разбирательства руководитель структурного подразделения совместно с ЦТП в срок не более 3 (трех) рабочих дней организовывает проведение мероприятий, направленных на снижение рисков информационной безопасности в будущем:

- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя КБ;
- доведение до всех сотрудников структурного подразделения требований внутренних нормативных документов ИВГПУ;
- обсуждение инцидента КБ на совещании руководителей или собрании коллектива;
- отмена неактуальных прав доступа к информационным ресурсам;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

6.3. О результатах проведенного разбирательства инцидента КБ ЦТП при необходимости инициирует подготовку сообщения об инциденте КБ в адрес руководства ИВГПУ.

7. Права, обязанности и ответственность участников разбирательства

7.1. ЦТП имеет право:

- по согласованию с непосредственным руководителем нарушителя КБ требовать предоставлений письменных объяснений по обстоятельствам инцидента КБ у нарушителя КБ;
- запрашивать и получать от сотрудников ИВГПУ, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента КБ.
- инициировать отключение от информационных ресурсов сотрудников, нарушивших правила или требования КБ, на период проведений расследования инцидента КБ в случае если имеется существенный риск того, что продолжение работы сотрудника с ИР может повлечь значительное увеличение ущерба или новые инциденты КБ;
- по результатам расследования инцидента КБ инициировать изменения в информационных ресурсах ИВГПУ с целью повышения их защищенности и снижения рисков инцидентов КБ;
- инициировать процедуры привлечения нарушителя КБ к дисциплинарной и (или)

материальной ответственность согласно внутренним нормативным документам ИВГПУ.

7.2. ЦТП обязан:

- объективно проводить разбирательство каждого инцидента КБ;
- определять первоочередные меры, направленные на локализацию инцидента КБ и минимизацию негативных последствий;
- фиксировать в регистрационной карточке инцидента КБ всю исходную информацию об инциденте КБ и результаты его расследования;
- предоставлять отчеты и рекомендации по проведенным разбирательствам руководству ИВГПУ;
- проводить анализ обстоятельств, способствовавших совершению каждого инцидента КБ, и на его основе, разрабатывать рекомендации и предложения по снижению ущерба от подобных инцидентов КБ и минимизации возможности их повторения в будущем.

7.3. Руководители структурных подразделений и сотрудники ИВГПУ обязаны:

- предоставлять по запросам ЦТП устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента КБ;
- информировать ЦТП о выявленных инцидентах КБ;
- информировать ЦТП имеющихся запросах и обращениях субъектов защищаемой информации.

Приложение 1
к Регламенту о реагировании на инциденты компьютерной безопасности в ФГБОУ ВО «ИВГПУ

КАРТОЧКА
данных об инциденте компьютерной безопасности

Дата события _____ Номер события _____

Информация о сообщающем лице

Фамилия, имя, отчество _____;
Подразделение, должность _____;
Телефон, электронная почта _____;

Описание события КБ

Что произошло _____
_____;
Как произошло _____
_____;
Почему произошло_____
_____;
Пораженные компоненты _____
_____;
Негативное воздействие на защищаемую информацию _____
_____;
Любые идентифицированные уязвимости _____
_____.

Детали события КБ

Дата и время возникновения события _____;
Дата и время обнаружения события _____;
Дата и время сообщения о событии _____;
Классификация события _____
_____;

Закончилось событие? (отметить квадрат)	Да	Нет

Если «ДА», то уточнить, как долго длилось событие в днях/часах/минутах

_____

Тип инцидента КБ

(Отметить один квадрат, затем заполнить соответствующие поля ниже)

Действительный □
Попытка □
Подозрение □

Указать типы угрозы, один из:

Намеренная □

Хищение □
Мошенничество □
Саботаж/физический ущерб □
Вредоносная программа □
Хакерство/Логическое проникновение □
Неправильное использование ресурсов □
Другой ущерб □

Случайная □

Отказ аппаратуры □
Отказ ПО □
Отказ связи □
Отказ электропитания □
Пожар, наводнение □
Другие природные события □

Ошибка □

Операционная ошибка □
Ошибка аппаратной поддержки □
Ошибка поддержки ПО □
Ошибка пользователя □
Ошибка конструкции □
Другие случаи (включая ненамеренные ошибки) □

Неизвестно □

(Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы)

Пораженные активы (если есть)

Информация/Данные _____

Аппаратура _____

Программное обеспечение _____

Средства связи _____

Документация _____

Негативное воздействие/влияние инцидента на финансовую структуру

(Сделать отметку в соответствующих квадратах для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на активы по шкале 1- 10, используя следующие сокращения (указатели категорий): (ФП) – финансовые потери, (КИ) - коммерческие и экономические интересы, (ПД) – информация, содержащая персональные данные, (ПО) – правовые и нормативные обязательства, (М) – менеджмент, (ПП) – потеря престижа.

Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость»)

Качества информации, пострадавшие в результате инцидента	***Отметка о нарушении качеств информации***	**Значимость**	**Указатели**	**Стоимость**
Нарушение конфиденциальности *(несанкционированное раскрытие)*				
Нарушение целостности *(несанкционированная модификация)*				
Нарушение доступности *(недоступность*				
Нарушение неотказуемости				
Уничтожение				

Полные стоимости восстановления после инцидента

	Значимость	Указатели	Стоимость
Где возможно, необходимо указать общие расходы на восстановление после инцидента			
КБ в целом по шкале 1-10 для «значимости» и в деньгах для «стоимости»			

Разрешение инцидента

Дата начала расследования инцидента	
Должность, Фамилия, инициалы лица (лиц) проводившего (их) расследования инцидента	
Дата окончания инцидента	
Дата окончания воздействия	
Дата завершения расследования инцидента	
Место хранения отчета о расследовании	

Причастные к инциденту лица

Лицо	
Организованная группа	
Легально учрежденная организация/учреждение	
Случайность	
Отсутствие нарушителя (*например, природные факторы, отказ оборудования, ошибка человека)*	

Описание нарушителя, действительная или предполагаемая мотивация

Криминальная/финансовая выгода	
Развлечение/хакерство	
Политика/Терроризм	
Месть	
Другие мотивы	

Действия, предпринятые для разрешения инцидента

(например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением…»)

_____

_____

_____

Действия, запланированные для разрешения инцидента

(включая возможные приведенные выше действия)

_____

_____

_____

Заключение

(Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения)

Значительный	Незначительный	Обоснование

Указать любые другие заключения:

Ознакомленные должностные лица с отчетом (должность, фамилия, организация)

_____

_____

_____

_____

_____

Привлеченные лица
(должность, фамилия, имя, отчество, в каком качестве привлекался к расследованию, подпись, дата)

_____

_____

_____

_____

_____

_____